

Analyse Kleine Anfrage „Digitale Souveränität und Nutzung von Open Source bei Clouds der Bundesverwaltung und der Status der Deutschen Verwaltungscloud-Strategie“

Aw BuReg: 21.03.25, DS: 20/15138

Anke Domscheit-Berg

Stand: 2.4.2025

Kosten für Cloud steigen stark, Budgets konzentrieren sich auf ITZ-Bund und AA

- **Kosten für Cloud im Bund in 3 Jahren verdoppelt:** 2021-2024 von 134 Mio auf 286 Mio (+152 Mio = +113%) (Bezug: Q17, Anlage 5)
- Die **Haushaltsmittel in 2024 waren sogar noch höher**, sie lagen bei über 360 Millionen Euro, wovon allein auf ITZ-Bund (242 Mio) und Auswärtiges Amt (95 Mio) mit insg. mehr als 336 Mio Euro ca. 93% entfielen. Wie die **50 Mio Euro Differenz zwischen HH-Budget und verausgabten Kosten in 2024** zustande kam, bleibt ein Rätsel. Für 2025 stehen 344 Mio zur Verfügung, die wieder vor allem auf ITZ-Bund und AA entfallen.
- Nur das BMI verfügt ebenfalls über ein mind. 6-stelliges Budget: 23 Millionen werden allein für die Sicherheitsbehörden BKA und ZITIS angegeben. 28 Mio standen bzw. stehen dem ZITIS allein in 2024 und 2025 an HH-Mitteln zur Verfügung! (Zu Datenlücken siehe weiter unten)
- Auf **Public Clouds** entfiel in 2024 nur ein sehr kleiner Teil der Haushaltsmittel: 8,4 Mio Euro, also nur etwas über 2 Prozent. (Q15, Anlage 3)

Anteil Open Source: lächerlich klein

- **Homöopatischer Anteil von OSS:** von den 286 Mio Kosten des Bundes für Cloud in 2024 betrug der Anteil **für OSS nicht einmal 2 Prozent**, und diese waren fast ausschließlich Software Entwicklungskosten. Von den 204 Mio **Betriebskosten** entfielen sogar **99,9 % auf proprietäre Dienste** (Cloud-Stack u Anwendungen in der Cloud); (Bezug: Q19, Anlage 6)
- **Bei OSS-Software-Entwicklungen sind ausgerechnet ZITIS und BKA Vorreiter**, beides Sicherheitsbehörden; beim Cloud Stack ist ZITIS sogar die einzige Behörde, die OSS entwickeln ließ, **bei Anwendungen entfallen 81% der OSS Ausgaben auf ZITIS und BKA** – ein Beleg dafür, dass das Argument „Open Source ist nicht sicher“ Unfug ist. (Bezug: Q19, Anlage 6)
- Die **Ziele des IT-Planungsrates** (Beschluss 2023/50) „Die Mechanismen der Dt. Verwaltungscloud fördern gezielt OS-Lösungen“ und „OSS wird für den Aufbau der dt. Verwaltungscloud priorisiert“ **werden offensichtlich ignoriert** und mit „unterschiedlichsten Anforderungen“ begründet – eine fadenscheinige Ausrede. Dies ist ein weiteres Beispiel dafür, dass **Ziele, deren Einhaltung niemand misst und überprüft** und die niemanden mit Entscheidungsbefugnis zu interessieren scheinen, **regelmäßig weit verfehlt** werden: you get what you measure!
- Das vom BMWK geförderte **Projekt „Sovereign Cloud Stack“** wurde (leider) beendet, die Förderung der Weiterentwicklung ist nicht geplant. Das ist bedauerlich und widerspricht früheren Plänen der Bundesregierung, denn der Sovereign Cloud Stack sollte zu einer OSS-Cloud für Wirtschaft und Verwaltung beitragen. Wünschenswert wäre eine Beauftragung des ZenDiS, um dieses Vorhaben weiterzuführen. (Q25)
- Die Existenz spezifischer **Hürden bei der Beschaffung von OSS** verneint die Bundesregierung und redet sich damit heraus, dass es ja erst einmal OSS Dienste am Markt geben müsse und Unternehmen, die diese pflegen und betreiben könnten. Damit ignoriert sie die vielfältigen Angebote am Markt, aber auch z.B. bestehende Defizite in Vergabestellen hinsichtlich der „Einkaufskompetenz“ für Open Source Produkte, ungeeignete WIBEn und andere Hürden. **Wer Probleme leugnet, kann sie nicht lösen.** Die Hoffnung der Bundesregierung, dass eine „soll“ Vorschrift im eGovernment Gesetz zu mehr Open Source Beschaffung führen wird, ist naiv. Deshalb hoffe ich, dass sich die SPD in den **Koalitionsverhandlungen** mit ihrem Wunsch nach einem **50% Open Source Anteil bis 2029** als Zielmarke durchsetzt. (Q28)

Ja, nur öffentlicher Code ist Open Source, aber die BuReg widerspricht sich selbst

- Erfreulich: die Bundesregierung teilt die Definition der Open Source Initiative, wonach **nur veröffentlichter Source Code auch als Open Source bezeichnet** werden kann (Q30). Sie **widerspricht sich damit aber selbst**, da sie mir in mehreren Anfragen, zuletzt in einer Kleinen Anfrage zu ZenDiS und Open Source vor wenigen Tagen (DS 20/15064) unterschiedliche Antworten auf die Frage nach der Anzahl als OSS beauftragter Software-Entwicklungen und Anzahl OSS-Software-Entwicklungen mit veröffentlichtem Source Code nannte. In der genannten Anfrage wurden 20% der 968 Fälle von Software Entwicklungen als Open Source bezeichnet, obwohl nur 7,6% auch veröffentlicht waren. Es besteht offensichtlich Aufklärungs- und Weiterbildungsbedarf zu Open Source Software im Bund. In Konsequenz ihrer klaren Aussage sollte die Bundesregierung den **Code sämtlicher 20 % entwickelter Open Source Software der abgelaufenen Legislatur zeitnah veröffentlichen – am besten auf OpenCoDe**.

Datenqualität: ungenügend, Blackbox Militär, Geheimdienste, Sicherheitsbehörden

- **Für ein dringend nötiges Lagebild „Digitale Souveränität“ braucht der Bund eine bessere Datenlage**, denn offensichtlich sind auch die vorliegenden Daten unvollständig. Noch in der KA zu Nachhaltigkeit gab die Bundesregierung für das BMI 20 Rechenzentren für Nov. 2024 an, bei Betriebskosten für Cloud gibt es jedoch keine einzige Angabe für das BMI, das ist schlicht unplausibel, denn irgendwo muss der Cloud Stack u die entwickelten Anwendungen ja auch betrieben werden und sicher nicht für lau. (Bezug Q19, Anlage 6)
- Dazu kommt eine **große Blackbox**. Für den Geschäftsbereich des **BMVg wird ohne Angabe von Gründen keine Zahl zu den Kosten und Haushaltsbudgets genannt** (Anlagen 3, 4 und 5), Angaben zu **Nachrichtendienste** werden aus Gründen der Sicherheit **verweigert**, Angaben zu **ZITIS**, der „Hacker-Behörde“ des BMI sind unplausibel, da sie **unlogische Lücken** aufweisen. Bei den realen Kosten für Cloud von 2021 bis 2024 steht beim ZITIS nur für 2021 eine Zahl: knapp 9 Mio Euro (Q17, Anlage 5). In 2024 gab es laut Anlage 3 für ZITIS 15 Mio Euro im Haushalt für Clouds – und davon soll kein einziger Euro ausgegeben worden sein? Auch in 2025 verfügt das ZITIS über 13 Mio Euro für Clouds (Q16, Anlage 4). Dennoch soll es keinerlei Ausgaben von ZITIS für Clouds in 2022, 2023 und 2024 gegeben haben? Das Grundgesetz verpflichtet die Bundesregierung zu vollständigen Antworten auf parlamentarische Anfragen, dieses Recht verletzt die Bundesregierung regelmäßig.

Cloud Service Portal der Deutschen Verwaltungscloud: langsamer Start, Priorisierung erforderlich

- Stand März 2025 gibt es **von 11 Cloud Anbietern insg. 40 Dienstleistungen** auf dem CSP, darunter Dienste für Hundesteuer, Hundemarken und Hundeverwaltung, aber auch zB der OSS Videokonferenzdienst BigBlueButton und ein Chatbot für Kommunen und Landkreise.
- Auf einer **Prüfungsliste mit unklarem Ausgang** und unklarem Zeithorizont finden sich weitere 78 Anwendungen, darunter auch wichtige Dienste für die Stärkung der digitalen Souveränität, wie der **Bundemessenger, die OZG Cloud, der Zugang zum VS-NfD fähigen Netz des Bundes und der OSS-Arbeitsplatz OpenDesk**, dessen breiter Roll-Out im Bund schon für 2025 geplant war. (Bezug: Frage 8, Anlage 1)
- Die neue Bundesregierung muss dringend einen **strategischen Plan zur Stärkung der Digitalen Souveränität** auf der Basis eines Lagebildes entwickeln und **Prioritäten festlegen**. Dienste, die für eine stärkere Unabhängigkeit elementar sind, wie z.B. OpenDesk, müssen auch bei der Bereitstellung im CSP Vorfahrt bekommen, um den Roll-Out zu beschleunigen.
- Dennoch ist **OpenDesk in der Cloud schon verfügbar**, allerdings nicht über öffentliche IT-Dienstleister, aber wenigstens über wirklich souveräne Clouds der privaten Anbieter STACKIT GmbH und IONOS SE. (Q11b)
- Das ITZ-Bund ist nicht mit eigenen Angeboten am CSP beteiligt (siehe Anlage 1). Laut Medienberichten, die das BMI zitieren (Behördenspiegel Beitrag vom 27.03.2025

<https://www.behörden-spiegel.de/2025/03/27/deutsche-verwaltungscloud-startet/>) gibt es dafür rechtliche Hürden.

Unkoordinierte Architekturplanung, unsichere, nicht cloudfähige Netze des Bundes

- Die NdB erfüllen die Voraussetzungen der Dt. Verwaltungscloud nicht (Q9). Sie sind unsicher (Q 9a, b) und ihre Kapazitäten erschöpft (Q9d). Für das notwendige Peering Netzwerk der Dt. Verwaltungscloud existiert bisher aber nur ein Grobkonzept. Von Anfang an mitgedacht wurde es bei der Neukonzeption der NdB aber offenbar nicht, denn die NdB sollen durch den im Aufbau befindlichen Informationsverbund der Verwaltung (IVÖV) ersetzt werden. Leider räumte der Bund nun ein, dass unklar sei, ob das Grobkonzept für das Peering Netzwerk der DVC überhaupt damit kompatibel sein wird (Q9). Was, wenn nicht? **Zwei wesentliche Architekturziele: der Weg in die Cloud und der Ersatz der Netze des Bundes - werden offenbar parallel, statt in engem Zusammenhang geplant**, ein strategischer Fehler, wie er typisch für den Bund ist und einer der Gründe, warum die Digitalisierung der Bundesverwaltung häufig in der Umsetzung scheitert.
- Die **Sicherheit der Netze des Bundes** wurde erst Ende 2024 vom BuReHof scharf kritisiert, da von 106 Bundesbehörden, die die NdB nutzten, fast jede zweite (52) die Sicherheitsvoraussetzungen dafür gar nicht erfüllte und eine schon 2022 bereitgestellte Lösung zur Erhöhung der Sicherheit von 45 dieser Behörden nicht genutzt wurde. Erst im Sommer soll diese Lösung nach und nach zentral bereitgestellt werden mit der Hoffnung, das würde dieses Problem lösen, ich habe da noch Zweifel.

Rein in die Cloud oder nicht? Entscheidungen ohne einheitliche Entscheidungskriterien

- Die Nutzung von Clouds ist mit zusätzlichen Risiken verbunden, sie hat Vor- und Nachteile, was davon überwiegt, hängt vom Einzelfall ab. Für die Bewertung **müsste es daher Leitlinien geben**, um auf Basis eines **verbindlichen, einheitlichen Kriterienkataloges** ergebnisoffen für jeden Einzelfall zu untersuchen, ob es sinnvoll ist, bestimmte Daten oder Prozesse in die Cloud zu verlagern. Obwohl solche Leitlinien für die Einhaltung hoher Sicherheitsstandards und zur Vermeidung teurer und riskanter Fehlentscheidungen wertvoll sein können, **gibt es keine**. Vor 10 Jahren festgelegte „Allgemeine Grundsätze“ zur Verwendung von Cloud-Diensten der Wirtschaft des IT-Planungsrates sollen dafür ausreichen, als hätte es im letzten Jahrzehnt nicht erhebliche Entwicklungen gegeben.

(Auch) Ressourcen- und Fachkräftemangel beim ITZ-Bund zwingt zu Multi-Cloud Ansatz

- Mit vielen und verschiedenen Anforderungen, aber auch mit internem Ressourcenmangel begründet die Regierung, dass die eigentliche Zielstellung des ITZ-Bund, „die **Bundescloud** zur zentralen Plattform für alle Dienste auszubauen“ einer Multi-Cloud-Strategie gewichen ist. (Q12)
- Während die Bundescloud des ITZ-Bund abgeschlossen ist, soll eine zusätzliche föderierte Cloud als Deutsche Verwaltungscloud interoperable Cloud-Dienste zwischen Bund und Ländern ermöglichen und so Ressourcen effizienter nutzen und dem Fachkräftemangel begegnen. (Q14)

Wie souverän sind Cloud-Angebote auf dem Markt? It's complicated!

- Der Bund misst die digitale Souveränität jeweils an den 3 Kriterien **Wechselfähigkeit, Gestaltungsfähigkeit** und **Einfluss auf den IT-Anbieter**. Wechselfähigkeit und Gestaltungsfähigkeit könne man nicht je nach Cloud-Anbieter beurteilen, obwohl eingeräumt wird, dass mitunter eine **tiefe Integration in das Cloud-Ökosystem eines Anbieters** die Wechselfähigkeit beeinflusst – Office365 und dessen Zusammenhang mit Microsoft Azure Cloud werden zwar nicht genannt, sind aber sicher gemeint. (Q24)
- **Nur beim Einfluss auf den Anbieter differenziert die Bundesregierung**, und bewertet nach Sitz in Deutschland, Beteiligung des Bundes am Unternehmen und Anteil am Gesamtumsatz bei Beauftragung durch den Bund. Für den Bund ist dabei egal, ob ein US Hyperscaler sein deutsches

Tochterunternehmen für den Vertrieb nutzt, oder ob es sich um ein insgesamt deutsches Unternehmen handelt – diese Gleichsetzung sollte spätestens nach den jüngsten Erfahrungen mit der Trump-Regierung und der US-Tech-Industrie beendet werden.

- Beim Einfluss durch Umsatzanteil bewertet der Bund die **IONOS** genauso wie Amazon, obwohl ein bestehender Rahmenvertrag des Bundes bei IONOS etwa 1,3 % des Jahresumsatzes entspräche, die gleiche Summe bei Amazon aber nur 0,014%. Das Deutsche Unternehmen IONOS wird vom Bund in seiner Antwort nicht nur mit Amazon und Oracle auf eine Souveränitäts-Stufe gestellt, sondern auch mit der DELOS Cloud, die auf Microsoft Azure basiert. (Q24)
- Die Prüfung der **DELOS** Cloud soll erst Ende 2026 abgeschlossen sein und dann auch Anforderungen des Bundes an von Dritten betriebene private Clouds beschrieben werden.(Q35a).

Sicherheitsmaßnahmen von Microsoft nach Kompromittierung der MSFT Cloud Infrastruktur und dem Bericht des Cyber Safety Review Boards sollen in die Prüfung der DELOS Cloud einfließen. (Q35b)
Die Bundesregierung teilt die kritische Bewertung des BSI auch zu anderen **Sicherheitsmängeln bei der Microsoft Cloud** und zur notwendigen Umsetzung empfohlener Maßnahmen. (Q36).

Hyperscaler Clouds ohne Ende zu Ende Verschlüsselung

- Auch wenn die Antworten der Bundesregierung unvollständig ausfallen, geht aus ihnen hervor, dass häufig die **Verschlüsselung von in diesen Clouds gespeicherten Daten unbekannt** ist oder dass man weiß, dass sie **nicht stattfindet**. Die häufigste Antwort auf die Frage nach **Verschlüsselung der Daten bei ihrer Verarbeitung in der Cloud** war „teilweise“. Die meisten Angaben bezogen sich auf AWS Cloud-Dienste.(Q42, Anlage 8)
- **(mindestens) 32 Cloud Dienste von Google, Amazon, Microsoft und Oracle** werden vom Bund genutzt, aber **nur bei einem einzigen** (AWS-Software VAULT Storage) genutzt von der Bundespolizei, stellt eine Ende zu Ende Verschlüsselung sicher, dass eine **Entschlüsselung von Meta- und Nutzerdaten ausschließlich auf den Endgeräten der Nutzenden möglich** ist – bei einer einzigen! Da Bundesbehörden nicht immer, aber doch oft mit sensiblen Daten zu tun haben, und die Vertrauenswürdigkeit von US-Hyperscalern unter einer Trump-Administration gelitten hat, ist diese Tatsache **höchst beunruhigend!**