Der Microsoft-365-Ausfall vom 12. November 2026 – Eine Beleuchtung der Situation

---

1. Anlass und Einordnung

Am Donnerstag, den 12. November 2026 gegen 16:17 Uhr (UTC) begann ein weltweiter Ausfall von Microsoft 365 und zugehörigen Cloud-Diensten. Der Ausfall dauerte über 21 Stunden und betraf 74 Länder. Er ist ein Lehrbeispiel für die strukturellen Risiken, die mit der zunehmenden Abhängigkeit von wenigen privaten Cloud-Anbietern einhergehen – und für die Frage, was das für eine funktionierende Gesellschaft und Demokratie bedeutet.

---

2. Was technisch passiert ist

Die Ursache

Ein geplantes Netzwerk-Upgrade (also eine Änderung der Verbindungsinfrastruktur zwischen Servern) wurde durchgeführt. In Kombination mit einer späteren Änderung an der Netzwerkkonfiguration wurde ein interner Prozess überlastet, der dafür sorgt, dass Server-Verbindungen stabil bleiben. Die betroffenen Server fielen daraufhin bei automatisierten Gesundheitsprüfungen durch – also bei regelmässigen automatisierten Tests, die prüfen, ob ein Server noch ordnungsgemäss arbeitet – und wurden aus dem Betrieb genommen. Die verbleibenden Server konnten die zusätzliche Last nicht tragen. Das Ergebnis: eine kaskadierende Überlastung, die sich weltweit ausbreitete.

Wichtig: Kein Cyberangriff

Microsoft hat ausdrücklich betont, dass es sich nicht um einen Hackerangriff, keine KI-Beteiligung und keinen ungewöhnlichen Datenanstieg handelte. Es war ein Betriebsunfall – vergleichbar mit einem Stromausfall durch einen Transformatorfehler, nur in digitaler Form.

Die Reaktionszeit

Microsoft hat erst nach Stunden die Ursache umgedeutet und erst in der Nacht den Rückbau der fehlerhaften Änderung eingeleitet. Die Wiederherstellung erfolgte bewusst langsam und gestaffelt, um eine erneute Instabilität zu vermeiden – was die Gesamtdauer unnötig verlängerte.

---

3. Das Ausmass

Betroffene Dienste	E-Mail (Outlook), Videokonferenzen (Teams), Dateiablage (SharePoint, OneDrive), KI-Assistent (Copilot), Sicherheitssoftware, Datenanalyse (Power BI) und weitere
Geografischer Umfang	74 Länder, ca. 130'000 Störungsmeldungen auf der Überwachungsplattform Downdetector

Dauer	Über 21 Stunden, allmähliche Erholung ab Freitagnachmittag
Betroffene Organisationen	Regierungen (u. a. US-Repräsentantenhaus, japanische Behörden, australischer Geheimdienst), Krankenhäuser, Gerichte, Polizei, Fluggesellschaften, Börsen
Geschätzter wirtschaftlicher Schaden	Ca. 7 Milliarden US-Dollar Produktivitätsverlust (Schätzung der Anderson Economic Group)
Erstattungspflicht	Microsoft muss geschätzungsweise ca. 800 Millionen US-Dollar pro Tag an Abo-Gebühren erstatten

4. Cloud vs. eigene Infrastruktur: Sicherheit im Vergleich

Was «Cloud» und «On-Premise» bedeutet

- **Cloud Computing:** Rechnerleistung, Speicher und Software werden von einem externen Anbieter (z. B. Microsoft, Amazon, Google) betrieben. Man mietet die Leistung, statt eigene Server zu kaufen und zu warten.
- **On-Premise** (von engl. «on premises» = auf dem eigenen Gelände): Die eigene Organisation betreibt die Server in einem eigenen Rechenzentrum und hat die volle Kontrolle über Hardware, Netzwerk und Daten.

Die Sicherheitslage in Zahlen

Metrik	**On-Premise**	**Public Cloud**
Durchschnittliche Kosten eines Datenlecks	4,56 Mio. US-Dollar	5,38 Mio. US-Dollar
Durchschnittliche Zeit bis zum Eindämmen eines Angriffs	244 Tage	251 Tage
Anteil an allen Datenlecks	30 %	23 %

Cloud-Datenlecks kosten also rund 18 % mehr und dauern länger.

Was für die Cloud spricht

- **Ressourcen:** Grosse Anbieter beschäftigen Dutzende Sicherheitsspezialisten rund um die Uhr, patchen automatisch und können sich Technologien leisten, die sich kleine Unternehmen nie leisten könnten.
- **Redundanz innerhalb der Cloud:** Ein einzelner Serverausfall wird abgefangen, weil die Daten über mehrere Rechenzentren auf verschiedenen Kontinenten verteilt sind.
- **Patch-Disziplin:** Kleine Unternehmen patchen eigene Server oft monatelang zu spät. Die Cloud zentralisiert diese Aufgabe.

Was gegen die Cloud spricht

- **Konzentrationsrisiko:** Die fünf grössten Anbieter hosten Assets von 75 % aller Organisationen. Wer nur einen Anbieter nutzt, hat eine vierfach höhere Angriffsfläche als diversifizierte Unternehmen.
- **Identität als Schwachstelle:** 70–83 % der Cloud- und SaaS-Eindringungen laufen über kompromittierte Zugangsdaten. Der klassische «Netzwerk-Perimeter» (die Firewall am Rand) wurde durch das Identitätssystem ersetzt – und Identität ist schwerer zu schützen.
- **Fehlkonfiguration:** 31 % der Cloud-Datenlecks entstehen durch einfache Bedienfehler bei der Einrichtung.
- **Keine physische Trennung:** In der Cloud können Daten nicht physisch vom Internet getrennt werden (sogenanntes Air-Gap). Für besonders sensible Daten (Regierung, Verteidigung) ist das ein qualitativ anderer Sicherheitsverlust.

Fazit zur Sicherheit

Der Sicherheitsvorteil der Cloud ist primär ein Ressourcen-Vorteil: Er gilt für Organisationen, die eigene Infrastruktur nicht professionell betreiben können. Für eine gut unterhaltene On-Premise-Struktur – mit funktionierendem Patch-Management, Zwei-Faktor-Authentifizierung, Netzwerksegmentierung und Backup – kippt die Rechnung: Man behält die physische Kontrolle, hat keinen Single Point of Failure auf Anbieter-Ebene und ist nicht vom Internet als Abhängigkeit abhängig.

---

5. Strukturelle Kritik: Monopol, Abhängigkeit, Resilienz

Das Asymmetrie-Problem

Das ist der Kern des Problems: Das Risiko ist ungleich verteilt.

- Microsofts Risiko endet bei einem Service-Credit – einem kleinen Nachlass auf die Abo-Gebühr.
- Das Risiko eines Kleinunternehmers endet bei Lohnkosten, Miete, verfallenen Aufträgen, Kreditwürdigkeit – im schlimmsten Fall bei der Insolvenz.

Ein konkretes Beispiel aus dem Ausfall: Ein australisches Kleinunternehmen schätzte den Verlust für einen einzigen Tag auf mindestens 30'000 australische Dollar – bei schmaler Marge.

Die Zirkel-Falle

Der Ausfall führt paradoxerweise zu mehr Abhängigkeit: Unternehmen kehren nicht zur eigenen Infrastruktur zurück, sondern kaufen noch mehr Business-Continuity-Tools vom selben Anbieter. Das ist ein Teufelskreis: Ausfall → mehr Vertrauen in den Anbieter → mehr Abhängigkeit → höheres Risiko beim nächsten Ausfall.

Die Externalisierung des Risikos

Der Anbieter internalisiert die Gewinne (Abo-Einnahmen), die Gesellschaft trägt die Ausfallkosten (Produktivitätsverlust, Insolvenz, gestörte kritische Dienste). Das ist ein klassisches Muster: Der Profit bleibt privat, das Risiko wird auf die Allgemeinheit abgewälzt – vergleichbar mit Umweltverschmutzung, nur in digitaler Form.

Der fehlende regulatorische Rahmen

Es gibt keine Sicherheitsvorschriften für digitale Infrastruktur, die denen für Energieversorger oder Bahnen entsprechen würden. Kein Redundanz-Zwang, keine Meldepflicht bei Ausfällen, keine Haftungsbeschränkung. Ein Energieversorger, der eine Region tagelang ohne Strom lässt, würde regulierend belangt. Ein Cloud-Anbieter, der 74 Länder lahmlegt, zahlt einen Service-Credit.

Die Souveränitätsfrage

Nur 20 % der europäischen digitalen Dienste laufen auf europäischer Infrastruktur. Die EU-Institutionen haben den Ausfall unbeschadet überstanden – weil sie eigene Infrastruktur betreiben. Für die übrigen europäischen Organisationen, die auf US-Infrastruktur angewiesen sind, gab es dieses Sicherheitsnetz nicht: Sie waren in hohem Masse verwundbar und hatten keine eigenständige Handlungsoption.

---

6. Der demokratische Aspekt

Demokratie setzt funktionierende Infrastruktur voraus

Wahlen, parlamentarische Arbeit, Justiz, öffentliche Sicherheit, Pressefreiheit, Bürgerkommunikation – all das läuft heute über dieselbe Schicht, die Microsoft betreibt. Wenn das ausfällt, fällt nicht ein «Dienst» aus, sondern die Handlungsfähigkeit der demokratischen Institutionen selbst.

Vier demokratiepolitische Probleme

1. **Keine Rechenschaft:** Ein privater Anbieter, der systemrelevante Infrastruktur betreibt, unterliegt keiner demokratischen Kontrolle. Es gibt keine Institution, die Microsoft zur Rechenschaft ziehen kann, wenn 74 Länder betroffen sind – weil die Jurisdiktion fragmentiert ist und der Anbieter über der nationalen Ebene agiert.
2. **Kein «Exit»:** Bürger und Unternehmen können nicht «mit den Füssen abstimmen». Die Wechselkosten sind so hoch, dass die praktische Wahl zwischen drei Anbietern keine echte Wahl ist. Das ist strukturell ein Monopol ohne demokratische Kontrolle.
3. **Informationsasymmetrie:** Der Anbieter weiss, was im System passiert. Die Öffentlichkeit, die Regierung, die betroffenen Unternehmen wissen es nicht. Das untergräbt die Voraussetzung, dass Bürger und Institutionen informierte Entscheidungen treffen können.
4. **Private Governance über öffentliches Leben:** Wenn 80% der Kommunikation, Kollaboration und Identitätsverwaltung über Plattformen laufen, die privaten Eigentümern gehören, üben diese faktisch Governance-Funktionen aus – ohne Wahl, ohne Transparenz, ohne Rechtsstaatlichkeit. Der Ausfall zeigt, dass diese Governance fragil ist.

Die zentrale Frage

Kann eine Gesellschaft, die ihre demokratischen und lebenswichtigen Funktionen auf ein privates Oligopol auslagert, noch als demokratisch bezeichnet werden? Die *formale* Demokratie bleibt intakt (Wahlen finden statt, Parlamente tagen). Aber die *materielle* Demokratie – die Fähigkeit der Institutionen, unabhängig von privaten Akteuren zu funktionieren – ist

untergraben. Und zwar nicht durch einen Angriff, sondern durch die logische Konsequenz des Modells: Je tiefer die Einbettung, desto höher die Abhängigkeit, desto geringer die Handlungsfähigkeit des öffentlichen Sektors.

Das ist die Beobachtung, dass strukturelle Bedingungen, die auf Gewinnmaximierung und Kostenminimierung optimiert sind, demokratische Voraussetzungen (Unabhängigkeit, Redundanz, Rechenschaft, Souveränität) systematisch aushöhlen.

---

7. Alternativen: Wege aus der Abhängigkeit

Der Ausfall zeigt: Abhängigkeit ist eine konkrete Gefahr und ein messbares Risiko. Es existieren jedoch funktionsfähige Alternativen – für verschiedene Nutzergruppen, mit verschiedenen Voraussetzungen und verschiedenen Kosten. Sie sind kein Allheilmittel, aber sie zeigen, dass die Abhängigkeit nicht unvermeidlich ist.

7.1 Linux als Betriebssystem (Workstations und Server)

Linux ist ein freies, offen gebautes Betriebssystem, das seit über 30 Jahren existiert und in der Industrie weitverbreitet eingesetzt wird. Über zwei Drittel der Rechenkerne in Microsofts eigener Azure-Cloud laufen auf Linux, nicht auf Windows.

Für Workstations (Arbeitsplätze):

- Ubuntu, Fedora, Linux Mint sind die geläufigsten Distributionen für den Alltagsgebrauch. Sie bieten ein grafisches Arbeitsumfeld, das für die meisten Büroaufgaben (Textverarbeitung, Tabellenkalkulation, E-Mail, Web) voll ausreicht.
- Red Hat Enterprise Linux Workstation richtet sich an Unternehmen, die professionellen Support benötigen.
- Einschränkung: Proprietäre Windows-Anwendungen (z. B. bestimmte Branchensoftware) laufen nicht nativ. Mögliche Lösungen: Virtualisierung, Remote-Desktop auf Windows-Servern, oder in vielen Fällen existierende Open-Source-Alternativen.

Für Server:

- Ubuntu Server, Debian, RHEL (Red Hat Enterprise Linux), Rocky Linux, AlmaLinux sind die Standard-Serverdistributionen. Sie sind stabil, sicher und für den 24/7-Betrieb ausgelegt.
- Fast jede Serverrolle, die Windows Server übernimmt, lässt sich mit Open-Source-Software ersetzen:

Serverrolle	**Open-Source-Alternative**	**Einschätzung**
Dateiserver	Samba, Nextcloud	Gut ersetzbar
DNS	BIND, Unbound, PowerDNS	Gut ersetzbar
DHCP	Kea	Gut ersetzbar
Webserver (IIS)	nginx, Apache	Gut ersetzbar

Mailserver (Exchange)	Stalwart, Mail-in-a-Box	Gut ersetzbar
Druckserver	CUPS	Bedingt
Datenbankserver	PostgreSQL, MariaDB	Bedingt (abhängig von der Anwendung)
Domain-Controller (Active Directory)	Samba, Zentyal, NethServer	Bedingt

7.2 Open-Source-Office-Suiten (Alternative zu Microsoft 365)

Tool	Lizenz	Deployment	Stärkste Eigenschaft
LibreOffice	MPL-2.0 (frei)	Desktop (Win/Mac/Linux)	Vollständige Büro-Suite, komplett kostenlos, kein Nutzerlimit
ONLYOFFICE	AGPL-3.0 (frei)	Desktop, Cloud, Self-Hosted	Sehr hohe Kompatibilität mit Word/Excel/PowerPoint, Echtzeit-Kollaboration
Collabora Online	MPL-2.0 (frei)	Cloud, Self-Hosted	Browserbasierte Kollaboration auf LibreOffice-Basis, Standard-Editor für Nextcloud
CryptPad	AGPL-3.0 (frei)	Cloud, Self-Hosted	Ende-zu-Ende-verschlüsselte Kollaboration, null-Wissen-Architektur
Nextcloud + Office-Integration	AGPL-3.0 (frei)	Self-Hosted	Vollständiger Self-Hosted-Stack: Dateien, Kalender, Kontakte, E-Mail, Büro

7.3 Self-Hosted-Stacks (eigene Infrastruktur)

Für Organisationen, die volle Datenhoheit wollen, existieren fertige Self-Hosted-Lösungen:

- **Nextcloud** (Deutschland): Dateiablage, Kalender, Kontakte, E-Mail, Videokonferenzen, Büro – alles auf eigenen Servern. Ab 100 Nutzern offizieller Support.
- **openDesk** (Deutschland): Von der Bundesregierung initiierte, souveräne und selbst hostbare Arbeitsplatz-Suite aus Nextcloud, Element (Chat), OpenProject und Collabora. Auf Kubernetes-basiert, ausserhalb der Reichweite des US CLOUD Act.
- **Mail-in-a-Box / Stalwart Mail Server:** Vollständige E-Mail-Server, die Microsoft Exchange ersetzen können.
- **Zentyal / NethServer:** Linux-Server-Distributionen mit grafischer Verwaltungsoberfläche, die Windows Server (Domain-Controller, Dateiserver, DNS, DHCP) ersetzen – ab ca. 230 USD/Jahr für kleine Organisationen.

7.4 EU-Souveräne Cloud-Anbieter (Alternative zu Azure, AWS, GCP)

Für Organisationen, die Cloud-Dienste weiterhin nutzen, aber nicht von US-Anbietern abhängig sein wollen, existieren europäische Anbieter, die unter EU-Recht stehen und dem US CLOUD Act nicht unterliegen:

Anbieter	Land	Besonderheit
OVHcloud	Frankreich	Grosse europäische Cloud, SecNumCloud-zertifiziert (französische Öffentlichkeit), breites Dienstespektrum
Hetzner	Deutschland	Preis-Leistung, dedizierte Server und Cloud-Instanzen, sehr beliebt bei KMU
Scaleway	Frankreich	Developer-freundlich, GPUs für KI-Workloads, gewann 2026 einen 180-Mio.-EUR-EU-Souveränitäts-Auftrag
IONOS	Deutschland	Paketlösungen für KMU (Hosting + Arbeitsplatz), S3-kompatibler Objektspeicher
STACKIT (Schwarz-Gruppe)	Deutschland	Managed Kubernetes, für den deutschen öffentlichen Sektor
Exoscale	Schweiz	Schweizer Jurisdiktion, starke Datenschutzlage
UpCloud	Finnland	Speicherperformance, für datenintensive Anwendungen

Wichtiger Hinweis zu den «Sovereign Cloud»-Angeboten der US-Hyperscaler: Auch wenn AWS (European Sovereign Cloud, seit Januar 2026 in Brandenburg), Microsoft (EU Data Boundary, seit Februar 2025) und Google (Sovereign Controls) «souveräne» Angebote für Europa machen, bleiben sie rechtlich Tochtergesellschaften US-amerikanischer Mutterkonzerne. Der US CLOUD Act – ein Gesetz, das US-Behörden erlaubt, Daten von US-Unternehmen weltweit einzufordern – gilt weiterhin. Der französische Generalanwalt von Microsoft hat vor dem französischen Senat ausdrücklich zugegeben, dass Microsoft nicht garantieren kann, dass EU-Daten vor CLOUD-Act-Anfragen sicher sind. Echte Souveränität bedeutet daher: EU-Eigentum, EU-Jurisdiktion, EU-Personal.

7.4.1 Schweiz-souveräne Cloud-Anbieter

Die Schweiz hat in dieser Hinsicht sogar eine besonders starke Position, weil sie weder dem US CLOUD Act noch EU-Recht unterliegt und die EU sie als datenschutzäquivalent anerkennt.

Anbieter	Sitz	Besonderheit
Infomaniak	Genf / Zürich	100 % Mitarbeitenden-eigen, Open-Source-basiert, Daten ausschliesslich in der Schweiz, Fokus auf Nachhaltigkeit
Exoscale	Lausanne (A1 Digital)	Kubernetes-first, 7 Rechenzentren (u. a. Genf, Zürich), Managed Databases, GPU-Instanzen für KI
Safe Swiss Cloud	Zürich	Spezialisiert auf sicherheitskritische Branchen (Finanz, Gesundheitswesen), ISO 27001, FINMA/BAFIN-konform
Hikube (Hidora SA)	Genf	Kubernetes-native Private Cloud, 3 physisch getrennte Rechenzentren (Genf, Gland, Luzern), synchrone Replikation
cloudscale.ch	Basel	100 % in Schweizer Besitz, OpenStack-basiert, Self-Service

Xelon	Zürich	User-freundlich, Windows und Linux, Fokus auf KMU und IT-Dienstleister
ELCA / EveryWare	Bern	Teil der ELCA Group, 6 Availability Zones über zwei Regionen (FR/DE), Teil des «Netzwerk für eine souveräne digitale Schweiz»
VSHN	Zürich	Schweizer AG, alle Aktionäre Schweizer Staatsangehörige, Managed Kubernetes, SEAL-3-Äquivalent nach EU-Framework
Swisscom	Bern	Sovereign Kubernetes Service (seit 2025), 390 Cluster in Produktion, Open-Source-basiert
CONVOTIS	Zürich	Managed Private & Sovereign Cloud in zertifizierten Schweizer Rechenzentren
Swiss Government Cloud (SGC)	Bund (FOITT)	Staatliche Hybrid-Multi-Cloud (2025–2032), für Bund, Kantone und Gemeinden

Wichtig: Seit Januar 2026 gelten in der Schweiz **verbindliche E-Government-Standards**, die für den öffentlichen Sektor und KRITIS-Betreiber eine «Bring Your Own Key»-Verschlüsselung vorschreiben – der Cloud-Anbieter hat technisch keinen Zugriff mehr auf die Daten. Das ist eine der strengsten Sovereign-Cloud-Vorgaben weltweit.

Der Unterschied zu «souveränen» US-Anbietern: Auch wenn Azure, AWS oder Google eigene Schweizer Regionen betreiben, unterliegen sie weiterhin dem US CLOUD Act. Echte Schweizer Souveränität bedeutet: Schweizer Eigentum, Schweizer Recht, Schweizer Personal – und kein ausländisches Gesetz, das Datenzugriff erzwingen kann.

7.5 Was realistisch ist – und was nicht

Ein vollständiger Wechsel von Microsoft 365 auf Open Source ist für grosse Organisationen mit tiefen Integrationsketten (z. B. Active Directory, Exchange, SharePoint, Teams, Power BI, Dynamics 365) ein Projekt mit Monaten bis Jahren Dauer. Es ist aber kein «Alles-oder-Nichts»:

- **Einfach zu ersetzen:** Büroanwendungen (LibreOffice/ONLYOFFICE), Dateiablage (Nextcloud), E-Mail (Stalwart), Videokonferenzen (Jitsi Meet), Chat (Element/Matrix), Kalender (Nextcloud CalDAV/CardDAV).
- **Mittlere Komplexität:** Identity-Management (FreeIPA, Keycloak), Domain-Controller (Samba/Zentyal), Webserver (nginx/Apache).
- **Schwierig zu ersetzen:** Proprietäre Branchensoftware, tiefe Microsoft-Integrationen (z. B. Dynamics 365, Power Automate), einzelne Windows-spezifische Anwendungen (Lösung: Virtualisierung oder Remote-Desktop).

Der pragmatische Ansatz lautet: Nicht «Cloud vs. On-Premise», sondern Redundanz und Wahlrecht. Welche Workloads wirklich in der Cloud sein müssen und welche lokal bleiben können, ist eine bewusste Entscheidung – nicht ein technisches Schicksal.

---

8. Was jetzt passiert (und was passieren wird)

Zeithorizont	Erwartete Folgen
Kurzfristig	Ca. 7 Mrd. USD Produktivitätsverlust; 26–51 Mio. tatsächlich betroffene Nutzer; Microsoft muss ~800 Mio. USD/Tag an Abo-Gebühren erstatten
Mittelfristig	Kleinbetriebe mit schmaler Marge und ohne Kontinuitätsplan gehen in Insolvenz oder Liquiditätskrise; gestörte kritische Dienste (Gesundheit, Justiz, Sicherheit)
Strukturell	Der Vorfall verstärkt die Abhängigkeit weiter (Teufelskreis); gleichzeitiger Druck auf Regierungen, Sovereign-Cloud-Optionen und Interoperabilitätsstandards zu fordern

Der ausstehende Post-Incident-Report

Microsoft hat einen detaillierten Nachbericht angekündigt, der die genaue Abfolge der Ereignisse, die Reaktionszeiten und die Massnahmen zur Vermeidung ähnlicher Vorfälle dokumentieren soll. Dieser Bericht wird das eigentliche Mass für die Glaubwürdigkeit der Reaktion sein.

---

9. Fazit

Der Ausfall vom 12. November 2026 war kein Sicherheitsvorfall, sondern ein ernsthafter Betriebsunfall mit systemischem Ausmass. Er ist kein Einzelfall, sondern die vorhersehbare Konsequenz einer Struktur, in der:

- systemrelevante Infrastruktur in die Hände eines Oligopols (3–4 Anbieter) fällt,
- das Risiko asymmetrisch verteilt ist (privater Gewinn, öffentliches Risiko),
- es keinen regulatorischen Rahmen gibt, der Redundanz und Rechenschaft erzwingt,
- die demokratischen Institutionen ihrer operativen Unabhängigkeit beraubt werden.

Die Frage, die sich stellt, ist nicht «Sollte Microsoft besser patchen?», sondern: **Wer trägt das Risiko, wenn die digitale Infrastruktur ausfällt – und warum ist es so ungleich verteilt?**

Die pragmatische Antwort, die in der Debatte zunehmend Gehör findet, lautet: Nicht «Cloud vs. eigene Infrastruktur», sondern Redundanz zwischen Anbietern, Datenhoheit über europäische Cloud-Optionen, Open-Source-Alternativen dort, wo sie funktional ausreichen, und die bewusste Entscheidung, welche Aufgaben wirklich in der Cloud sein müssen und welche lokal bleiben können.

Der Ausfall ist eine Chance, diese Fragen nicht nur theoretisch zu diskutieren, sondern konkret zu beantworten. Die Alternativen existieren. Die Frage ist die politische Willensbildung, sie zu nutzen.

Stand: 13. November 2026. Der Post-Incident-Report von Microsoft steht noch aus.