OSB Open Source Business ALLIANCE
Bundesverband für digitale Souveränität e.V.

Mindestanforderungen an die Nutzung von Cloud-Angeboten durch die öffentliche Hand – Version 2

Die Veröffentlichung des Dokuments „Mindestanforderungen an die Nutzung von Cloud-Angeboten durch die öffentliche Hand“ im Herbst 2022 hat ein breites, positives Echo hervorgerufen. Wir wurden von vielen Institutionen angesprochen, haben viel Beifall und viele Ideen für eine weitere Präzisierung bekommen. Diese fassen wir hier in der vorliegenden Version 2 zusammen.

Bund, Länder und Gemeinden stehen vor massiven und drängenden Aufgaben im Bereich der Digitalisierung. Zu ihrer Lösung setzt die öffentliche Hand zunehmend auf die Nutzung von Cloud-Angeboten. Allerdings bestehen dabei für die Verwaltung in besonderem Maße Anforderungen an den Schutz von Daten sowie an die nachhaltige Sicherstellung von Betriebs- und Gestaltungsfähigkeit digitaler Infrastrukturen. Open Source Software ist besonders gut geeignet, diese Anforderungen zu erfüllen.

Schutz von Daten, Diensten und Infrastruktur

Der Staat muss persönliche Daten von Bürgerinnen und Bürgern ebenso wie eigene vertrauliche Informationen wirkungsvoll vor unerlaubtem Zugriff schützen. Dazu muss er jederzeit die Kontrolle darüber bewahren, wer, wann und unter welchen Umständen auf welche Daten zugreifen darf.

Zusätzlich müssen wirtschaftliche Abhängigkeiten und die Gefahr daraus resultierender politischer Zwänge vermieden werden, damit der Staat auch in Krisen- oder Katastrophenfällen resilient ist und die kontinuierliche Verfügbarkeit elementarer staatlicher Funktionen sicherstellen kann. Dazu muss die Einsatzfähigkeit wichtiger digitaler Infrastrukturen und Dienste unabhängig von den Interessen nicht oder nur schwer beeinflussbarer Staaten oder Unternehmen gewährleistet, funktional kontrolliert und an neue Bedürfnisse angepasst werden können. Die Fähigkeiten zur Kontrolle von Datenflüssen sowie zur Nutzung und Gestaltung von Informationstechnologie bilden gemeinsam die Grundlage der digitalen Souveränität des Staates.

Digitale Souveränität schaffen und stärken

Schon heute bestehen auch ohne den Einsatz von Cloud-Computing etwa bei Funktionen der Arbeitsplatzproduktivität kritische Abhängigkeiten, durch die erhebliche Herausforderungen im Bereich digitaler Souveränität entstanden sind. Diese wurden beispielsweise 2019 im Abschlussbericht der im Auftrag des Bundesministeriums des Innern, für Bau und Heimat beauftragten PwC-Studie „Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern“ ausführlich dargestellt.

Darüber hinaus besteht beim Cloud Computing die Gefahr deutlich weitreichender Abhängigkeiten, etwa weil Cloud-Betreiber die Regeln zum Zugriff auf Daten oder für die Erweiterung der eigenen Angebote durch Dritte eigenständig festlegen und ändern können. Auch sinkt bei der Verwendung fremder Infrastrukturen die Möglichkeit zur Kontrolle von Datenflüssen. Die Nutzung von Cloud Computing macht es deswegen zwingend erforderlich, solche potentielle Gefahren einzuschätzen und bewusst damit umzugehen, um später nicht unerwartet mit wirtschaftlich, technologisch oder gar politisch teuer zu bezahlenden Abhängigkeiten konfrontiert zu sein. Nicht zuletzt deswegen wurde eine deutliche Stärkung der digitalen Souveränität Deutschlands zum wichtigen Bestandteil des 2021 beschlossenen Koalitionsvertrages der aktuellen Bundesregierung sowie zum Leitmotiv der 2022 verabschiedeten Digitalstrategie für Deutschland 1.

Im Spannungsfeld aus dem großen Nutzen des Cloud Computings auf der einen und der Gefahr erheblicher Abhängigkeiten mit möglicherweise dramatischen Konsequenzen auf der anderen Seite müssen Staat und Verwaltung nun einen Weg finden, der die Nutzung der Potentiale von Cloud Computing so gut wie möglich erlaubt und gleichzeitig den Erfordernissen digitaler Souveränität, also an Kontrollfähigkeit, Resilienz, Handlungs- und Gestaltungsfähigkeit, Rechnung trägt. Ein wichtiges Instrument dazu ist die Definition von Mindestanforderungen, also von mindestens einzuhaltenden Eigenschaften von Cloud-Diensten 2, welche die Kontroll- und Gestaltungsfähigkeit des Staates jederzeit sicherstellen.

„Digitale Souveränität“ ist im politischen Raum in der Ausgestaltung von Definitionen und Handreichungen ein derzeit breit diskutiertes Feld. Dabei ist das politische Ziel unbestritten. Meist werden Bedingungen definiert, die den Eintritt von „Abhängigkeiten“ vermeiden sollen. In dem Papier „Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung“ 3 werden drei Anforderungskategorien aufgeführt (Selbständigkeit, Selbstbestimmtheit und Sicherheit), die in einem korrespondierenden Eckpunktepapier des IT-Planungsrates festgelegt wurden.

Jedoch sind die vorgeschlagenen Regularien, **wie** dieser „Zustand“ zu erreichen ist, sehr oft auf juristische und prozessuale Aspekte beschränkt. Cloud-Anbieter können z.B. durch Erklärungen und Vertragswerke Zusicherungen geben, deren Einhaltung schwer oder nicht nachprüfbar ist. Oder sie gewähren Nachprüfbarkeit (Sourcecode-Einsicht) einzelnen Parteien gegenüber nur unter strikter Geheimhaltung.

Ob das Ziel der „Nicht-Abhängigkeit“ tatsächlich erreicht wird, hängt jedoch in hohem Maße von Eigenschaften der eingesetzten Technologie ab. Sicherheit in Bezug auf Unabhängigkeit ist ein Ergebnis von **Vertrauenswürdigkeit,** und Selbständigkeit / Selbstbestimmtheit eines von **Offenheit** (im Sinne von Verfüg- und Gestaltbarkeit der Technologie, Resilienz und Anpassungsfähigkeit).

Daraus abgeleitete Mindestanforderungen müssen unabhängig von der Größe des Anbieters gelten, und sollen dementsprechend keinen Anbieter per se ausschließen. Es geht vielmehr darum, dass die Mindestanforderungen zur Sicherung der digitalen Souveränität öffentlich einsehbar und prinzipiell von

1 https://digitalstrategie-deutschland.de/static/67803f22e4a62d19e9cf193c06999bcf/220830_Digitalstrategie_fin-barrierefrei.pdf

2 Unter Cloud-Diensten wird im Kontext dieses Dokuments die Gesamtheit aller notwendigen Bestandteile des Software-Stacks zur Bereitstellung eines „Dienstes“ subsumiert, also Betriebssystem sowie die jeweiligen *aaS Ebenen.

3 https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf

jedermann prüfbar sind. Sie werden im Übrigen schon heute von verschiedensten deutschen und europäischen Cloud- und Software-Anbietern erfüllt.

Die OSB Alliance teilt zudem die in diversen Papieren und Beschlüssen festgehaltene Auffassung von Bundesregierung und IT-Planungsrat, dass diese Eigenschaften in Summe und die Stärkung der digitalen Souveränität nur durch den Einsatz von Open Source Software erreichbar sind. Die OSB Alliance empfiehlt daher, die hier formulierten Kriterien – sinngemäß – in normative Anforderungen z.B. im Rahmen der Deutschen Verwaltungscloud-Strategie, den Sicherheitsanforderungen des BSI und Beschaffungsanforderungen zu verankern.

Sicherheitsanforderungen

Sicherheit spielt beim Cloud Computing eine zentrale Rolle und erfordert unter anderem die kompromisslose Einhaltung von Mindeststandards. Anerkannte und etablierte Sicherheitszertifizierungen des BSI (C5) und künftig der EU (EUCS) sind dabei eine Mindestvoraussetzung für den Betreiber eines Cloud-Angebots. Sie greifen allerdings zu kurz im Sinne prüfbarer technischer Sicherheit. Die hier formulierten Sicherheitsanforderungen sollen stattdessen konkrete technische Voraussetzungen für den verwendeten Softwarestack definieren, die zur Erreichung von echter Souveränität und Unabhängigkeit führen. Ausschließlich vertragliche Konstrukte oder nur begrenzte Verfügbarkeit von Source Code und Konstruktionsdetails der Software führen nicht zu einer dauerhaften Unabhängigkeit des Cloud-Angebots.

Die Kriterien sollen einen Schutz vor der Kontrolle oder eines unberechtigten Zugriffs von Dritten auf sensible Daten – auch und insbesondere durch staatliche Akteure – gewährleisten, vor allem aber auch Resilienz und Sicherheit durch die Unabhängigkeit von einzelnen Softwareanbietern schaffen. Dazu muss unter anderem auch jederzeit eine unabhängige, unangekündigte Prüfung der Einhaltung von Sicherheitskriterien stattfinden können. Weiter sind mindestens die folgenden Anforderungen durch Cloud-Anbieter umzusetzen:

- Cloud-Lösungen bestehen aus komplexen Kombinationen verschiedener Software-Komponenten, die mit so genannten „Software Bill of Materials“ (SBOM) vollständig dokumentiert und für Anwenderorganisationen vollständig transparent gemacht werden müssen. Es muss jederzeit möglich sein, anhand der SBOM festzustellen, welche Software-Komponenten in welchen Versionen der Betreiber zur Zeit nutzt und ob gegebenenfalls Updates zur Korrektur bekannter Sicherheitsprobleme vorliegen und diese bereits in das Cloud-Angebot integriert wurden.
- Typischerweise arbeiten Entwickler und DevOps-Personal bei Betrieb und Weiterentwicklung von Cloud-Diensten international auf komplexe Weise zusammen. Auf Seiten des Anbieters kann dabei gegebenenfalls nicht ausgeschlossen werden, dass Mitarbeiterinnen und Mitarbeiter aufgrund der Einwirkung fremder Gerichtsbarkeiten (z.B. auf Basis des US-amerikanischen CLOUD Act) oder durch unzulässige Beeinflussung auf den Source Code der Cloud einwirken und Schadsoftware oder Hintertüren einbauen. Es muss daher etwa durch die Möglichkeit von Quellcodeanalysen ausgeschlossen werden können, dass Schadsoftware ohne Kenntnis der Kundinnen und Kunden eingespielt werden kann, bzw. vorhanden ist.

- Ohne den jederzeit möglichen Einblick in den Source Code der Softwarekomponenten, mit denen ein Cloud-Dienst realisiert ist, kann der betreffende Dienst nicht als sicher angesehen werden. Die dazu notwendige Möglichkeit der unabhängigen Prüfung darf nicht einseitig durch den Anbieter oder durch Dritte in seinem Auftrag wahrgenommen werden, sondern muss für Kundinnen und Kunden jederzeit selbst durchführbar sein. Es ist deswegen für alle Bestandteile der Cloud jeweils eine Lösung zu bevorzugen, die Open Source ist.
- Der eingesetzte Source Code darf nicht von dem zur Prüfung zugänglich gemachten Source Code abweichen. Die Gleichheit der eingesetzten Versionsstände ist beispielsweise mittels eines Prüfsummenvergleichs zu attestieren.
- Kritische Teile der Cloud-Lösung wie das Nutzermanagement, die Zertifikatsverwaltung und -ausstellung sowie das Schlüsselmanagement sind mittels nachzuweisender architektureller Sicherheitsmaßnahmen, wie sie z.B. als Confidential Computing beschrieben werden, zusätzlich abzusichern.

Resilienz und Widerstandsfähigkeit

Ein zentraler Aspekt von Resilienz ist die operative Souveränität, also die Fähigkeit, IT-Infrastruktur unabhängig von Dritten betreiben, sicher zu halten und an aktuelle Anforderungen anpassen zu können.

- Sofern für den Betrieb Mitarbeiterinnen und Mitarbeiter eingesetzt werden, die nicht ausschließlich lokaler Gesetzgebung verpflichtet sind, besteht die Gefahr, dass diese auf Grund von Gesetzen wie dem US-amerikanischen CLOUD Act verpflichtet sein können, auf Anweisung der jeweiligen Regierungen oder Rechtssysteme Dritten Zugriff auf Daten zu ermöglichen oder den Betrieb der gesamten Infrastruktur zu gefährden. Es dürfen deswegen nur Mitarbeiterinnen und Mitarbeiter eingesetzt werden, die ausschließlich lokaler Gesetzgebung unterstehen.
- In der zum Betrieb von Cloud-Services verwendeten Software dürfen keine Funktionen enthalten sein, die nach Aktivierung den Zugriff auf Daten ermöglichen oder den Betrieb der Infrastruktur gefährden (so genannte „Kill Switches“). Der Nachweis solcher Funktionen ist ohne Zugriff auf den Quellcode praktisch unmöglich, dieser ist deswegen zwingend zu fordern.
- Es muss sichergestellt werden, dass Software-Aktualisierungen, insbesondere solche zur Korrektur sicherheitsrelevanter Probleme, auch dann zur Verfügung gestellt werden können, wenn dies nicht mehr dem Willen des ursprünglichen Herstellers oder des Staates entspricht, in dessen Rechtssystem sich der betreffende Hersteller befindet.
- Schließlich müssen Anpassungen an neuere Anforderungen oder Schnittstellen auch unabhängig vom ursprünglichen Hersteller möglich sein. Dies wird am besten durch die Nutzung von Open Source Code sichergestellt.
- Die Komplexität des gesamten Softwarestacks erfordert die Entwicklung und Einhaltung von Standards beziehungsweise standardisierten Schnittstellen, die sich bestenfalls an weltweit etablierten offenen Industriestandards orientiert.

- Es muss möglich sein, Anwendungen unabhängig von der Infrastruktur zu betreiben und auch beim Wechsel der darunterliegenden Infrastruktur einen Weiterbetrieb ohne größere Anpassungen an der Anwendung sicherzustellen. Daher wird die Verwendung einer universellen Abstraktionsschicht zwischen Anwendungen und Infrastruktur empfohlen. Die OSB Alliance wird dazu in Kürze ein Konzept vorlegen.

Rechtliche Anforderungen

Bei der Beschaffung von Cloud Services durch die öffentliche Verwaltung müssen insbesondere die folgenden rechtlichen und vertraglichen Eigenschaften der jeweiligen Angebote sichergestellt werden:

- Sämtliche verarbeiteten Daten (wie Nutzerdaten, Log-Dateien, Abrechnungsdaten, etc.) müssen Anwenderinnen und Anwendern durch den Cloud-Anbieter jederzeit unmittelbar und / oder im Rahmen eines zertifizierten „Takeout"-Verfahrens zur Verfügung gestellt werden können. Zur Nachvollziehbarkeit, Zertifizierung und jeder anderen Bewertung im Bereich Datenschutz und Datensicherheit ist ebenfalls erforderlich, dass die Software und deren spezifischer Code quelloffen und auditierbar sind.
- Der Cloud-Anbieter muss sicherstellen, dass die gesamte Datenhaltung und die Technik ihrer Verarbeitung portabel und mit quelloffenen Software-Stacks auf anderen IaaS-Plattformen einsetzbar ist. Dies kann z.B. durch quelloffene Standards bei Dateiformaten und quelloffener Darstellung der algorithmischen Verarbeitung umgesetzt werden. Es muss technisch und organisatorisch möglich sein, die Datenverarbeitung jederzeit zwischen Datenräumen beliebiger Anbieter transportabel zu machen. Datenräume in diesem Sinne basieren auf Open Source Software und der Möglichkeit, auf beliebigen IaaS-Plattformen lauffähig zu sein.
- Die von einem Cloud-Anbieter bzw. einem Subunternehmer implementierten technischen und organisatorischen Maßnahmen (sog. TOMs) müssen - neben den klassischen Schutzzielen an die allgemeine Daten- und Informationssicherheit (unter anderem Vertraulichkeit, Verfügbarkeit und Integrität von Daten, wie sie z.B. auch in Art. 32 DSGVO benannt sind) - auch Maßnahmen in Bezug auf Quelloffenheit und Transportabilität enthalten. Verträge mit einem Cloud-Anbieter sollten nur dann abgeschlossen werden dürfen, wenn Quelloffenheit und Transportabilität der Daten innerhalb gesicherter Datenräume gegeben ist und der Cloud-Anbieter diesbezüglich vertragliche Zusagen macht.
- Alle Daten „at rest" oder „in flight" müssen jederzeit nachvollziehbar (mit quelloffenen Algorithmen) und zertifizierbar bzgl. der Kriterien der Sicherheit und Portabilität verschlüsselt werden. Gleichzeitig ist sicherzustellen, dass über algorithmische Vorkehrungen gesicherte Wege bestehen, Daten in anonymisierter Form oder anonym konvertiert für Auswertungen etc. zu verwenden. Denn zu keinem Zeitpunkt sollten Daten, die besonderen Compliance-Anforderungen unterliegen (wie z.B. der DSGVO) in unsicheren Kontexten bearbeitet werden. Die technische Realisierung und Umsetzung der eingesetzten Verschlüsselungs- und Pseudonymisierungstechnologien ist nachvollziehbar und auditierbar nachzuweisen.

- Anbieter sind zu verpflichten, die Rechte von Bürgerinnen und Bürgern bezüglich des Umgangs mit personenbezogenen Daten zu achten und Wege für die Erfüllung von Betroffenenrechten (wie z.B. Einsicht, Löschung, Recht auf Berichtigung, Recht auf Löschung) nachvollziehbar bzgl. Verarbeitung, Umsetzung und Speicherort umzusetzen. Dazu müssen offene Standards und quelloffene Software verpflichtend gemacht werden.

Handlungsempfehlungen für Politik und Verwaltung:

Ein planvolles Handeln von Politik und Verwaltung auf Bundes-, Landes- und kommunaler Ebene ist in besonderem Maße Voraussetzung für die Schaffung und Sicherung digitaler Souveränität. Hierzu sprechen wir die folgenden Empfehlungen aus:

- Auf den verschiedenen staatlichen Ebenen müssen klare Verantwortlichkeiten für Beschreibung und Festlegung von verbindlichen Mindestanforderungen an Cloud-Lösungen benannt werden. Die Übernahme dieser Aufgabe durch den IT-Planungsrat als gemeinsames Instrument des Bundes und der Länder sollte evaluiert werden.
- Die Festlegung von Mindestanforderungen sollen in einem mehrstufigen, für die Wirtschaft transparenten und iterativen Prozess erfolgen.
- Die Anforderungen auf nationaler Ebene sind eng mit der europäischen Ebene abzustimmen. In diesem Kontext ist auf einen gemeinsamen Vergaberahmen in Europa hinzuwirken, der die hier aufgeführten Empfehlungen zur Absicherung digitaler Souveränität in Europa berücksichtigt.
- Verbindliche Mindestanforderungen müssen als wichtige Basis in Beschaffungsprozessen integriert werden. Dabei sollten zusätzlich zu den verbindlichen Anforderungen (Muss-Bedingungen) ergänzende Kann-Bedingungen in die Wertung aufgenommen werden.
- Im Rahmen der Definition der Mindestanforderungen sollte eine Metrik zur Messung der Kritikalität von Cloud-Diensten erarbeitet werden. Mit verschiedenen, zu definierenden Stufen der Kritikalität sollen dedizierte Muss-Anforderungen an den Betreiber wie auch die technologische Basis des Services verknüpft werden. Bei einer hohen Kritikalität der Services sollen alle formulierten Anforderungen - etwa der Betrieb in Deutschland durch Personal mit deutscher Staatsbürgerschaft unter ausschließlichem Einsatz von Open-Source-Software – erfüllt werden.
- Im Rahmen von Beschaffungsprozessen sind langfristige Wirtschaftlichkeitsbetrachtungen vorzunehmen, die auch Kosten für die Außerbetriebnahme von Cloud-DIensten und die Ersetzung von Anbietern berücksichtigen („Exit-Kosten“). Zur Reduktion der Kosten bei der Ersetzung eines Anbieters sind Angebote, bei denen alternative Anbieter den Betrieb eines Cloud-Dienstes übernehmen können, stets zu bevorzugen.
- Bei der Auswahl von Cloud-Diensten ist darauf zu achten, dass diese Angebote ausschließlich offene Schnittstellen, für die es Open-Source-Referenzimlementierungen gibt, nutzen und anbieten.
- Im Falle von durch den Staat beauftragter Individualsoftwareentwicklung, sollten entsprechende Ergebnisse immer unter Open-Source-Lizenz veröffentlicht werden. Werden Standard-Services

eingekauft, so sollten für diese immer Open-Source-Lösungen proprietären Lösungen gegenüber bevorzugt werden.

- Bei den Förderstrategien des Bundes und der Länder für Forschungs- und Entwicklungsaktivitäten sind die Erfordernisse zur Gewährleistung digitaler Souveränität mit einem besonderen Fokus auf Open-Source-Lösungen zu berücksichtigen. Hierdurch sollen in spätere Produktentwicklungen mündende Forschungs- und Entwicklungsaktivitäten auf die Erfüllung der Mindestanforderungen von Beginn an konsequent vorbereitet werden.

Autoren:

- Marius Feldmann, Cloud & Heat
- Peter Ganten, Vorstandsvorsitzender der OSB Alliance, Univention
- Bernhard Hecker
- Stephan Ileander (initial Stefan Herold), STACKIT
- Stephan Ilaender, STACKIT
- Timo Levi, stellvertretender Vorstandsvorsitzender OSB Alliance, T-Systems International
- Kai Martius, secunet
- Rainer Sträter, IONOS