DIGITALE SOUVERÄNITÄT IM CLOUD-ZEITALTER

7 Hebel für mehr Souveränität in der öffentlichen Verwaltung

cloud ahead

Autor: Gregor Schumacher
Kontributoren: Jockel Merholz, Max Hille, Andreas Tamm, Prof. Dr. Roland Frank, Lisa Steigertahl, Wilfried Bauer

20. März 2023
Vers. 1.0

Inhaltsverzeichnis

Management Summary

Die Erwartungen der Bürger an die Rolle der öffentlichen Hand haben sich mit zunehmender Digitalisierung gewandelt. Der Staat soll nicht nur Daten und Infrastrukturen unter Kontrolle behalten, er soll auch digital leistungsfähiger werden.

Die wichtigsten Hebel für mehr Souveränität hat cloud ahead in der vorliegenden Studie untersucht. Die zentralen Ergebnisse lauten: **Verschlüsselung** schützt besonders vor Kriminellen, **Multi-Cloud** vor Abhängigkeiten gegenüber einzelnen Unternehmen und **Open-Source-Software** vor fremder Legislation und geo-politischen Abhängigkeiten. Die **Kontrolle der Wertschöpfungskette** („rote Linien des BSI") ermöglicht den Zugang zu überlegener Technologie, erhöht aber einzelne Abhängigkeiten. **Eigenleistung** in Architektur und Steuerung verbessert sowohl Leistungsfähigkeit als auch Kontrolle. Die Nutzung der **Public Cloud** verbessert besonders die Leistungsfähigkeit, führt aber zu geopolitischen Abhängigkeiten sowie Risiken beim Zugriff fremder Legislationen. Die Optimierung der eigenen Organisation anhand der **Best-Practices der Software-Branche** bringt Vorteile in allen Bereichen, erfordert aber die organisationsinterne Bereitschaft zum Wandel.

cloud ahead empfiehlt folgendes Toolkit für mehr Souveränität in der IT:

Die Nutzung der Cloud führt zu einer Industrialisierung der klassischen IT – vergleichbar mit der Einführung der Dampfmaschine in der Textilindustrie des 19. Jahrhunderts. Diese Industrialisierung bedeutet einen **Paradigmenwechsel** für alle Beteiligten. Führungskräfte und ExpertInnen sollten daher stets vor der Planung einer umfangreichen Cloud-Transformation die **neuen Technologien und Arbeitsweisen in geschützten Umgebungen** und angepasst auf den **jeweiligen Anwendungsfall ausprobieren**.

Einleitung

Die Rolle des Staates im digitalen Wandel

Der IT-Planungsrat definierte 2019 digitale Souveränität[1] wie folgt: Öffentliche Institutionen sollen „ihre Rolle in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben können". Die Anforderungen insbesondere der BürgerInnen an die Rolle des Staates haben sich geändert. Nicht nur soll er sorgsam und vertraulich mit den Daten der BürgerInnen umgehen, er soll sie auch zu deren Nutzen einsetzen.

Seien es die Corona-Warn-App, der Bafög-Antrag oder die digitale Patientenakte, die Erwartungen an die digitale Leistungsfähigkeit des Staates sind gestiegen. BürgerInnen wissen, was technisch möglich ist und fordern dies von Ministerien, Bürgerämtern und Krankenhäusern ein.

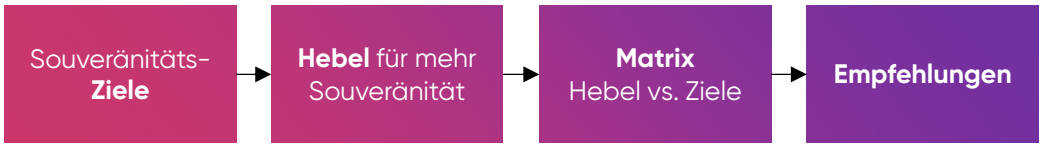
„Die jetzige IT-Infrastruktur vieler Verwaltungen kann die modernen digitalpolitischen Anforderungen an eine agile Ressort und Fachübergreifende Bearbeitung nicht erfüllen."

Lisa Steigertahl
Microsoft

Den Diskurs um Souveränität sortieren

In diesem Whitepaper werden die Erwartungen an die digitale Souveränität des Staates analysiert und eingeordnet. LeserInnen können mit dieser Hilfe die eigenen Anforderungen an digital souveräne IT für ihren Anwendungsfall bestimmen. Zudem gibt das Whitepaper eine erste Hilfestellung, mit welchen Stellschrauben die LeserInnen ihre Souveränitätsziele besser erreichen können.

Im ersten Teil werden die vielfältigen Souveränitätsziele in jeweils sechs Ziele für Leistungsfähigkeit und Kontrolle kategorisiert. Im zweiten Teil werden sieben Stellhebel erläutert, die im medialen Diskurs als Mittel zur Steigerung der Souveränität genannt werden. Mit Hilfe einer Matrix bewertet die Studie von cloud ahead, wie diese Stellhebel auf die Erreichung der Souveränitätsziele einwirken. Unter Berücksichtigung der für die jeweiligen Hebel notwendigen Ressourcen werden im dritten Teil strategische Empfehlungen ausgesprochen und ein operativer Handlungsvorschlag erstellt.



Im vierten und letzten Teil werden Anwendungsfälle vorgestellt, welche die empfohlenen Maßnahmen mit Praxisbeispielen unterlegen.

1. Was ist Souveränität genau?

Autarkie vs. Souveränität auf der Ebene der IT

Die AutorInnen der Schwerpunktstudie Digitale Souveränität[2] haben die Sichtweisen von Organisationen, wie der Bertelsmann Stiftung, dem Bitkom sowie der Konrad-Adenauer-Stiftung und diverser Bundes-Ministerien zusammengetragen. Die Sortierung der Schlüsselworte aller 18 Definitionen führt zu drei Wortclustern[3]: Organisationen möchten (1) digitale Leistungsfähigkeit erreichen ohne dabei an (2) Kontrolle zu verlieren. Alle Entscheidungen in diesem Kontext sollen in (3) Selbstbestimmung erfolgen. Der gemeinsame Kern aller Definitionen ist somit:

Digitale Souveränität ist die selbstbestimmte Kombination aus Leistungsfähigkeit und Kontrolle.

Richtig klar wird die Herausforderung erst im Lichte des Impulses des Bitkom[4] aus dem Jahr 2015. Dort zieht der Verband eine Linie zwischen Autarkie und Souveränität. Erstere priorisiert die mit Eigenleistung verbundene Kontrolle, auch wenn diese mit Einbußen an Leistungsfähigkeit verbunden ist. Letztere versucht mittels Steuerung von Alternativen eine insgesamt bessere Balance aus Leistungsfähigkeit und Kontrolle zu erreichen.

Die deutsche Akademie der Technikwissenschaften (acatech)[5] hat in ihrer Studie aus dem Jahr 2021 ebenfalls zu diesem Thema geforscht und viele relevante Handlungsebenen definiert. Beleuchtet wurden dort neben IT-Themen unter anderem die Aspekte Rohstoffe (wie z.B. Silizium), Komponenten (wie z.B. Chips) und Werte (z.B. Datenschutz).

Dieses Whitepaper fokussiert sich allerdings ausschließlich auf jene Bereiche, die im Handlungsspielraum der IT von Unternehmen und öffentlichen Organisationen liegen, wie etwa IT-Infrastruktur und Software.

„Emotionalität und mangelnde Klarheit zu den eigentlichen Souveränitätszielen führen zu Debatten, die sich im Kreis drehen."

Gregor Schumacher
cloud ahead

Diese Whitepaper fokussiert sich auf die Souveränität in der IT.

Die konkreten Ziele der digitalen Souveränität

Der Versuch, Leistungsfähigkeit und Kontrolle in einer Organisation gleichzeitig zu optimieren, führt zu komplexen interdisziplinären Fragestellungen. Mit der Public Cloud lassen sich Anwendungen schnell entwickeln, aber wie ist es mit dem Datenschutz?

Die Private Cloud schützt vor dem Cloud Act, aber löst sie die Abhängigkeit von amerikanischer Technologie? Vor geopolitischen Risiken schützt uns Open-Source-Software, aber verstehen NutzerInnen deren graphische Oberflächen?

Reduktion der Vielfalt der Diskussion mittels Ziel-/Mittel-Hierarchie

In der Praxis sind viele **Souveränitätsziele gegenläufig**.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinem Dokument „rote Linien des BSI“[6] insgesamt 121 Anforderungen an IT-Infrastrukturen gestellt, damit diese als „souverän“ gelten können. Das Dokument wiederum verweist auf weitere Anforderungskataloge, wie IT-Grundschutz oder C5.

Um Dialoge transparenter führen zu können, hat cloud ahead die Vielzahl dieser Anforderungen auf die Frage hin analysiert, ob sie ein zugrundeliegendes Ziel formulieren („Ein Drittstaat darf keinen Zugang zu den Daten erhalten“) oder lediglich ein Mittel zu einem solchen Ziel darstellen („Das Rechenzentrum muss auf deutschem Grund stehen“).

Als Ergebnis dieser Analyse hat cloud ahead jeweils sechs Souveränitätsziele bezogen auf Leistungsfähigkeit und Kontrolle identifiziert.

Souveränitätsziele bezogen auf Leistungsfähigkeit

Bürger erwarten eine **Leistung vom Staat**, wie sie es von Amazon, Tesla und Microsoft gewöhnt sind.

Die private Nutzererfahrung der Bürger gibt die Leistungswünsche vor: Die Apps des Staates sollen einfach verständlich und intuititv nutzbar sein. Anträge sollen sofort und automatisiert in der Anwendung bearbeitet werden. Besonders in Krisenzeiten, wie einer Pandemie, sollen neue Funktionen schnell verfügbar sein.

Fachliche Probleme	Fachliche Probleme sollen technisch und endnutzerfreundlich gelöst werden.
Automatisierung	Der Automatisierungsgrad der Organisation soll durchgängig erhöht werden.
Schnelle Innovationen	Innovationen werden schnell in Software umgesetzt.
Applikations-Landschaft	Alle Applikationen sollen zuverlässig betrieben werden können.
Einfache Zugänglichkeit	Services und Daten sollen sicher und aktuell sowie einfach zugänglich sein.
Skalierbarkeit	Die Applikation muss den Nachfrage-Schwankungen entsprechend skalieren können.

Souveränitätsziele bezogen auf Kontrolle

Kontrollziele lassen sich häufig der Berichterstattung der Medien entnehmen: Die Rechenzentren sollen vor Schäden geschützt werden, Kriminelle und Geheimdienste sollen nicht an Daten gelangen. Abhängigkeiten zu einzelnen Unternehmen oder Drittländern dürfen nicht entstehen. Letztere sollen auch keinen legislativen Zugriff auf Daten erhalten.

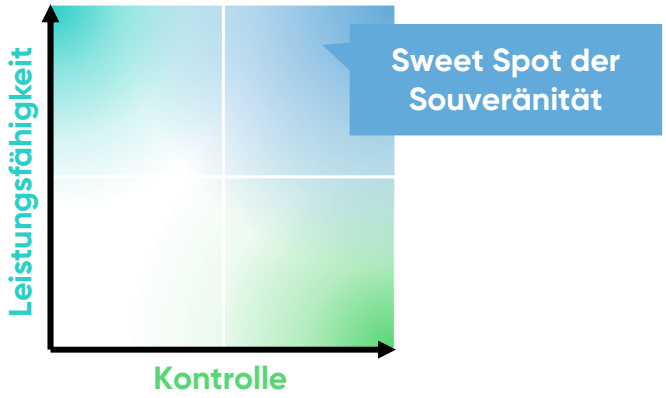
Physische Gefahren	Funktionsfähigkeit bei physischen Gefahren soll erhalten bleiben.
Einzelne Abhängigkeiten	Abhängigkeiten zu einzelnen Unternehmen sollen beherrschbar sein.
Kriminelle	Zugriff durch Kriminelle soll verhindert werden.
Fremde Legislation	Zugriff durch fremde Legislation soll verhindert werden.
Fremde Geheimdienste	Zugriff durch fremde Geheimdienste soll verhindert werden.
Geopolitische Krisen	Funktionsfähigkeit bei geopolitischen Krisen soll erhalten bleiben.

Kontrollziele vollständig zu erreichen, ist auch für die größten Akteure nicht trivial. Amazon etwa arbeitete jahrelang daran, seine Abhängigkeit von Oracle-Datenbanken aufzulösen.[7] Die USA wiederum streben nach Reduktion ihrer geopolitischen Risiken, beispielsweise bezogen auf die Verwundbarkeit der Chip-Produktion in Taiwan durch China.[8]

Kontrollziele erreichen bedeutet insbesondere **negative Berichterstattung in den Medien** zu vermeiden.

Die Matrix der Souveränität nach cloud ahead

Souveränität ist die selbstbestimmte Kombination aus Leistungsfähigkeit und Kontrolle. Mit den konkreten Souveränitätszielen im Hinterkopf kann sich nun jede Organisation selbst in einem der vier Quadranten einer Matrix verorten.



Instagram konnte mit lediglich **13 Mitarbeitenden und der Public Cloud** binnen 551 Tagen auf 30 Millionen globale NutzerInnen wachsen.[9]

Das Pentagon gibt 9 Mrd. US$ aus, um basierend auf Technologie von Microsoft, Google, Oracle und AWS eine **eigene Cloud mit mehr operativer Kontrolle** zu erhalten.[10]

2. Wie ist mehr Souveränität möglich?

Hebel für mehr Souveränität in der IT

Wie aber sehen Lösungen aus? Welche Maßnahmen können Organisationen ergreifen, wenn sie digital leistungsfähiger werden möchten? Welche Optionen bestehen für mehr Kontrolle? Von ExpertInnen, BeraterInnen und Verbänden werden meist folgende Maßnahmen genannt:

Hebel	Beschreibung	Beispiele
Verschlüsse-lung	Daten und Kommunikation werden verschlüsselt, es werden besondere Schlüsselverfahren genutzt und die Schlüssel selbst werden gesondert verwaltet.	Encryption at transit, at rest, at compute, BYOK, HYOK, DKE, Confidential Computing, Quantum safe, …
Multi-Cloud	Anwendungen werden auf mehrere Clouds verteilt, Architektur und Betrieb entsprechend angepasst, übergreifende Steuerungsprozesse etabliert.	Multi-Cloud, Hybrid Cloud, Graceful Degradation, API Layer, Container-Orchestrierung, …
Open-Source	Der Code der genutzten Software ist frei verfügbar und kann, gemäß der eigenen Bedarfe, angepasst werden.	OpenStack, Linux, Kubernetes, log4j, dPhoenix, LibreOffice, …
Kontrolle der Wert-schöpfung	Software und Hardware unterliegen besonderen Anforderungen oder Regulierungen und werden hinsichtlich dieser kontrolliert.	C5-Zertifizierung, Collaborative Cloud Audit Group (CCAG), Cloud Platform Requirements („rote Linien") des BSI, …
Eigen-leistung	Der Nutzer der IT erbringt die gesamte Leistung oder Teile der Wertschöpfung eigenständig.	Lieferantensteuerung, Architektur, Software-Entwicklung, Betrieb, Hardware-Design, …
Public Cloud	Nutzer konsumieren frei am Markt verfügbare Standard-IT-Services für Infrastruktur & Middleware oder mit fachlicher Ausrichtung wie Sales oder Workplace.	AWS, Azure, GCP oder Google Workplace, O365, Salesforce, DeepL, Okta, …
Software-Flow	Die Organisation übernimmt Best-Practices aus Software-Unternehmen um die Fluss von der Idee bis zur funktionierenden Applikation zu optimieren.	Agile, SAFe, Scrum, CI/CD, DevOps, SRE, automatisierte Tests, entkoppelte Architekturen, API Management, …

„Der unternehmens-übergreifende Open-Source-Ansatz von cloud ahead ist der neutralste Weg, um die Diskussion zur digitalen Souveränität zu sortieren."

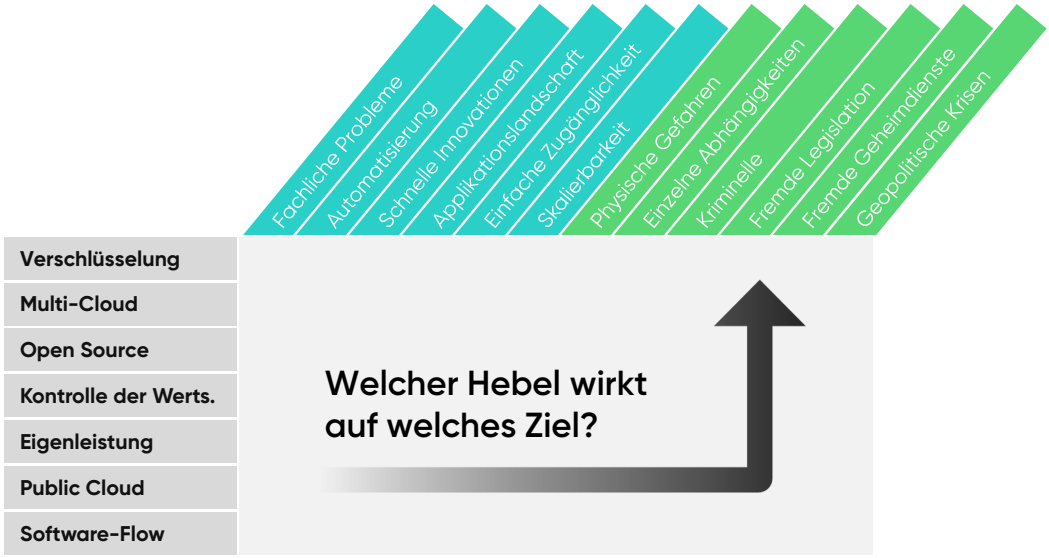
Prof. Dr. Roland Frank
cloud ahead

Die 7 Hebel sind nicht überschneidungsfrei (MECE)[11] sondern greifen bewusst die meist-genutzten Begriffe der Fachdebatte auf.

Welcher Hebel wirkt auf welches Souveränitätsziel?

Die LeserInnen dieses Dokuments sollen eine Hilfestellung erhalten, mit welchen Maßnahmen sie ihre spezifischen Souveränitätsziele erreichen können. Hilft beispielsweise Multi-Cloud bei dem Schutz vor Kriminellen? Können sich Organisationen mit Verschlüsselung in der Public Cloud vor fremder Legislation schützen? Ist Eigenleistung der Schlüssel zu schnellen Innovationen?

Insgesamt 84 Hebel/Ziel-Kombinationen hat cloud ahead überprüft und bewertet. In der unter www.cloudahead.de abrufbaren Excel-Datei wird beispielsweise abgewogen, inwiefern die Einführung einer Multi-Cloud-Lösung bei einer geopolitischen Auseinandersetzung mit der USA[12] schützt – oder ob die Public Cloud Vorteile bei der Absicherung gegenüber physischen Gefahren mit sich bringt.



Weitere Details zur Methodik der Abwägung werden in einer Excel-Datei auf www.cloudahead.de erläutert.

Auf den folgenden Seiten werden die Ergebnisse daraus kondensiert dargestellt und mit Hilfe von Farben visualisiert. Rot (mit entsprechenden Schattierungen) bedeutet, dass der Hebel überwiegend negativ auf das Souveränitätsziel wirkt, grün (mit entsprechenden) Schattierungen deutet auf eine überwiegend positive Wirkung hin.

Mehr Leistungsfähigkeit durch Public Cloud und Software-Flow

Die Kriterien der digitalen Leistungsfähigkeit sind intuitiv gut greifbar: Organisationen, deren Softwares einfach zu nutzen sind, schnell an aktuelle Bedarfe angepasst werden und automatisiert Kundenbedarfe lösen, werden als leistungsfähig wahrgenommen.

Die folgende Tabelle zeigt die für Leistungsfähigkeit wichtigsten Hebel in grün.

Besonders hervorzuheben ist der Software-Flow[13]. Dieser entsteht, wenn Organisationen sich nach den Best-Practices der Software-Entwicklung ausrichten. Dazu gehört die Einführung agiler Methoden (z.B. Scrum oder SAFe), eine enge Verzahnung von fachlichen ExpertInnen mit EntwicklerInnen und Betriebs-ExpertInnen (zB. DevOps, SRE) sowie eine weitgehende Automatisierung der Test- und Deployment-Prozesse (zB. CI/CD).

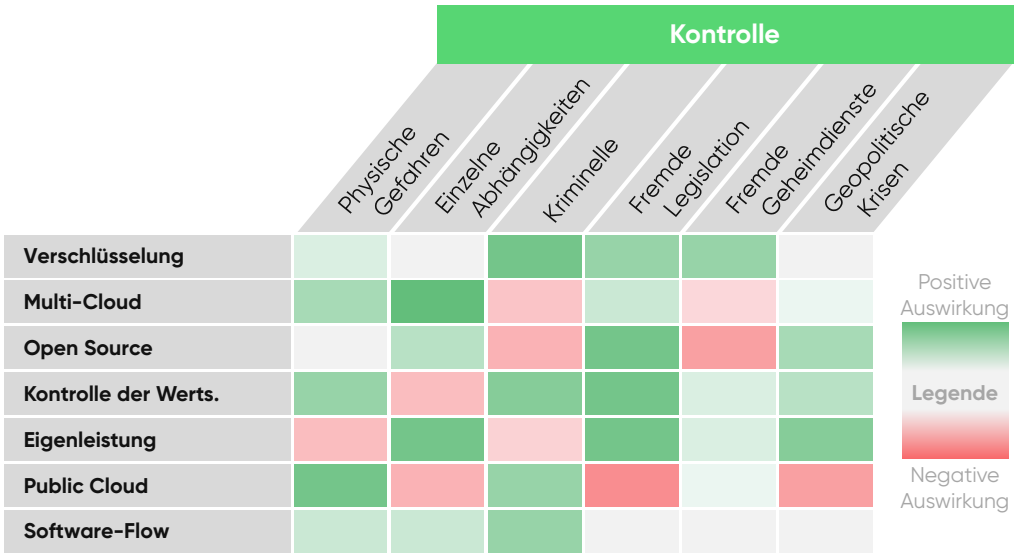
Der Hebel Public Cloud kann sich ebenfalls sehr positiv auf die Leistungsfähigkeit auswirken[14]. Aufgrund der vielen verfügbaren Standard-Services können Organisationen mit wenig eigenen Mitteln komplexe Applikationen entwickeln. Der größte Vorteil gegenüber Private Clouds ist die Tatsache, dass alle Services für Software-Entwickler sehr einfach zugänglich sind – sowie automatisiert bestellt, genutzt und abgerechnet werden können. Die Public Cloud ist daher besonders einfach in den oben genannten Software-Flow einzubinden.

Als dritter Faktor zu nennen ist die Eigenleistung. Insbesondere die Optimierung des Software-Flows sowie die Nutzung der Public Cloud benötigt viel Kompetenz in Software-Architektur, Compliance, Steuerung von Lieferanten und Veränderung der eigenen Organisation.

Mehr Kontrolle durch Datenkategorisierung

Die Beantwortung der Frage nach Hebeln für mehr Kontrolle gestaltet sich schwieriger. Denn einige Kontrollziele verhalten sich gegenläufig. Beispielsweise bietet die Public Cloud, aufgrund ihrer physischen Skalierung, ihrer hoch-automatisierten Update-Prozesse und des Umfangs ihrer Cybersecurity-Abteilungen, einen sehr guten Schutz gegenüber einigen physischen Gefahren und Kriminellen.[15]

Umgekehrt gibt es bezogen auf Public Cloud berechtigte Sorgen hinsichtlich fremder Legislation oder geopolitischer Risiken. Multi-Cloud hingegen kann vor Abhängigkeiten gegenüber einzelnen Unternehmen schützen, reduziert aber im Regelfall kaum geopolitische Abhängigkeiten. An dieser Stelle wird daher keine pauschale Empfehlung gegeben. Je Anwendungsfall kann aus der Hebel-/Ziel-Matrix abgeleitet werden, welche Souveränitätsziele mit welchen Hebeln erreicht werden können:



Arvato Systems hat im Zuge der Pandemie eine pragmatische Datenkategorisierung vorgenommen und **binnen 4 Wochen eine funktionierende Multi-Cloud-Lösung** bereitgestellt.[17]

Multi-Cloud löst insbesondere Abhängigkeiten gegenüber einzelnen Unternehmen auf. Open-Source und Eigenleistung sind der Schlüssel im Umgang mit geopolitischen Risiken sowie bei der Auflösung von Abhängigkeiten gegenüber einzelnen Unternehmen. Verschlüsselung mit nativen Methoden der Public Cloud schafft hohe Leistungsfähigkeit bei einer Optimierung der Kontrolle, bezogen auf physische Gefahren und Kriminelle[16].

In allen Fällen aber bleibt eine pragmatische Betrachtung der individuellen Situation der Schlüssel für eine tatsächliche Verbesserung der Kontrolle. Werden etwa Daten und Applikationen aktuell in einem unzureichend geschützten Serverschrank gehostet und Softwarestände dort nicht zügig aktualisiert, dann summieren sich Eintrittswahrscheinlichkeit und Schaden einer Cyberattacke zu einem sehr hohen tatsächlichen Risiko. Im Vergleich dazu stehen Eintrittswahrscheinlichkeit und Schaden bei der Anfrage einer US-Behörde auf verschlüsselte Daten bei der Nutzung eines vergleichbaren Standard-Services der Public Cloud.

Mit einer guten Analyse von Daten und Souveränitätszielen kann im konkreten Fall genau der jeweils relevante Kontrollgewinn erzeugt werden.

Realistische Betrachtung der eigenen Ressourcen

Für eine ganzheitliche Betrachtung der Steigerung der digitalen Souveränität in der IT fehlt bisher die Analyse der Ressourcenanforderungen für die jeweiligen Hebel. Die Erhöhung der Eigenleistung wäre theoretisch der Schlüssel für fast alle Souveränitätsziele, würde aber, laut der bereits zitierten Studie des Bitkom, zur Autarkie führen. Diese ginge bei realistischer Betrachtung der Investitionskosten, der laufenden Kosten sowie des Bedarfs an qualifiziertem Personal einher mit erheblichen und nicht gewollten Abstrichen an Leistungsfähigkeit.

Die Hebel-/Ziel-Matrix wurde deswegen um eine Ressourcenbetrachtung ergänzt.

Eine zentrale Erkenntnis dieser Analyse lautet: Public Cloud und Eigenleistung verhalten sich entgegengesetzt. Erstere ist besonders günstig bei Investitionen, laufenden Kosten und Personalbedarf, wird in Summe aber bei intensiver Nutzung über die variablen Kosten deutlich teurer. Eigenleistung hingegen benötigt hohe Investitionen und qualifiziertes Personal sowie hohe laufende Kosten, skaliert aber gut bei großen Mengen.

Verschlüsselung ist bei den meisten gewählten Methoden wenig ressourcen-intensiv. Software-Flow benötigt einige Investitionen und insbesondere qualifiziertes Personal, gepaart mit modernem Führungsverständnis. Open-Source ist ebenfalls wenig ressourcen-intensiv. Wenn es zur Abfederung geopolitischer Risiken genutzt werden soll, muss allerdings eigenes, qualifiziertes Personal vorgehalten werden.

Ebenfalls mit wenig Investitionen geht die Kontrolle der Wertschöpfung einher. Wird diese allerdings genutzt, um den Einsatz der Public Cloud zu ermöglichen, ist mit entsprechenden variablen Kosten zu rechnen.

„Ein Streben nach voller Kontrolle gleichzeitig in allen Bereichen bedeutet sehr viel Eigenleistung. Es wären hohe Investitionen und viel IT-Kompetenz, besonders in Führungspositionen, notwendig."

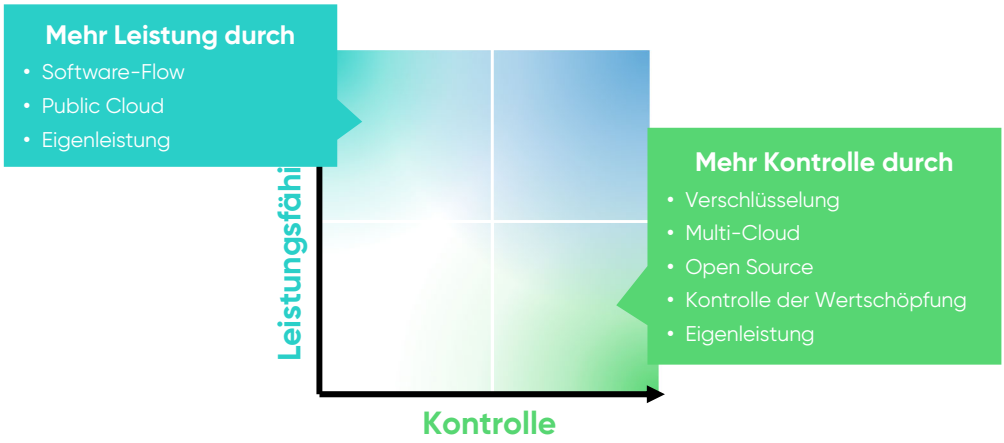
Andreas Tamm
Arvato Systems

3. Welche Maßnahmen empfehlen wir?

Strategische Empfehlungen

Die Bewertung der Hebel bezogen auf die Souveränitätsziele hat ergeben, dass auch öffentlichen Organisationen einige Möglichkeiten zum Ausbau der eigenen digitalen Souveränität offen stehen. Die folgende Grafik nennt die wichtigsten je Zielkategorie.

Eine ausführliche Abwägung von Hebel zu Ziel findet sich unter **www.cloudahead.de.**



cloud ahead spricht fünf strategische Empfehlungen aus:

1. **Verwendung anerkannter Best-Practices der Software-Branche:** Der vorteilhafteste einzelne Hebel für mehr Leistungsfähigkeit ist die Nutzung moderner Software-Methodiken. Beispiele wie DeepL zeigen, dass dies mit wenig Ressourcen-Einsatz möglich ist. Beispiele wie Innus zeigen, dass auch im Bafin-regulierten Umfeld und der Private Cloud eine hohe digitale Leistungsfähigkeit möglich ist.

Das Unternehmen Innus hat dank Software-Best-Practices binnen **2 Jahren mit ~10 Mitarbeitenden** eine Software für Bankprozesse entwickelt. Es läuft in einer **deutschen Private Cloud** und **ist Bafin-Zertifiziert**.[18]

2. **Nutzung der Public Cloud nach pragmatischer Datenkategorisierung:** Die Standard-Services der Hyperscaler AWS, Microsoft und Google sind den meisten der ~50.000 Private Clouds in Deutschland, in den Bereichen Service-Breite, Stabilität, Sicherheit und Einfachheit der Nutzung, überlegen. Wird deren Nutzung – etwa nach dem Vorbild der Niederlande[20] – auch für den öffentlichen Dienst ermöglicht, wird die digitale Leistungsfähigkeit deutlich erhöht. Die Verwendung der nativen Cloud-Verschlüsselungsmethoden erhöht zudem in vielen Fällen die Kontrolle, bezogen auf die Ziele „Physische Sicherheit" sowie „Kriminelle".

Bis zur ersten guten Version seiner Übersetzungs-Software benötigte DeepL lediglich **22 Mitarbeitende** und 800.000€ Investionen.[19]

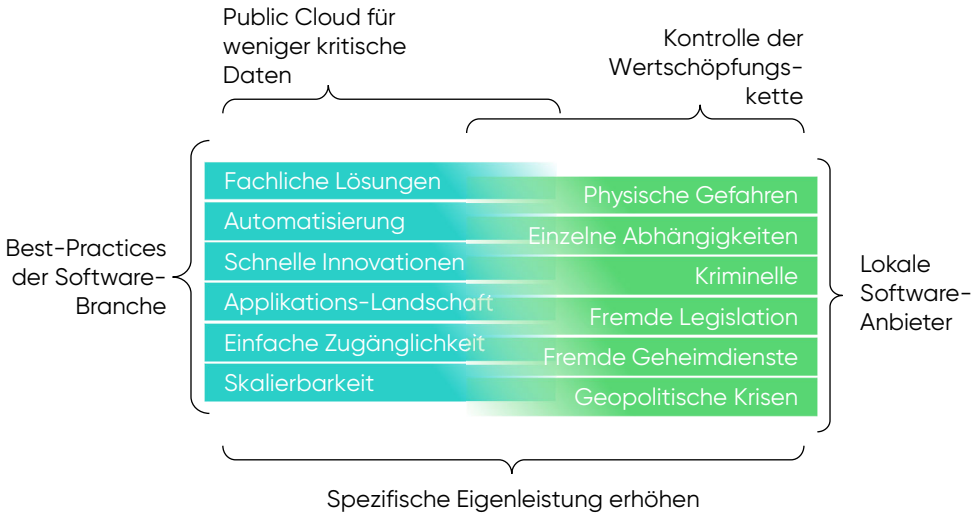
3. **Kontrolle und Regulierung der Software-Wertschöpfung**: Initiativen wie die „roten Linien des BSI“[21] sind der Schlüssel, dem öffentlichen Dienst auch für kritischere Daten die Nutzung der überlegenen US-Technologien zu ermöglichen. Methoden und Tools in der Public Cloud unterscheiden sich deutlich von den Best Practices der meisten klassischen Rechenzentren. Daher sollten Organisationen die Zeit bis souveräne Clouds in der Breite verfügbar sind nutzen, um mit unkritischen Daten und Anwendungen zu üben.

4. **Lokale Software-Anbieter:** Im Grundsatz sind leistungsfähige, lokale Software-Anbieter sowie Open-Source-Softwares die idealen Ansätze zur Auflösung geostrategischer Abhängigkeiten. In der Praxis tritt Unabhängigkeit bei Open-Source lediglich dann ein, wenn regional qualifizierte ExpertInnen zur Pflege und Weiterentwicklung dieser Software zur Verfügung stehen.[22] Zudem leiden viele Open-Source-Lösungen aufgrund des Mangels an Nutzerfreundlichkeit an geringer User-Akzeptanz. Beide Probleme sind lösbar wenn der öffentliche Dienst seine Vergabemacht dazu nutzt, die Wettbewerbsfähigkeit der lokalen Software-Branche auszubauen sowie diese dazu anreizt, die Usability der Anwendungen ständig zu verbessern.

5. **Spezifische Eigenleistung:** Der Auf- und Ausbau eigener Kompetenz in den Bereichen Architektur, Betrieb und externer Steuerung ist eine notwendige Grundlage für praktisch alle genannten Hebel. Für die Weiterentwicklung der internen Organisation sowie für Erstellung und erfolgreiche Umsetzung von Tech-Strategien ist zudem umfassende IT-Kompetenz in führenden Management-Positionen notwendig.

„Die Delos Cloud kombiniert die Leistungsfähigkeit von Azure mit den deutschen Anforderungen an Souveränität in den Bereichen Betrieb, Technologie und Datenverarbeitung.“

Wilfried Bauer
Microsoft



Operative Handlungsempfehlungen

Einige der strategischen Handlungsempfehlungen übersteigen den Handlungsspielraum des einzelnen Akteurs in einer öffentlichen Institution. Welche Möglichkeiten aber stehen dem individuellen IT-Entscheider dennoch offen? In der Praxis bietet sich der Fokus auf den einzelnen Anwendungsfall an.

Der Umstieg von klassischen IT-Umgebungen in die Welt der automatisierten Clouds ist eine Herausforderung insbesondere für die betroffenen ExpertInnen und EntscheiderInnen. In der neuen Welt der IT läuft alles automatisch, alles skaliert, alles wird Code. Sicherheitslücken sind Code, Kriminelle automatisieren ihre Angriffe. Genauso aber wird Kontrolle zu Code: Automatisierte Updates, Compliance-by-design, AI-basierte Identifikation von Angreifern.

Um in der Welt der Cloud den eigenen Weg zu Leistungsfähigkeit und Kontrolle zu finden, ist es für jeden Beteiligten wichtig, diese Welt selbst zu erfahren. Nur anhand dieser persönlicher Erfahrungen können Organisationen ein Gefühl dafür entwickeln, welche Chancen die nächste Stufe der Industrialisierung der IT für sie bietet.

„Der Umstieg in Richtung Cloud-Computing ist für viele Organisationen bereits ein Paradigmenwechsel. Die wirkliche Arbeit liegt aber in der Wahl der richtigen Use Cases, dem Change Management und der nutzer-orientierten Herangehensweise."

Max Hille
Cloudflight

4. Wie kann Souveränität in der Praxis aussehen?

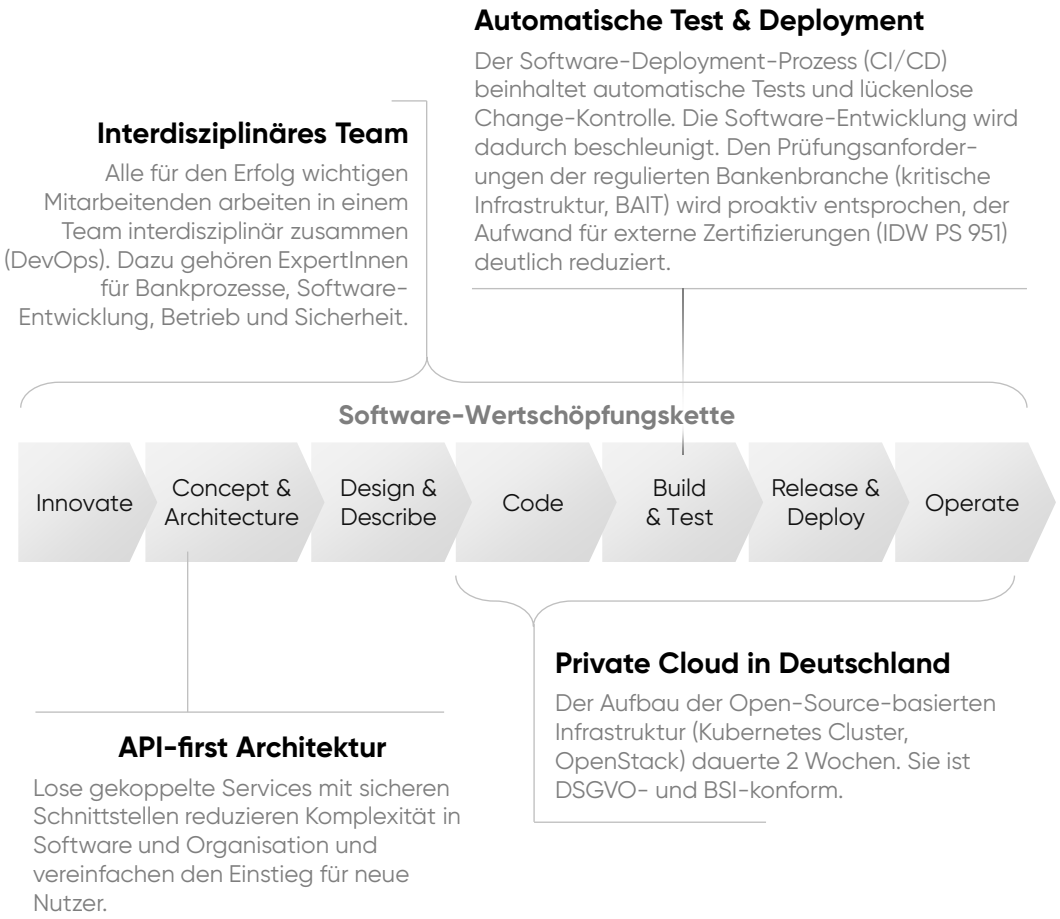
innus – Software-Flow im regulierten Umfeld

innus ist ein deutsches Unternehmen, das Software für Banken entwickelt und in einer deutschen Private Cloud bereitstellt. Gegründet wurde es 2019 mit dem Ziel ein neues, sicheres und schnell zu implementierendes Kern-Bankensystem auf den Markt zu bringen. Mit insgesamt 7 Mitarbeitenden konnte innus nach 2 Jahren Entwicklungszeit den ersten Kunden gewinnen. Die Software bietet umfassende Funktionen für Buchführung, Produktmanagement, Vertrieb, Revision, Risikomanagement und Gesamtbanksteuerung. Sie ist mehrsprachig und mehrmandantenfähig sowie für den Einsatz in Finanzinstituten nach BAIT, BSI und IDW Standards zertifiziert.

„Wir haben unsere Organisation anhand der Software-Best-Practices ausgerichtet. Somit konnten wir Leistungsfähigkeit und Kontrolle gleichermaßen steigern."

Bernd Greitemeier
innus

www.innus.de



innus zeigt, dass auch im regulierten Umfeld und in der Private Cloud ein hohes Maß an Leistungsfähigkeit erreichbar ist. Durch den Einsatz von Open-Source ergibt sich zudem eine sehr hohe Unabhängigkeit von geopolitischen Krisen.

Arvato Systems – Impfmanagement für Gesundheitsbehörden

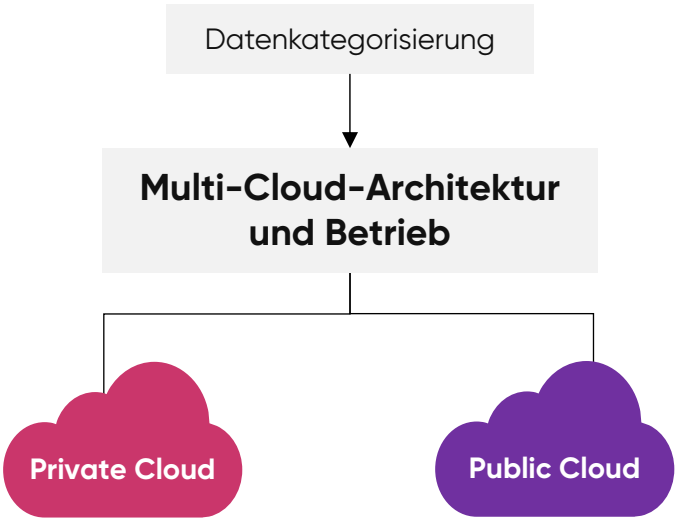
Ende 2021 stand das Gesundheitssystem Deutschlands vor einer großen Aufgabe: Möglichst viele Menschen sollten nach festgelegter Priorität möglichst schnell geimpft werden. Dazu mussten Impfstoffe und deren Logistik gesteuert sowie Impfende und Impflinge koordiniert werden.

Arvato Systems und das Schwester-Unternehmen Majorel hatte bereits für viele der benötigten Teilprozesse Software-Lösungen zur Verfügung stehen.

Mitte November starteten die Partner mit der Kategorisierung der Daten und konzipierten eine entsprechend differenzierte Multi-Cloud-Lösung. Die Plattform war einen Monat später einsatzbereit und konnte weitere zwei Wochen später die erste Impfung erfolgreich abwickeln.

„Dank einer smarten Multi-Cloud-Architektur konnten wir die Vorteile von Public und Private Cloud miteinander kombinieren."

Markus Krenn
Arvato Systems



Dank der erfolgten Datenkategorisierung konnten alle Leistungs- und Kontrollziele gleichermaßen erreicht werden: Die benötigte Infrastruktur wurde schnell und automatisiert bereitgestellt, personenbezogenen Daten wiederum wurden nur in privaten Clouds gespeichert.

Über uns

Unsere Mission

cloud ahead ist ein Gruppe von Enthusiasten, die der Wunsch nach mehr digitaler Selbstbestimmung in Deutschland und Europa eint.

Selbstbestimmt und selbstbewusst zwischen Alternativen leistungsfähiger und vertrauenswürdiger Partner[4] zu handeln, erfordert ein hohes Maß an Wissen aus unterschiedlichen Disziplinen. Dieses Wissen auf einfache Weise und ausgewogen zu kommunizieren, haben wir uns zur Aufgabe gemacht.

Unser Ziel ist es, EntscheiderInnen und ExpertInnen in Unternehmen und Staat die Kompetenz zu vermitteln, Leistungsfähigkeit und Kontrolle in ihrer digitalen Wertschöpfung gleichermaßen zu verbessern.

cloud ahead glaubt an den Open-Source-Ansatz als Schlüssel zur organisationsübergreifenden Zusammenarbeit. Dieser ermöglicht es den ExpertInnen unseres Netzwerks, gemeinsam Inhalte mit großer Perspektivenbreite zu erstellen.

Hintergrund und Nutzung

Das Whitepaper wurde frei von kommerziellen Verpflichtungen erstellt und entspricht dem aktuellen Wissensstand der genannten Kontributoren. Die LeserInnen sind herzlich eingeladen, die Dokumente im Sinne der Stärkung der digitalen Selbstbestimmung Europas zu nutzen und weiterzuentwickeln.

Weitere Infos zu diesem Whitepaper, zusätzliche Inhalte und unsere Kontaktdaten finden sich auf unserer Webseite www.cloudahead.de.

Kontaktieren Sie uns, um mehr über uns oder unsere Ideen zu erfahren. Wir freuen uns auf Ihr Feedback und den Austausch mit Ihnen.

cloud ahead

Quellen

1. IT-Planungsrat 2019: https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf
2. BMWi 2021: https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.pdf?__blob=publicationFile&v=6
3. cloud ahead 2022: https://www.cloudahead.de/2-was-ist-digitale-souveraenitaet
4. Bitkom 2015: https://www.bitkom.org/Themen/Politik-Recht/Digitale-Souveraenitaet/Das-verstehen-wir-unter-Digitaler-Souveraenitaet.html#_
5. Acatech 2021: https://www.acatech.de/publikation/digitale-souveraenitaet-status-quo-und-handlungsfelder/
6. Frag den Staat 2022: https://fragdenstaat.de/anfrage/rote-linien-des-bsi-fuer-cloud-angebote-fuer-die-oeff-verwaltung/
7. CNBC 2018: https://www.cnbc.com/2018/08/01/amazon-plans-to-move-off-oracle-software-by-early-2020.html
8. CNBC 2022: https://www.cnbc.com/2022/10/04/micron-to-spend-up-to-100-billion-to-build-new-york-chip-plant.html
9. Brandriddle: https://brandriddle.com/instagram-success-story/
10. Faz 2022: https://www.faz.net/aktuell/wirtschaft/unternehmen/milliardengeschaeft-pentagon-vergibt-cloud-auftrag-jetzt-an-vier-unternehmen-18520639.html
11. Wikipedia 2023: https://de.wikipedia.org/wiki/MECE-Regel
12. Futurezone 2020: https://www.stern.de/digital/smartphones/trump-stuerzt-huawei-in-sein-groesstes-smartphone-problem-9370336.html
13. cloud ahead 2023: https://www.cloudahead.de/weniger-experten-mehr-feedback
14. cloud ahead 2022: https://www.cloudahead.de/2-warum-ist-die-public-cloud-so-viel-besser
15. cloud ahead 2023: https://www.cloudahead.de/private-oder-public-cloud-was-ist-sicherer
16. cloud ahead 2023: https://www.cloudahead.de/verschluesselung-in-der-public-cloud
17. Bertelsmann 2021: https://www.bertelsmann.de/news-und-media/nachrichten/kampf-gegen-das-corona-virus-mit-hilfe-von-bertelsmann.jsp
18. Scaleuptech 2022: https://www.scaleuptech.com/de/wp-content/uploads/2021/02/innus_gmbh_casestudy.pdf
19. Deutsche Startups 2018: https://www.deutsche-startups.de/2018/07/05/deepl-koelner-uebersetzungskoenig-macht-millionengewinn/
20. Computer weekly 2022: https://www.computerweekly.com/news/252524519/Dutch-government-finally-allowed-to-use-public-cloud
21. cloud ahead 2023: https://www.cloudahead.de/die-roten-linien-des-bsi
22. Sovereign Tech Fund 2022: https://sovereigntechfund.de/SovereignTechFund_Machbarkeitsstudie_en.pdf Seite 10

cloud ahead gmbh

Karl-Schrader-Str. 1
10781 Berlin

info@cloudahead.de
www.cloudahead.de