jambit

Souveräne Cloud-Transformation

für Energieversorger und Netzbetreiber

Wie Stadtwerke, EVU und energienahe Infrastrukturunternehmen digitale Modernisierung, regulatorische Sicherheit und operative Kontrolle verbinden

EXECUTIVE SUMMARY

Energieversorger, Netzbetreiber und insbesondere Stadtwerke stehen vor einer neuen Phase der digitalen Transformation. Die Energiewende verändert nicht nur Erzeugung und Verbrauch, sondern auch die Anforderungen an Daten, Plattformen, Betrieb, Sicherheit und Steuerungsfähigkeit. Dezentrale Erzeugung, Smart Meter, Prosumer-Modelle, Wärmepumpen, Ladeinfrastruktur, volatile Märkte und steigende Kundenerwartungen erzeugen eine Systemkomplexität, die mit gewachsenen IT-Landschaften immer schwerer beherrschbar wird.

Gleichzeitig steigt der Druck auf die Organisationen selbst. Fachkräfte werden knapper, regulatorische Anforderungen nehmen zu, Cyberrisiken wachsen und klassische Geschäftsmodelle geraten unter wirtschaftlichen Druck. Energieversorger müssen neue digitale Services entwickeln, Daten besser nutzen, Prozesse automatisieren und kritische Systeme resilient betreiben – ohne Versorgungskontinuität, Compliance oder operative Kontrolle zu gefährden.

Cloud-Technologie kann dafür ein wichtiger Hebel sein. Doch die entscheidende Frage lautet nicht: **Welche Cloud nutzen wir?** Die entscheidende Frage lautet: **Welche digitale Grundlage brauchen wir, um Modernisierung, Daten, AI, Security und neue Services kontrolliert skalieren zu können?**

> ***Genau hier beginnt digitale Souveränität. Sie entsteht nicht allein durch Datenresidenz oder durch die Wahl eines bestimmten Infrastrukturmodells. Souveränität entsteht durch kontrollierbare Architektur, klare Verantwortlichkeiten, nachvollziehbare Datenflüsse, Zugriffskontrolle, Security-by-Design, Auditierbarkeit, Betriebsfähigkeit, Kostensteuerung und organisatorische Steuerbarkeit.***

Dieses Whitepaper zeigt, wie Energieversorgungsunternehmen, Netzbetreiber und Stadtwerke souveräne Cloud-Transformation strukturiert angehen können. Es beschreibt typische Fehlmuster punktueller Modernisierung, definiert digitale Souveränität als Architektur- und Governance-Frage und zeigt anhand ausgewählter Use Cases, wo moderne Plattform-, Daten- und Security-Architekturen konkret Wirkung erzeugen: Smart Meter und Datenplattformen, dezentrale Energieressourcen, IT-/OT-Security, Anwendungsmodernisierung und AI-gestützter Kundenservice.

AWS European Sovereign Cloud wird dabei als mögliche Infrastruktur-Option eingeordnet – insbesondere für Organisationen mit hohen Anforderungen an Datenresidenz, betriebliche Autonomie und europäische Governance. Sie ersetzt jedoch keine Strategie, keine Zielarchitektur und kein Betriebsmodell. Entscheidend bleibt, wie Cloud-, Daten-, Security- und Plattformentscheidungen in eine tragfähige Umsetzungslogik übersetzt werden.

jambit unterstützt EVU, Netzbetreiber und energienahe Infrastrukturunternehmen an genau dieser Schnittstelle: von der strategischen Einordnung über Zielarchitektur, Daten- und Plattformkonzepte, Security-by-Design und Use-Case-Priorisierung bis zur technischen Umsetzung und Betriebsfähigkeit.

Die zentrale Botschaft:
Entscheider*innen in der Energiewirtschaft müssen digitale Modernisierung nicht gegen Kontrolle, Sicherheit oder Souveränität ausspielen. Entscheidend ist eine Architektur- und Governance-Logik, die Innovation und operative Verantwortung zusammenführt.

Was Sie aus diesem Whitepaper mitnehmen

Dieses Whitepaper unterstützt Entscheider*innen dabei, souveräne Cloud-Transformation nicht als isolierte Technologiefrage zu betrachten, sondern als steuerbare Architektur-, Daten-, Security- und Betriebsentscheidung.

01	Warum punktuelle Cloud-, Daten- und AI-Initiativen häufig nicht skalieren
02	Welche sieben Dimensionen digitale Souveränität für Energieversorger und Netzbetreiber steuerbar machen
03	Welche fünf Use Cases den größten Architektur-, Daten- und Plattformhebel bieten
04	Welche Plattformbausteine für souveränen Cloud-Betrieb notwendig sind
05	Wie AWS European Sovereign Cloud als mögliche Infrastruktur-Option eingeordnet werden kann
06	Wie ein realistischer Einstieg in eine souveräne Cloud-Transformation aussehen kann

INHALTSVERZEICHNIS

1. Warum Energieversorger und Netzbetreiber jetzt handeln müssen

Die Energiewirtschaft befindet sich in einem strukturellen Umbau. Was früher planbarer, zentraler und stärker linear organisiert war, wird heute dezentraler, datenintensiver und dynamischer. Energieversorger, Netzbetreiber und Stadtwerke müssen bestehende Systeme stabil betreiben und gleichzeitig neue digitale Fähigkeiten aufbauen: als Steuerungsinstanz, Plattformbetreiber, Datenverarbeiter, Serviceanbieter und Partner lokaler Energiewenden.

Diese Entwicklung ist besonders für Stadtwerke sichtbar. Viele von ihnen sind integrierte Energieunternehmen: Sie verbinden Versorgung, Netzbetrieb, Kundenservice, Energiedienstleistungen, Messwesen, Ladeinfrastruktur und kommunale Verantwortung. Damit bündeln sie mehrere Marktrollen – und damit auch mehrere digitale Problemstellungen – in einer Organisation.

DIE ENERGIEWENDE WIRD ZUR DATEN- UND STEUERUNGSAUFGABE

Mit der zunehmenden Dezentralisierung verändert sich die operative Realität. Photovoltaikanlagen, Batteriespeicher, Wärmepumpen, Ladepunkte, Prosumer-Modelle und flexible Verbraucher erhöhen die Komplexität im Netz und an der Kundenschnittstelle. Gleichzeitig steigt der Bedarf, Daten aus unterschiedlichen Systemen zu integrieren, auszuwerten und für operative Entscheidungen nutzbar zu machen.

Smart Meter, IoT-Systeme, Netzleittechnik, Kundenplattformen, Abrechnungssysteme, CRM, ERP und externe Datenquellen erzeugen ein immer dichteres Informationsnetz. Doch der Wert dieser Daten entsteht nicht durch ihre bloße Verfügbarkeit. Er entsteht erst dann, wenn sie sicher integriert, qualitativ abgesichert, nachvollziehbar verarbeitet und in Entscheidungen oder Prozesse übersetzt werden.

> **Für Netzbetreiber bedeutet das:** Netzplanung, Netzstabilität, Engpassmanagement und dezentrale Steuerung werden stärker datengetrieben.
>
> **Für Energieversorger bedeutet es:** Kundenangebote, Energieberatung, Tarife, Serviceprozesse und neue digitale Geschäftsmodelle hängen zunehmend von Datenqualität, Integrationsfähigkeit und Plattformfähigkeit ab.

FACHKRÄFTEMANGEL ERHÖHT DEN AUTOMATISIERUNGSDRUCK

Parallel zur technischen Komplexität steigt der organisatorische Druck. Viele Energieversorger müssen mehr digitale Aufgaben bewältigen, ohne im gleichen Maß zusätzliche Fachkräfte aufbauen zu können. Besonders in Betrieb, Kundenservice, IT, Netzsteuerung und Datenmanagement entstehen Engpässe.

Automatisierung und AI können hier entlasten – aber nur, wenn sie kontrolliert eingesetzt werden. Ein Chatbot, eine Prognosekomponente oder ein AI-Agent löst noch kein strukturelles Problem, wenn Datenqualität, Systemintegration, Governance, Verantwortlichkeiten und menschliche Kontrolle fehlen.

Das ist gerade in der Energiewirtschaft entscheidend. Bei kritischer Infrastruktur dürfen Automatisierung und AI nicht zu Kontrollverlust führen. Sie müssen Fachkräfte unterstützen, Entscheidungsgrundlagen verbessern und Routineaufgaben reduzieren – innerhalb klar definierter Leitplanken.

REGULATORIK UND CYBERSECURITY WERDEN ZUM ARCHITEKTURTHEMA

Energieversorger und Netzbetreiber arbeiten in einem besonders sensiblen Umfeld. Sie betreiben versorgungsnahe oder kritische Systeme, verarbeiten sensible Daten und müssen regulatorische Anforderungen erfüllen. Gleichzeitig wachsen die Angriffsflächen: durch vernetzte Systeme, Cloud-Nutzung, IT-/OT-Konvergenz, Drittanbieter, Schnittstellen und datengetriebene Plattformen.

Damit wird Security nicht erst im Betrieb relevant. Sie muss bereits in Architekturentscheidungen, Plattformdesign, Datenflüsse, Rollenmodelle, Entwicklungsprozesse und Betriebsmodelle integriert werden. Belastbare IT-Sicherheit entsteht nicht durch einzelne Prüfungen oder nachgelagerte Compliance-Projekte, sondern durch Risikologik, sichere Architekturentscheidungen und ein tragfähiges Betriebsmodell.

NEUE DIGITALE SERVICES BRAUCHEN EINE TRAGFÄHIGE PLATTFORMGRUNDLAGE

Neben regulatorischem und operativem Druck entsteht wirtschaftlicher Veränderungsdruck. Energieversorger müssen neue digitale Angebote schneller entwickeln, Kundenbeziehungen digital stärken und datenbasierte Services in den Markt bringen: digitale Kundenportale, Energieberatung, dynamische Tarife, Lade- und Mobilitätsservices, Prosumer-Angebote, Flexibilitätsmodelle oder Plattformservices für kommunale Partner.

Doch neue Geschäftsmodelle entstehen nicht nachhaltig auf fragmentierten Systemlandschaften. Wenn Fachsysteme schlecht integriert sind, Daten in Silos liegen, Schnittstellen fehlen und Betrieb, Security oder Kostensteuerung uneinheitlich sind, wird jede neue digitale Initiative zum Einzelprojekt. Das erhöht Abstimmungsaufwand, verlängert Time-to-Market und erschwert Skalierung.

Die eigentliche Herausforderung ist deshalb nicht Cloud allein.
Die eigentliche Herausforderung ist digitale Steuerungsfähigkeit.

2. Warum punktuelle Modernisierung nicht reicht

Viele Energieversorger, Netzbetreiber und Stadtwerke modernisieren bereits. Sie führen Cloud-Infrastrukturen ein, bauen Datenplattformen auf, testen AI-Anwendungen, digitalisieren Kundenprozesse oder modernisieren einzelne Fachsysteme. Das ist richtig – aber häufig bleibt die Wirkung hinter den Erwartungen zurück.

Der Grund liegt selten in fehlendem Veränderungswillen. Meist liegt er in der Art, wie Modernisierung organisiert wird: als Sammlung einzelner Initiativen statt als zusammenhängende Architektur-, Daten-, Security- und Betriebsentscheidung.

Ein Cloud-Projekt löst kein Datenproblem. Ein AI-Pilot ersetzt keine Datenstrategie. Eine neue Kundenplattform beseitigt keine Integrationslücken in gewachsenen Fachsystemen. Und eine souveräne Cloud-Option schafft noch keine digitale Souveränität, wenn Rollen, Zugriffe, Betrieb, Monitoring, Kostensteuerung und Verantwortlichkeiten unklar bleiben.

TYPISCHE FEHLMUSTER

Cloud wird als Hosting-Frage behandelt.

Die Frage lautet dann: Welche Anwendungen können wir in die Cloud verschieben? Diese Frage ist legitim, aber zu klein. Eine schlecht integrierte Anwendung wird durch Cloud nicht automatisch integrationsfähig. Ein unklarer Datenfluss wird durch Cloud nicht automatisch nachvollziehbar.

Ein heterogenes Rechte- und Verantwortlichkeitsmodell wird durch Cloud nicht automatisch sicher.

Daten bleiben in Silos gebunden.

Smart-Meter-Daten, Netzsysteme, Kundenplattformen, Abrechnung, CRM, ERP, Ladeinfrastruktur, IoT-Komponenten und Prognosemodelle erzeugen enorme Datenmengen. Doch ohne gemeinsame Datenarchitektur entstehen widersprüchliche Informationsstände, manuelle Abstimmungen und unsichere Entscheidungsgrundlagen. Data Governance ist deshalb kein nachgelagerter Verwaltungsaufwand, sondern Voraussetzung für Skalierung.

AI-Piloten lösen kein Skalierungsproblem.

Viele Energieversorger experimentieren mit AI. Doch AI erzeugt nur dann nachhaltigen Wert, wenn sie produktiv, sicher und kontrolliert in bestehende Prozesse integriert wird. Im produktiven Umfeld stellen sich Fragen nach Datenqualität, Schnittstellen, Zugriffen, Verantwortlichkeiten, Nachvollziehbarkeit, Human-in-the-Loop, Security, Datenschutz und Betrieb. Ohne diese Grundlagen bleibt AI ein Experiment.

Security und Compliance werden zu spät integriert.

Wenn erst eine Plattform aufgebaut, eine Anwendung modernisiert oder ein digitaler Service entwickelt wird und danach Sicherheits- oder Nachweisanforderungen ergänzt werden, entstehen Nacharbeiten und Risiken. In der Energiewirtschaft kann das kritisch werden. Security muss Teil der Architektur sein.

Heterogener Betrieb erzeugt Kontrollverlust.

Wenn jedes Projekt Monitoring, Deployments, Rechte, Kostenstellen, Backup, Logging und Incident-Prozesse anders löst, entsteht ein Flickenteppich. Kurzfristig wirkt das flexibel. Langfristig wird Modernisierung schwer steuerbar.

Neue digitale Geschäftsmodelle brauchen mehr als eine gute Idee.

Wenn jedes neue Angebot eine Sonderintegration braucht, wird Time-to-Market langsam. Wenn Datenqualität nicht gesichert ist, entstehen unzuverlässige Services. Wenn Security und Compliance nachträglich ergänzt werden, steigen Aufwand und Risiko. Damit wird aus einem innovativen Service schnell ein weiteres Einzelprojekt.

Genau deshalb müssen Architektur, Transformation und Engineering als zusammenhängende Plattformstrategie betrachtet werden. Plattformentscheidungen wirken unmittelbar auf Skalierbarkeit, Kostenstruktur, Stabilität und regulatorische Belastbarkeit.

FRAGEN FÜR ENTSCHEIDER*INNEN

1. Entstehen Cloud-Initiativen ohne klares Zielbild für Architektur, Betrieb und Governance?
2. Liefern Datenprojekte einzelne Dashboards, aber keine belastbare Datensteuerung?
3. Bleiben AI-Piloten im Teststatus stecken?
4. Werden Security-Anforderungen spät geprüft?
5. Lösen Teams Monitoring, Deployment, Kosten und Betrieb unterschiedlich?
6. Lassen sich Kosten nicht zuverlässig nach Workloads, Services oder Verantwortlichkeiten steuern?
7. Sind Betriebs- und Notfallprozesse für neue digitale Services unklar?

Wenn mehrere dieser Punkte zutreffen, besteht kein reines Technologieproblem. Dann fehlt eine übergreifende Architektur- und Governance-Logik.

3. Digitale Souveränität ist mehr als Datenresidenz

Digitale Souveränität wird häufig auf eine einfache Frage reduziert: Wo liegen unsere Daten?

Diese Frage ist wichtig. Für Energieversorger, Netzbetreiber und Stadtwerke kann Datenresidenz ein entscheidendes Kriterium sein – besonders bei sensiblen Kunden-, Netz-, Betriebs- oder Infrastrukturdaten. Doch Datenresidenz allein reicht nicht aus.

Ein System kann Daten in Deutschland oder Europa speichern und trotzdem schwer steuerbar sein. Zugriffe können unklar bleiben. Datenflüsse können intransparent sein. Betriebsverantwortlichkeiten können diffus sein. Kosten können unkontrolliert wachsen. Security kann nachgelagert bleiben. Notfallfähigkeit kann ungetestet sein. Und Abhängigkeiten können entstehen, ohne dass sie bewusst bewertet wurden.

> **Digitale Souveränität** beginnt deshalb nicht beim Rechenzentrumsstandort. Sie beginnt bei der Fähigkeit, Kontrolle strukturiert auszuüben.

DIE ENERGIEWENDE WIRD ZUR DATEN- UND STEUERUNGSAUFGABE

Souverän ist nicht, wer alles selbst betreibt. Souverän ist, wer bewusst entscheiden, steuern, nachweisen und im Ernstfall handeln kann.

Für Energieversorger und Netzbetreiber umfasst digitale Souveränität sieben Dimensionen:

Dimension	Leitfrage
Daten	Welche Daten sind kritisch, wo dürfen sie verarbeitet werden und wer trägt Verantwortung?
Zugriff	Welche Rollen, Identitäten und Berechtigungen sind notwendig und wie werden sie überwacht?
Architektur	Welche Cloud-, Plattform- und Integrationsmodelle tragen die fachlichen und regulatorischen Anforderungen?
Security	Wie werden Security-by-Design, Monitoring, Incident-Prozesse und Resilienz integriert?
Betrieb	Wie werden Verfügbarkeit, Backup, Desaster Recovery, Support, Updates und Eskalation geregelt?
Nachweisbarkeit	Welche Dokumentation, Logs, Reports und Governance-Strukturen machen Kontrolle überprüfbar?
Weiterentwicklung	Wie bleiben Plattform, Datenbasis und Anwendungen erweiterbar, portierbar und wirtschaftlich steuerbar?

Diese Dimensionen machen digitale Souveränität praktisch greifbar. Sie zeigen: Souveränität entsteht nicht durch eine einzelne Entscheidung, sondern durch das Zusammenspiel kontrollierbarer Bausteine.

WARUM DAS THEMA AUF DIE MANAGEMENT-AGENDA GEHÖRT

Souveräne Cloud-Transformation ist kein rein technisches Architekturthema. Für Geschäftsführung, IT-Leitung, Operations und Compliance entscheidet sie darüber, wie kontrollierbar digitale Modernisierung in den nächsten Jahren bleibt.

Eine tragfähige Souveränitätslogik schafft:

- geringere Risiken bei Cloud-, Daten- und AI-Initiativen
- bessere regulatorische Nachweisfähigkeit
- höhere Transparenz über kritische Daten, Systeme und Abhängigkeiten
- schnellere Entwicklung neuer digitaler Services
- kontrollierbare Betriebs- und Skalierungskosten
- mehr Resilienz bei Sicherheitsvorfällen, Ausfällen oder regulatorischen Änderungen
- eine belastbare Grundlage für künftige Plattform-, Daten- und AI-Entscheidungen

Damit wird digitale Souveränität zur Führungsaufgabe: Sie verbindet Innovationsfähigkeit mit Verantwortung, Kontrolle und langfristiger Handlungsfähigkeit.

SCHUTZBEDARF STATT ONE-SIZE-FITS-ALL

Nicht jeder Workload braucht denselben Souveränitätsgrad. Ein öffentliches Informationsangebot hat andere Anforderungen als ein Kundenportal. Ein Analytics-Dashboard hat andere Anforderungen als Netzsteuerung. Eine Testumgebung hat andere Anforderungen als produktionskritische Plattformkomponenten. Eine AI-Anwendung im Kundenservice hat andere Anforderungen als eine AI-Komponente mit netzrelevanten Daten.

Deshalb sollte digitale Souveränität abgestuft gedacht werden: nach Schutzbedarf, regulatorischer Relevanz, operativer Kritikalität, Kostenwirkung und technischer Machbarkeit.

Diese Abstufung verhindert zwei Extreme: unreflektierte Cloud-Nutzung ohne ausreichende Kontrolle – und pauschale Blockade von Modernisierung aus Sorge vor Risiken. Souveräne Transformation entsteht in der Mitte: durch bewusste Klassifizierung, klare Architekturprinzipien und nachvollziehbare Betriebsmodelle.

SCHUTZBEDARF STATT ONE-SIZE-FITS-ALL

Souveräne Cloud-Modelle wie AWS European Sovereign Cloud können für Organisationen mit hohen Anforderungen an Datenresidenz, betriebliche Autonomie und europäische Governance relevant sein. Für bestimmte Workloads kann eine solche Option neue Handlungsspielräume schaffen.

Aber auch hier gilt: Eine souveräne Infrastruktur ersetzt keine souveräne Architektur.

Wenn Datenklassifizierung fehlt, Zugriffe unklar sind, Betriebsprozesse nicht definiert wurden, Security nachträglich ergänzt wird oder Kostensteuerung diffus bleibt, löst auch eine souveräne Cloud-Option das Grundproblem nicht. Sie kann ein wichtiger Baustein sein – aber nur innerhalb einer tragfähigen Zielarchitektur.

4. Fünf Use Cases, in denen souveräneCloud-Architekturen konkret wirksam werden

Digitale Souveränität bleibt abstrakt, solange sie nur über Datenresidenz, Cloud-Modelle oder regulatorische Anforderungen diskutiert wird. Für Energieversorger, Netzbetreiber und Stadtwerke wird sie dort greifbar, wo konkrete Anwendungsfälle produktiv umgesetzt werden sollen.

Die folgenden fünf Use-Case-Cluster zeigen, wo Cloud, Daten, Security, AI und Plattformmodernisierung gemeinsam betrachtet werden müssen.

USE CASE 1

Smart Meter & Datenplattformen

01

Smart Meter verändern die Datenlogik von Energieversorgern. Aus periodischen Abrechnungswerten werden granulare Datenströme. Aus isolierten Messpunkten entsteht eine Grundlage für Netzsteuerung, Kundenservice, Energieberatung, Prognosen und neue digitale Geschäftsmodelle.

Klassische Systeme wurden jedoch oft nicht für diese Datenmengen, Granularitäten und Integrationsanforderungen gebaut. Der Wert entsteht erst, wenn Messdaten sicher integriert, qualitativ abgesichert, skalierbar verarbeitet und fachlich nutzbar gemacht werden.

BENÖTIGTE FÄHIGKEITEN

- sichere Schnittstellen zu Mess- und Gateway-Systemen
- skalierbare Datenpipelines
- Datenklassifizierung und Data Governance
- Rollen- und Zugriffskonzepte
- nachvollziehbare Datenflüsse
- Analytics- und AI-fähige Datenarchitektur
- Monitoring und Observability

BUSINESS IMPACT

Souverän nutzbare Messdaten ermöglichen bessere Netzplanung, schnellere Störungserkennung, personalisierte Energieberatung, höhere Verbrauchstransparenz und neue digitale Services. Sie schaffen außerdem eine Grundlage für dynamische Tarife, Flexibilitätsmodelle und AI-gestützte Prognosen.

SOUVERÄNITÄTSFRAGE

Können Messdaten so integriert und genutzt werden, dass neue digitale Services entstehen, ohne Datenschutz, Zugriffskontrolle, Nachvollziehbarkeit und Betriebssicherheit zu gefährden?

USE CASE 2

DERMS & dezentrale Energieressourcen

02

Photovoltaikanlagen, Batteriespeicher, Wärmepumpen, Ladepunkte, Prosumer-Modelle und flexible Verbraucher erzeugen neue Steuerungsanforderungen. DERMS steht exemplarisch für diese neue Aufgabe: dezentrale Energieressourcen erfassen, überwachen, prognostizieren und netzdienlich einsetzen.

DERMS ist nicht nur ein Netzprojekt. Es berührt Smart-Meter-Daten, Netzmodelle, Asset-Daten, Wetter- und Prognosedaten, Marktinformationen, Kundensysteme, Leitsysteme, IoT-Plattformen und externe Partner.

BENÖTIGTE FÄHIGKEITEN

- robuste Integrationsarchitektur
- APIs und Datenmodelle für heterogene Quellen
- klare Latenz- und Verfügbarkeitsanforderungen
- Security-by-Design für IT-/OT-nahe Prozesse
- Monitoring, Fallback und Verantwortungsmodell
- abgestufte Schutzbedarfslogik

BUSINESS IMPACT

Ein tragfähiger DERMS-Ansatz kann Netzstabilität verbessern, erneuerbare Energien besser integrieren, vorhandene Infrastruktur effizienter nutzen und neue Flexibilitätsmodelle ermöglichen. Für integrierte EVU und Stadtwerke kann daraus außerdem die Grundlage für neue energienahe Services entstehen.

SOUVERÄNITÄTSFRAGE

Können dezentrale Energieressourcen digital gesteuert werden, ohne Kontrolle über Datenflüsse, Zugriffe, Betriebsverantwortung und kritische Entscheidungen zu verlieren?

USE CASE 3

IT-/OT-Security & regulatorische Resilienz

03

Energieversorger arbeiten an der Schnittstelle zwischen IT, OT und kritischer Infrastruktur. Je stärker Cloud-, Daten- und AI-Anwendungen produktiv werden, desto wichtiger werden klare Sicherheitsarchitekturen, Segmentierung, Monitoring, Zugriffskontrolle und Incident-Prozesse.

Security darf dabei nicht als Kontrollschicht am Ende verstanden werden. Sie muss Teil der Zielarchitektur sein.

BENÖTIGTE FÄHIGKEITEN

- Risiko- und Schutzbedarfsanalyse
- Security-by-Design
- Identitäts- und Berechtigungsmodelle
- Netzwerksegmentierung
- Logging, Monitoring und Incident Response
- Backup und Disaster Recovery
- auditfähige Dokumentation

BUSINESS IMPACT

Ein struktureller Security- und Resilienzansatz reduziert Betriebs- und Sicherheitsrisiken, verbessert Auditfähigkeit und schafft mehr Management-Transparenz.

Gleichzeitig können neue digitale Services schneller produktiv gehen, weil Sicherheitsanforderungen nicht jedes Mal neu ausgehandelt werden müssen.

SOUVERÄNITÄTSFRAGE

Können digitale Plattformen, Datenflüsse und operative Systeme so abgesichert werden, dass Risiken nicht nur reduziert, sondern auch überwacht, nachgewiesen und im Ernstfall gesteuert werden können?

USE CASE 4

Modernisierung geschäftskritischer Anwendungen

04

Viele Energieversorger arbeiten mit gewachsenen Systemlandschaften: Abrechnung, ERP, CRM, Netzplanung, Messwesen, Kundenportale, Fachverfahren, Integrationsschichten und individuelle Anwendungen. Diese Systeme sind stabil, geschäftskritisch und tief in Prozesse eingebettet – aber häufig schwer erweiterbar.

Modernisierung ist deshalb selten ein Greenfield-Projekt. Sie muss im laufenden Betrieb erfolgen.

BENÖTIGTE FÄHIGKEITEN

- Architektur-Assessment
- Transparenz über Abhängigkeiten und Datenflüsse
- API- und Integrationsstrategie
- kontrollierte Entkopplung
- Cloud-Readiness-Bewertung
- schrittweises Re-Platforming
- standardisierte Betriebsmodelle

BUSINESS IMPACT

Kontrollierte Modernisierung ermöglicht schnellere Entwicklung neuer Services, reduziert technische Schulden, senkt Betriebsrisiken und verbessert Datenverfügbarkeit. Für Entscheider*innen wird Modernisierung dadurch planbarer: nicht als riskanter Big Bang, sondern als priorisierter Pfad mit klaren Abhängigkeiten und messbarer Wirkung.

SOUVERÄNITÄTSFRAGE

Können geschäftskritische Anwendungen so modernisiert werden, dass Abhängigkeiten reduziert, Betriebskontinuität gesichert und neue digitale Fähigkeiten schrittweise aufgebaut werden?

USE CASE 5

05

AI-gestützter Kundenservice und Prozessautomatisierung

Kundinnen und Kunden erwarten einfache digitale Services, transparente Informationen und schnelle Antworten. Gleichzeitig werden Produkte komplexer: dynamische Tarife, PV, Speicher, Wärmepumpen, Ladeinfrastruktur, Energieberatung und Prosumer-Angebote erzeugen neue Fragen und Beratungsbedarfe.

AI kann hier ein starker Entlastungshebel sein – aber nur, wenn sie sauber eingebettet wird.

BENÖTIGTE FÄHIGKEITEN

- konsistente Kundendaten
- angebundene Wissensquellen
- Prozessintegration
- rollenbasierte Zugriffe
- Human-in-the-Loop
- Qualitätsprüfung und Monitoring
- AI-Governance

BUSINESS IMPACT

Richtig umgesetzt kann AI Fachkräfte entlasten, Routineanfragen schneller bearbeiten, Anliegen besser klassifizieren und konsistentere digitale Services ermöglichen. Darüber hinaus kann AI-gestützter Kundenservice zur Grundlage neuer Plattformservices werden: Energieberatung, Verbrauchstransparenz, Empfehlungen für PV, Speicher oder Wärmepumpen, digitale Begleitung von Ladeinfrastruktur oder Self-Service-Angebote für Gewerbe und Wohnungswirtschaft.

SOUVERÄNITÄTSFRAGE

Kann AI so eingesetzt werden, dass Fachkräfte entlastet und Kunden besser unterstützt werden – ohne Kontrolle über Daten, Entscheidungen und Verantwortung zu verlieren?

WAS DIE USE CASES VERBINDET

Die fünf Use Cases wirken auf den ersten Blick unterschiedlich. Smart Meter ist ein Daten- und Integrationsfall. DERMS ist ein Steuerungs- und Netzfall. IT-/OT-Security ist ein Resilienzfall. Anwendungsmodernisierung ist ein Plattform- und Legacy-Fall. AI-gestützter Kundenservice ist ein Automatisierungs- und Kundenschnittstellenfall.

Doch unter der Oberfläche zeigen alle dasselbe Muster: Keiner dieser Use Cases lässt sich nachhaltig als isoliertes Einzelprojekt lösen. Jeder braucht eine gemeinsame digitale Grundlage:

- skalierbare Plattformarchitektur

- belastbare Datenintegration
- klare Data Governance
- Security-by-Design
- Rollen- und Zugriffskontrolle
- Monitoring und Logging
- Betrieb, Backup und Notfallfähigkeit
- nachvollziehbare Verantwortlichkeiten
- Kosten- und Betriebssteuerung
- klare Priorisierung nach Schutzbedarf und Business Impact

Genau deshalb ist souveräne Cloud-Transformation für Energieversorger und Netzbetreiber keine Frage einzelner Technologien. Sie ist die Fähigkeit, wiederkehrende Plattform-, Daten-, Security- und Betriebsanforderungen so zu standardisieren, dass neue Use Cases schneller und sicherer entstehen können.

5. Vom Zielbild zur betreibbaren Plattform

Souveräne Cloud-Transformation entsteht nicht durch ein Zielbild allein. Sie entsteht erst dann, wenn Architektur, Daten, Security, Betrieb und Verantwortlichkeiten so umgesetzt werden, dass digitale Services dauerhaft sicher, skalierbar und wirtschaftlich steuerbar betrieben werden können.

Für Energieversorger, Netzbetreiber und Stadtwerke ist diese Übersetzung besonders wichtig. Sie können es sich nicht leisten, digitale Innovation auf instabilen Betriebsmodellen aufzubauen. Neue Services müssen anschlussfähig, sicher, auditierbar und im Störfall steuerbar sein.

DIE ZENTRALEN PLATTFORMBAUSTEINE

Baustein	Funktion im souveränen Betriebsmodell
Landing Zone	Strukturierter Ausgangspunkt für kontrollierten Cloud-Betrieb mit Grundprinzipien für Accounts, Netzwerke, Identitäten, Sicherheitsstandards, Logging, Monitoring, Kostenstrukturen und Verantwortlichkeiten.

Baustein	Funktion im souveränen Betriebsmodell
Guardrails	Verbindliche Leitplanken für Architektur, Security, Betrieb und Kosten. Sie ermöglichen Innovation innerhalb definierter Standards, statt Sicherheits- und Betriebsfragen in jedem Projekt neu zu verhandeln.
Rollen und Verantwortlichkeiten	Klare Zuständigkeiten zwischen Plattformteam, Applikationsteams, Fachbereichen, Security und externen Partnern.
Monitoring und Logging	Grundlage für Resilienz, Security, Compliance und Management-Transparenz. Was nicht sichtbar ist, lässt sich nicht steuern.
Backup und Disaster Recovery	Notfallfähigkeit als Teil der Architektur. RTO und RPO übersetzen Business- und Versorgungskritikalität in Betriebsanforderungen.
Infrastructure as Code	Reproduzierbare, versionierbare und überprüfbare Umgebungen statt manueller Einzelkonfiguration.
FinOps	Kostensteuerung über Account-, Tagging-, Verantwortlichkeits- und Reporting-Standards.
Enablement und Support	Befähigung der Teams, Plattformen, Prozesse und Use Cases zu verstehen, zu steuern und weiterzuentwickeln.

DER ENTSCHEIDENDE PUNKT

Eine souveräne Plattform soll nicht nur kontrollieren. Sie soll befähigen.

Wenn Teams für jedes neue digitale Vorhaben Datenbanken, Monitoring, Schnittstellen, Zertifikate, Deployment-Prozesse oder Sicherheitsbausteine neu definieren müssen, geht Geschwindigkeit verloren. Wiederverwendbare Plattformservices schaffen dagegen eine Grundlage, auf der neue Use Cases schneller und sicherer entstehen können.

Damit wird aus Cloud-Nutzung eine organisatorische Fähigkeit: neue digitale Services wiederholbar entwickeln, sicher betreiben und kontrolliert erweitern zu können.

6. AWS European Sovereign Cloud als mögliche Infrastruktur-Option

Souveräne Cloud-Transformation stellt Energieversorger, Netzbetreiber und Stadtwerke vor eine anspruchsvolle Abwägung. Einerseits brauchen sie moderne Cloud-Fähigkeiten: Skalierbarkeit, Automatisierung, Datenverarbeitung, AI-Services, resiliente Plattformen und schnellere Innovationszyklen. Andererseits arbeiten sie in einem Umfeld, in dem Datenschutz, Versorgungssicherheit, regulatorische Nachweisbarkeit und operative Kontrolle besonders hohe Bedeutung haben.

In diesem Spannungsfeld können souveräne Cloud-Modelle relevant werden.

AWS European Sovereign Cloud ist eine mögliche Option für Organisationen mit hohen Anforderungen an Datenresidenz, betriebliche Autonomie und europäische Governance. Für dieses Whitepaper ist jedoch entscheidend: AWS ESC ist nicht der Ausgangspunkt der Strategie. Sie ist eine mögliche Infrastruktur-Option innerhalb einer souveränen Cloud-Architektur.

WANN AWS ESC RELEVANT WERDEN KANN

AWS ESC kann insbesondere für Workloads prüfenswert sein, bei denen besondere Anforderungen an Datenresidenz, Zugriffskontrolle, Nachweisbarkeit oder europäische Governance bestehen. Für Energieversorger und Netzbetreiber können das zum Beispiel sein:

- sensible Datenplattformen mit Kunden-, Mess-, Netz- oder Betriebsdaten
- regulierte Analyse- und AI-Anwendungen
- zentrale Logging-, Monitoring- oder Audit-Komponenten
- geschäftskritische digitale Services
- modernisierte Fachanwendungen mit regulatorischem Bezug

Gleichzeitig sollte AWS ESC nicht pauschal für „alles“ oder „nichts“ bewertet werden. Sinnvoll ist eine Workload-Klassifizierung nach Schutzbedarf, Nutzen, Kosten, Flexibilität und Betriebsfähigkeit.

KEIN ERSATZ FÜR ZIELARCHITEKTUR

Eine souveräne Cloud-Infrastruktur löst nicht automatisch alle Souveränitätsfragen. Sie beantwortet bestimmte Infrastruktur- und Betriebsanforderungen. Andere Fragen bleiben Aufgabe der Organisation und ihrer Architekturpartner:

- Welche Daten sind kritisch?

- Welche Workloads gehören in welches Betriebsmodell?
- Welche Zugriffe sind erlaubt?
- Wie werden Anwendungen sicher entwickelt?
- Wie werden Datenflüsse dokumentiert?
- Wie werden Monitoring, Logging, Backup und Disaster Recovery umgesetzt?
- Wie werden Kosten gesteuert?
- Wie wird Exit-Fähigkeit berücksichtigt?

Der Wert entsteht, wenn souveräne Cloud-Optionen in ein belastbares Plattform- und Betriebsmodell eingebettet werden. Dann können Energieversorger moderne Cloud-Fähigkeiten nutzen, ohne Kontrolle, Nachweisbarkeit und operative Verantwortung aus der Hand zu geben.

7. Der jambit-Ansatz: Von der Entscheidung zur Umsetzung

Souveräne Cloud-Transformation beginnt mit einer strategischen Frage, wird aber erst durch Umsetzung wirksam.
Der jambit-Ansatz setzt an der Schnittstelle zwischen Zielbild und Realisierung an: bei der Übersetzung strategischer Ziele in eine belastbare Architektur-, Daten-, Security- und Umsetzungslogik.

1 Ausgangslage verstehen

Am Anfang steht eine strukturierte Standortbestimmung:

- Welche digitalen Services oder Use Cases sind geplant?
- Welche Systeme und Datenquellen sind betroffen?
- Welche Schutzbedarfe gelten?
- Welche regulatorischen Anforderungen sind relevant?
- Welche Betriebsstandards existieren bereits?
- Wo entstehen Risiken durch Legacy, Silos oder unklare Verantwortlichkeiten?

2 Zielarchitektur definieren → 3 Use Cases priorisieren

Auf Basis der Standortbestimmung entsteht eine Zielarchitektur. Sie beschreibt nicht nur, welche Technologie genutzt werden soll, sondern wie digitale Fähigkeiten künftig strukturiert bereitgestellt werden: Cloud- und Infrastrukturmodelle, Integrationsarchitektur, Datenarchitektur, Sicherheitsprinzipien, Plattformstandards, Betriebsmodelle, Verantwortlichkeiten und Migrationspfade.

Der richtige erste Use Case ist nicht zwingend der größte. Es ist derjenige, der strategische Relevanz, technische Machbarkeit und kontrollierbares Risiko verbindet – und dabei wiederverwendbare Plattform-, Daten- oder Security-Fähigkeiten schafft.

4 Plattform- und Betriebsmodell aufbauen → 5 Erste Use Cases produktiv realisieren

jambit bringt Erfahrung aus Plattform- und Cloud-Projekten ein: Landing Zone, Guardrails, Rollen- und Rechtekonzepte, Monitoring, Logging, Backup, Disaster Recovery, Infrastructure as Code, Deployment-Standards, FinOps und Supportprozesse.

Ein MVP darf im Kontext souveräner Cloud-Transformation kein Wegwerf-Pilot sein. Er sollte so aufgebaut sein, dass zentrale Plattform-, Daten- und Governance-Prinzipien bereits validiert werden. So entsteht aus einem ersten Projekt ein wiederholbares Modell.

6 Enablement und Skalierung absichern

Digitale Souveränität darf nicht in einer Black Box verschwinden. jambit setzt deshalb auf gemeinsamen Aufbau, Wissenstransfer und strukturierte Übergabe. Plattform, Prozesse und Use Cases werden nicht nur implementiert, sondern so dokumentiert und operationalisiert, dass interne Teams sie verstehen, steuern und weiterentwickeln können.

DER MEHRWERT FÜR ENTSCHEIDER*INNEN

Der Wert liegt nicht in einer einzelnen Technologieempfehlung. Er liegt darin, strategische Anforderungen in belastbare digitale Strukturen zu übersetzen.

Für Energieversorger, Netzbetreiber und Stadtwerke bedeutet das: Cloud, Daten, AI, Security, Plattformen und Softwareentwicklung werden so zusammengeführt, dass Modernisierung kontrolliert, betreibbar und skalierbar wird.

8. Checkliste für Entscheider*innen

Die folgende Checkliste hilft Ihnen, die Ausgangslage Ihrer Organisation strukturiert einzuordnen. Sie ersetzt kein Audit, schafft aber Orientierung: Wo bestehen belastbare Grundlagen? Wo gibt es Unklarheiten? Und wo lohnt sich ein strukturierter Einstieg?

STRATEGIE UND GESCHÄFTSMODELL

- Welche digitalen Services sollen in den nächsten drei Jahren entstehen?
- Welche bestehenden Geschäftsmodelle geraten unter Druck?
- Wo entstehen neue Chancen durch Daten, Plattformen oder AI?
- Sind Geschäftsführung, IT, Fachbereiche und Betrieb auf dieselben Prioritäten ausgerichtet?

DATEN UND GOVERNANCE

- Welche Daten sind geschäfts-, kunden- oder versorgungskritisch?
- Gibt es eine Datenklassifizierung nach Schutzbedarf?
- Sind Datenflüsse zwischen Fachsystemen, Plattformen und externen Diensten nachvollziehbar?
- Sind Datenverantwortlichkeiten klar definiert?

ARCHITEKTUR UND PLATTFORM

- Gibt es ein klares Zielbild für Public, Private, Hybrid oder souveräne Cloud-Modelle?
- Welche Workloads sind cloudfähig, welche nicht?
- Gibt es eine standardisierte Plattformgrundlage mit Landing Zone, Guardrails und Rollenmodell?
- Sind Infrastruktur, Konfigurationen und Deployments reproduzierbar?

SECURITY UND COMPLIANCE

- Welche regulatorischen Anforderungen betreffen IT-, OT- und Cloud-Landschaft?
- Werden Security-Anforderungen bereits in Architektur und Entwicklung integriert?
- Sind Identitäten, Rollen und privilegierte Zugriffe klar geregelt?
- Können Sicherheits- und Compliance-Maßnahmen auditfähig nachgewiesen werden?

BETRIEB UND RESILIENZ

- Wer ist für Plattform, Anwendungen, Datenflüsse und Betriebsprozesse verantwortlich?
- Sind RTO- und RPO-Ziele für kritische Workloads definiert?
- Gibt es Backup- und Disaster-Recovery-Konzepte, die regelmäßig getestet werden?
- Sind Runbooks, Supportprozesse und Eskalationswege dokumentiert?

KOSTEN UND STEUERUNG

- Können Kosten den Workloads, Teams, Services oder Produkten zugeordnet werden?
- Gibt es verbindliche Tagging-, Account- und Budgetstandards?
- Werden Cloud-Kosten regelmäßig analysiert und optimiert?
- Werden Architekturentscheidungen auch unter Betriebs- und Skalierungskosten bewertet?

EINSTIEGSSZENARIO

- Welcher Use Case eignet sich für einen kontrollierten Einstieg?
- Welche Architektur- und Governance-Fragen sind zuerst zu klären?
- Welche Teams müssen eingebunden werden?
- Welche Ergebnisse sollen nach 6, 8 oder 12 Wochen sichtbar sein?
- Welche wiederverwendbaren Fähigkeiten sollen durch den Einstieg entstehen?

9. Fazit und nächster Schritt

Energieversorger, Netzbetreiber und Stadtwerke stehen vor einer anspruchsvollen Transformationsaufgabe. Sie müssen digitale Modernisierung beschleunigen, Daten besser nutzen, neue Services entwickeln, AI kontrolliert einsetzen, Security und Compliance stärken und geschäftskritische Systeme weiterentwickeln – ohne operative Kontrolle, Versorgungskontinuität oder regulatorische Belastbarkeit zu gefährden.

Cloud kann dabei ein wichtiger Hebel sein. Aber Cloud allein ist nicht die Lösung.

Die entscheidende Fähigkeit liegt darin, Cloud, Daten, Security, AI, Plattformen und Betrieb in eine kontrollierbare Architektur- und Governance-Logik zu übersetzen. Digitale Souveränität entsteht nicht durch eine einzelne Infrastrukturentscheidung. Sie entsteht durch das Zusammenspiel aus Datenkontrolle, Zugriffskontrolle, Zielarchitektur, Security-by-Design, auditierbarem Betrieb, klaren Verantwortlichkeiten, Kostensteuerung und organisatorischer Handlungsfähigkeit.

Die gute Nachricht:
Souveräne Cloud-Transformation muss nicht als Big Bang beginnen. Sie kann mit einer strukturierten Standortbestimmung, einer klaren Schutzbedarfslogik und einem priorisierten Einstiegsszenario starten.

Der erste Schritt ist nicht die **vollständige Migration.**
Der erste Schritt ist **Klarheit.**

CLOUD-SOUVERÄNITÄTS-CHECK FÜR ENERGIEVERSORGER UND NETZBETREIBER

Mit dem Cloud-Souveränitäts-Check unterstützt jambit Energieversorger, Netzbetreiber und energienahe Infrastrukturunternehmen dabei, ihre Ausgangslage strukturiert einzuordnen und einen realistischen Einstieg in souveräne Cloud-Transformation zu definieren.

Im Mittelpunkt stehen konkrete Entscheidungsfragen:

- Welche Cloud-, Daten- und Plattformentscheidungen sind für Ihre Ausgangslage sinnvoll?
- Welche Daten, Systeme und Workloads haben besonderen Schutzbedarf?
- Wo entstehen Risiken durch Legacy, Silos, fehlende Governance oder unklare Betriebsmodelle?
- Welche Use Cases liefern den besten Einstieg?
- Welche Rolle können AWS European Sovereign Cloud oder andere Cloud-Modelle spielen?
- Welche Architektur- und Betriebsbausteine sollten zuerst aufgebaut werden?

Das Ergebnis ist keine theoretische Strategiepräsentation, sondern eine priorisierte Entscheidungsgrundlage: mit ersten Architekturleitplanken, Use-Case-Einordnung, Souveränitätsbewertung und konkretem nächsten Schritt.

SCHLUSSGEDANKE:

Energieversorger müssen digitale Innovation nicht gegen Sicherheit, Kontrolle oder Souveränität ausspielen. Der entscheidende Punkt ist, Modernisierung nicht als Folge einzelner Projekte zu betrachten, sondern als Aufbau wiederverwendbarer digitaler Fähigkeiten: belastbare Daten, sichere Plattformen, klare Governance, skalierbarer Betrieb und kontrollierte Umsetzung.

IHRE ANSPRECHPARTNER BEI JAMBIT

Dr. Christoph Schaffer
Head of Digital Energy Solutions

Fabian Stuhlmiller
Business Relationship Manager

Sie benötigen Beratung oder Unterstützung bei Ihrer souveränen Cloud-Transformation?

Natürlich beraten wir bei jambit Sie gerne dabei, wie Sie Cloud-, Daten-, Security- und Plattformstrategien in der Energiewirtschaft sicher, kontrolliert und zukunftsfähig umsetzen können. Haben Sie Fragen zu konkreten Punkten aus diesem Whitepaper? Suchen Sie einen erfahrenen Partner für die Modernisierung Ihrer digitalen Plattformen, Datenarchitekturen oder Cloud-Landschaften? Kontaktieren Sie uns und lassen Sie uns in den persönlichen Austausch gehen.

In einem unverbindlichen Beratungstermin klären wir gemeinsam mit Ihnen Ihre Fragestellungen rund um souveräne Cloud-Transformation, digitale Plattformen, Datenarchitekturen, Security-by-Design und moderne Betriebsmodelle.

Mehr über unsere Leistungen für Energieversorger, Netzbetreiber und energienahe Infrastrukturunternehmen erfahren Sie auf der jambit Webseite.

Warum warten?

Nutzen Sie die Gelegenheit und sichern Sie sich kompetente Beratung für Ihre digitalen Transformations- und Softwareprojekte.

Unser Experte steht Ihnen gerne zur Verfügung. Wir freuen uns über Ihre Nachricht. Einfach QR-Code scannen oder über diesen Link Kontakt aufnehmen.

Gemeinsam erreichen wir 100 % Begeisterung!

IMPRESSUM

Über jambit

jambit ist ein innovatives Softwareunternehmen mit Sitz in München, Stuttgart, Leipzig, Erfurt und Jerewan/Armenien. Seit 1999 entwickeln wir maßgeschneiderte Softwarelösungen, die exakt auf die individuellen Bedürfnisse unserer Kunden abgestimmt sind. Wir arbeiten eng mit namhaften Kunden aus verschiedenen Branchen zusammen, darunter die Automobilindustrie, Medien, Finanzen, Industrie und Energie. Unsere Expertise umfasst Beratung, Konzeption und Entwicklung mit modernsten Technologien. Auf der Mission nach 100 % Begeisterung!

Publikationshinweis

Diese Publikation stellt eine allgemeine, unverbindliche Information dar. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf Richtigkeit, Vollständigkeit und/oder Aktualität. Insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung der Leserschaft. Jegliche Haftung wird ausgeschlossen.

Auf eine Tasse Kaffee! Lassen Sie uns bei einem guten Kaffee über Ihre Softwareprojekte sprechen. Einfach QR-Code scannen und persönlich Kontakt aufnehmen.

jamb.it/souveräne-cloud

Herausgeber

jambit GmbH
Friedenheimer Brücke 20
80639 München
Tel.: +49.89.45 23 47 - 0
Fax: +49.89.45 23 47 - 70
E-Mail: office@jambit.com

Co-CEO: Franz Haßlberger,
Thomas Rottach
Beirat: Peter F. Fellinger,
Markus Hartinger

Umsatzsteuer-ID: DE205045965
Handelsregisternummer:
Amtsgericht München, HRB 129139

Datum der Veröffentlichung

Mai 2026