Bundescloud Realität Check: Zwischen Anspruch und Praxis

Category: Opinion
geschrieben von Tobias Hager | 23. Januar 2026



Bundescloud Realität Check: Zwischen Anspruch und Praxis

Die Bundescloud klingt wie das digitale Versprechen der Republik: sicher, souverän, leistungsfähig – und endlich Schluss mit Datenchaos im föderalen Flickenteppich. Doch wer genauer hinschaut, sieht vor allem politische Claims, technische Altlasten und eine Bürokratie, die Cloud-Innovation eher ausbremst als entfesselt. Willkommen beim großen Bundescloud Realität Check: Wir zerlegen Hype, Mythen und Missverständnisse. Und liefern dir die schonungslose Analyse, warum die Bundescloud 2025 immer noch mehr Schlagwort als Schaltzentrale ist.

- Was die Bundescloud wirklich ist – und warum sie sich von klassischen Public-Cloud-Angeboten unterscheidet
- Die wichtigsten technischen, organisatorischen und politischen Anforderungen an die Bundescloud
- Wo Anspruch und Realität auseinanderklaffen: Von Datenhoheit bis Vendor-Lock-in
- Welche Cloud-Technologien, Architekturen und Sicherheitsstandards (nicht) umgesetzt sind
- Weshalb Bürokratie, Vergaberecht und Föderalismus echte Cloud-Innovation verhindern
- Wie Behörden, IT-Dienstleister und Politik die Bundescloud praktisch nutzen (oder eben nicht)
- Step-by-Step: Was für eine wirklich souveräne, performante Bundescloud nötig wäre
- Warum der deutsche Sonderweg im Cloud Computing internationale Wettbewerbsfähigkeit gefährdet
- Fazit: Zwischen digitalem Anspruch und Realität – und was wirklich passieren müsste, damit die Bundescloud kein Rohrkrepierer bleibt

Wer „Bundescloud“ hört, denkt an Hochsicherheit, Datenhoheit und einen deutschen Gegenentwurf zu AWS, Azure & Co – made by Verwaltung, für Verwaltung. Die Marketingfolien der Bundes-IT zeichnen das Bild einer souveränen, hochverfügbaren Infrastruktur, die Behörden endlich ins Cloud-Zeitalter katapultiert. Doch die Praxis sieht anders aus: Legacy-Systeme, Insellösungen, föderale Streitigkeiten und eine politische Angst vor echter Digitalisierung. Während andere Länder längst “Cloud first” leben, kämpft Deutschland weiter mit halbgaren Hybridansätzen, und jede technische Entscheidung wird zum politischen Minenfeld. Zeit für eine ehrliche Bestandsaufnahme.

Was ist die Bundescloud eigentlich? Definition, Zielsetzung und Abgrenzung zu Public Cloud

Die Bundescloud ist nicht einfach ein weiterer IaaS- oder PaaS-Anbieter, sondern eine speziell für den Bund und seine Behörden konzipierte Cloud-Infrastruktur. Ihr Anspruch: höchste Sicherheitsstandards, vollständige Datenhoheit und Unabhängigkeit von ausländischen Hyperscalern. Im Unterschied zu Public-Cloud-Angeboten wie AWS, Azure oder Google Cloud liegt die Bundescloud technisch und organisatorisch komplett in staatlicher Hand – betrieben durch zentrale IT-Dienstleister des Bundes, insbesondere die Bundesdruckerei und die ITZBund.

Technisch basiert die Bundescloud auf klassischen Cloud-Prinzipien: Virtualisierung, Self-Service, Multi-Tenancy, flexible Skalierung und

automatisierte Bereitstellung von Ressourcen (Compute, Storage, Network). Doch während Hyperscaler auf proprietäre Plattformen und APIs setzen, nutzt die Bundescloud bevorzugt Open-Source-Komponenten (wie OpenStack oder Kubernetes), um Vendor-Lock-in zu vermeiden. Die Bundescloud soll Behörden ermöglichen, Anwendungen und Daten flexibel, sicher und skalierbar bereitzustellen – von der einfachen VM bis zu komplexen Microservices-Architekturen.

Die Abgrenzung zur Public Cloud ist nicht nur eine Frage des Standorts (deutsche Rechenzentren, deutsche Betreiber), sondern vor allem der Kontrolle. Während ein AWS-Service nach US-Cloud-Act potentiell dem Zugriff ausländischer Behörden unterliegt, soll die Bundescloud volle Souveränität garantieren. Im Idealfall können deutsche Behörden so sensible Dienste und Daten in einer Umgebung betreiben, die keine externen Abhängigkeiten kennt.

Doch genau hier beginnt das Problem: Die Bundescloud bleibt in der Praxis oft ein Kompromiss zwischen Security-Hardliner, föderalen Befindlichkeiten und technischer Realität. Und das hat massive Folgen für Architektur, Usability und Innovationsfähigkeit.

Technische, organisatorische und politische Anforderungen: Anspruch und Realität der Bundescloud

Die Bundescloud steht unter ständigem Erwartungsdruck. Der politische Anspruch: maximale IT-Sicherheit, höchste Compliance, absolute Datenhoheit und gleichzeitig flexible, moderne Cloud-Services. Die Realität? Ein Spagat zwischen BSI-Minimumstandards, föderalem Kompetenzgerangel und einer IT, die oft noch im Zeitalter von On-Premises und Windows Server 2008 lebt.

Die technischen Kernanforderungen sind hoch: Zertifizierte Rechenzentren (mindestens BSI C5 oder ISO 27001), Zero-Trust-Architekturen, Multi-Faktor-Authentifizierung, Verschlüsselung auf allen Ebenen, sowie die vollständige Trennung von Mandanten (Multi-Tenancy). Hinzu kommen strikte Vorgaben zur Protokollierung, Auditierung und Absicherung der Cloud-APIs. Kein Wunder, dass viele zentrale Bundesbehörden lieber noch ein paar Jahre ihre Alt-Systeme weiterbetreiben, statt auf die Bundescloud zu migrieren.

Organisatorisch bedeutet Cloud für die Verwaltung: Rollenkonzepte, Rechte- und Identitätsmanagement, Self-Service-Portale, automatisierte Bereitstellung (Infrastructure as Code) und ein zentrales Monitoring. Doch hier dominiert oft die Angst vor Kontrollverlust: Jede Automatisierung wird im Zweifel von vier Stellen gegengezeichnet, jede neue API als potenzielles Sicherheitsrisiko betrachtet. Die Folge: Prozesse, die so träge sind wie das Vergaberecht selbst.

Politisch ist die Bundescloud ein Minenfeld. Jeder Bundesminister will “seine” Cloud, jede Fachanwendung hat Sonderlocken, und die föderale Struktur produziert Insellösungen am Fließband. Statt eines echten, konsolidierten Cloud-Stacks gibt es ein Sammelsurium aus Pilotprojekten, Testumgebungen und inkompatiblen Plattformen. Wer von der Bundescloud als einheitlicher, skalierbarer Infrastruktur spricht, hat das föderale IT-Chaos noch nie aus der Nähe gesehen.

Herausforderungen der Bundescloud: Technik, Sicherheit, Vendor-Lock-in und Souveränität

Der größte Unterschied zwischen Bundescloud-PR und Realität zeigt sich in den technischen Details. Während “Datenhoheit” als Buzzword auf jedem Whitepaper steht, sieht die Praxis so aus:

- Legacy-Altlasten: 70 % der behördlichen Anwendungen laufen noch immer auf nicht-cloudfähiger, monolithischer Infrastruktur. Eine Migration ist oft unmöglich, weil Schnittstellen fehlen oder die Systeme schlichtweg veraltet sind.
- Fehlende Cloud-Native-Architektur: Kubernetes und Microservices sind auf dem Papier Standard – in der Praxis aber werden klassische VMs geklont und als “Cloud” verkauft. Von echter Container-Orchestrierung, Service Discovery oder automatisiertem Scaling ist wenig zu sehen.
- Sicherheitsparanoia: Das BSI diktiert Standards, die kaum ein Hyperscaler je erfüllen würde. Jede Schnittstelle wird zum Risiko, jeder API-Call zum Prüfstein. Gleichzeitig gibt es immer noch Behörden, die Passwörter in Excel-Tabellen speichern – die Schizophrenie ist komplett.
- Vendor-Lock-in durch Open Source? Ironischerweise schafft auch der Fokus auf Open-Source-Komponenten wie OpenStack, Ceph oder Kubernetes neue Abhängigkeiten – denn die Wartung liegt bei wenigen Dienstleistern, und Customizing verhindert Upgrades und echte Interoperabilität.
- Fehlende Skalierbarkeit und Verfügbarkeit: Während AWS und Azure mit globalen Regionen und Multi-AZ-Setups glänzen, kämpft die Bundescloud mit Kapazitätsengpässen, Wartungsfenstern und Ausfällen. Hochverfügbarkeit ist oft eher Hoffnung als SLA.

Das Resultat: Die Bundescloud bleibt ein Sammelbecken aus Sicherheitskompromissen, technischen Altlasten und halbgaren Eigenentwicklungen. Wer hier skalierbare, hochverfügbare Cloud-Infrastruktur nach Hyperscaler-Maßstäben erwartet, erlebt eine bittere Enttäuschung. Von echter Souveränität ist man so weit entfernt wie die Verwaltung vom agilen DevOps-Mindset.

Die Cloud-Architektur der Bundesverwaltung: Was läuft, was nicht – und warum?

Ein Blick in die Bundescloud-Architektur zeigt: Vieles ist Stückwerk. Die Basis bildet meist OpenStack, ergänzt um Ceph für Storage, Kubernetes für Container-Orchestrierung und diverse Eigenentwicklungen für Identity- und Access-Management. Doch was auf dem Papier nach Cloud-Native klingt, ist in der Praxis oft das Gegenteil: Umständliche Self-Service-Portale, nicht dokumentierte APIs, und eine Fragmentierung, die jeden DevOps-Fan in den Wahnsinn treibt.

Die häufigsten technischen Schwachstellen im Überblick:

- Komplexe, unübersichtliche Netzwerktopologien, die jede Automatisierung torpedieren
- Fehlende Integration zwischen Identity Management, Monitoring und Cloud-Ressourcen
- Limitierte Auswahl an Services: keine echten Managed Databases, keine KI-Services, keine Serverless-Optionen
- Undurchsichtige Ressourcenzuteilung, die Skalierung praktisch unmöglich macht
- Unklare SLAs, keine automatische Fehlerbehandlung – und Wartungsfenster zu Bürozeiten

Hinzu kommt: Behörden müssen jedes Feature einzeln beantragen, genehmigen und durch interne Gremien schleusen. Neue Technologien wie Infrastructure as Code oder Continuous Delivery werden zwar pilotiert, enden aber oft im Pilotstatus. Innovationen verpuffen im Nebel aus Abstimmungen, Datenschutz-Audits und politischen Befindlichkeiten.

Das Ergebnis: Die Bundescloud ist technisch ein Flickenteppich, operativ ein Bremsklotz, und strategisch Lichtjahre entfernt von echter Cloud-Souveränität. Wer ernsthaft digitale Innovation will, muss hier mehr als nur ein paar OpenStack-Instanzen hochziehen.

Step-by-Step: Was braucht die Bundescloud für echte digitale Souveränität?

Jammern bringt nichts. Wer die Bundescloud wirklich in Richtung Souveränität, Performance und Zukunftsfähigkeit bringen will, braucht einen radikalen Neustart – technisch, organisatorisch und politisch. Die folgenden Schritte sind kein Wunschdenken, sondern Mindestanforderung für eine funktionierende,

wettbewerbsfähige Cloud-Infrastruktur:

1. Raus aus Legacy, rein in Cloud-Native:
   Massiver Umbau der Anwendungslandschaft, konsequente Migration auf Microservices, Container und APIs. Keine neuen VMs oder Monolithen mehr – alles, was nicht cloudfähig ist, wird abgelöst oder refaktoriert.
2. Automatisierung und Self-Service by Default:
   Self-Service-Portale, Automated Provisioning und Infrastructure as Code müssen Standard werden – inklusive klarer Rollenkonzepte, Rechte- und Identitätsmanagement.
3. Sicherheitsarchitektur modernisieren:
   Zero-Trust-Modelle und vollständige Verschlüsselung auf Transport- und Applikationsebene. MFA und rollenbasiertes Access Management als Pflicht, nicht als Option.
4. Integration und Interoperabilität:
   Verbindliche APIs, konsolidierte Schnittstellen und einheitliche Monitoring-Lösungen. Schluss mit Insellösungen und Eigenentwicklungen, die nicht miteinander sprechen.
5. SLAs und Betriebsmodelle nach Hyperscaler-Standard:
   Hochverfügbarkeit, Disaster Recovery, automatische Skalierung und echte Multi-AZ-Setups. Wartung darf nicht mehr Hauptarbeitszeit blockieren.
6. Föderale Kooperation statt Kompetenzgerangel:
   Zentrale Governance, klare Zuständigkeiten und gemeinsame Standards. Keine 16 Bundesländer-Clouds, sondern eine konsolidierte, skalierbare Infrastruktur.
7. Kontinuierliches Monitoring und Auditing:
   Permanente Überwachung aller Systeme, automatisierte Sicherheitsprüfungen und regelmäßige Penetrationstests. Compliance darf kein Bremsklotz sein, sondern muss in die Prozesse integriert werden.

Ohne diese Mindeststandards bleibt die Bundescloud ein teures Digitalexperiment, das weder Souveränität noch Innovation liefert. Die Alternative? Weiterhin digitale Steinzeit – und ein kompletter Kontrollverlust über die eigene IT.

Bundescloud und internationale Cloud-Standards: Der deutsche Sonderweg als Innovationsbremse

Deutschland liebt den Sonderweg – auch und gerade in der Cloud. Während internationale Unternehmen längst auf Multi-Cloud- und Hybrid-Cloud-Architekturen setzen, will die Bundesverwaltung maximale Kontrolle, minimale Flexibilität und ein Regelwerk, das jeder Innovation im Keim erstickt. Die Folge: Während andere Länder KI-basierte Dienste, Serverless Computing und Big Data Analytics “as a Service” beziehen, diskutiert Deutschland noch über

Storage-Limits und Netzwerkzonen.

Die größten Risiken des deutschen Cloud-Sonderwegs:

- Verpasste Anschlussfähigkeit an internationale Standards, APIs und Tools
- Keine Innovationszyklen – neue Features brauchen Jahre, bis sie implementiert werden
- Abhängigkeit von wenigen spezialisierten Dienstleistern, die das Open-Source-Ökosystem der Bundescloud dominieren
- Risiko der digitalen Abschottung: Behörden-Anwendungen werden inkompatibel zum Rest der Welt
- Wettbewerbsnachteile für deutsche Unternehmen, die auf Bundescloud-Standards setzen müssen

Der Traum von der souveränen Bundescloud wird so zur Innovationsbremse. Wer echte Cloud-Kompetenz, Geschwindigkeit und Skalierbarkeit will, muss sich an internationalen Best Practices orientieren – nicht an föderalem Kompetenzgerangel.

Fazit: Die Bundescloud zwischen Anspruch und Realität – und was jetzt passieren muss

Die Bundescloud bleibt 2025 ein politischer Placebo: ein teures Digitalprojekt, das seinen eigenen Ansprüchen kaum gerecht wird. Technisch ist sie ein Sammelsurium aus Legacy, Open-Source-Komponenten und halbgaren Eigenentwicklungen. Organisatorisch dominiert die Angst vor Kontrollverlust, und politisch verhindert der Föderalismus einen echten Innovationsschub. Von der “Cloud made in Germany” bleibt oft nur ein Marketingversprechen übrig.

Wer wirklich digitale Souveränität will, braucht Mut zur radikalen Neuaufstellung: technisch, organisatorisch und politisch. Cloud-Transformation ist kein Compliance-Projekt, sondern ein strategischer Wettbewerbsvorteil. Solange die Bundescloud zwischen Anspruch und Realität pendelt, bleibt Deutschland digital abgehängt. Wer das ändern will, muss aufhören, über Sicherheit zu reden – und anfangen, Cloud-Architektur und Governance endlich ernst zu nehmen. Alles andere ist Zeitverschwendung. Willkommen in der digitalen Wirklichkeit. Willkommen bei 404.