Microsoft

Schweiz Dunkel – wie Teams (+M365) weiterläuft, wenn nichts mehr läuft

DVS Onevoice, 17. Juni 2026

Cyril Hollenstein
Senior Account Technology Strategist · Public Sector Schweiz

Jürg Stadelmann
Senior Cloud Solution Architect

Das Szenario

"Schweiz Dunkel" — Strom, Festnetz, Mobilfunk gleichzeitig.

0 h

Stromausfall

Wenige Stunden

Garantierte Telco-Autonomie endet

Wenige Tage

Strukturelle BORS-Schicht

Risikoeinordnung

KNS 2025 (BABS): Strommangellage ist eines der zwei grössten Landesrisiken.
Quelle: BABS, 02.03.2026

Kommerzielle Netze

SR 784.101.1 (FDV) : Mobilfunktanbieter müssen im minimum 4h Stromautonomie garantieren.

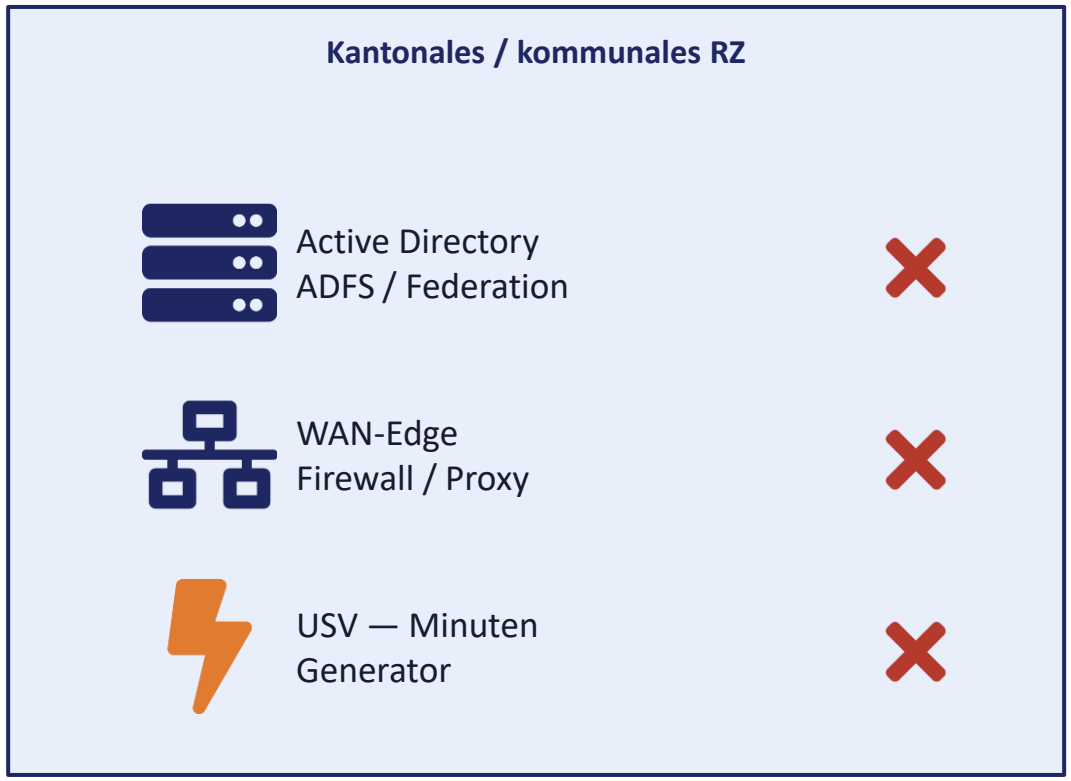
Strukturelle Antwort

Polycom (~60.000 BORS-Nutzer),
SDVN+ (14 Tage Notstrom),
MSK in Aufbau.

Wer ist der Meinung, dass die heutige Infrastruktur für die **organisationsübergreifende** Krisenkommunikation und Zusammenarbeit im Schweiz Dunkel Szenario durchgängig funktioniert?

Warum klassische On-Prem-IT zuerst kippt

Drei Bruchstellen — alle innerhalb der Schweizer Ausfallzone.



1

Strom

USV-Autonomie ist typisch minuten-, nicht tagesbemessen. Generatoren brauchen Dieselversorgung — Tankstellen hängen am Strom.

2

WAN / Internet

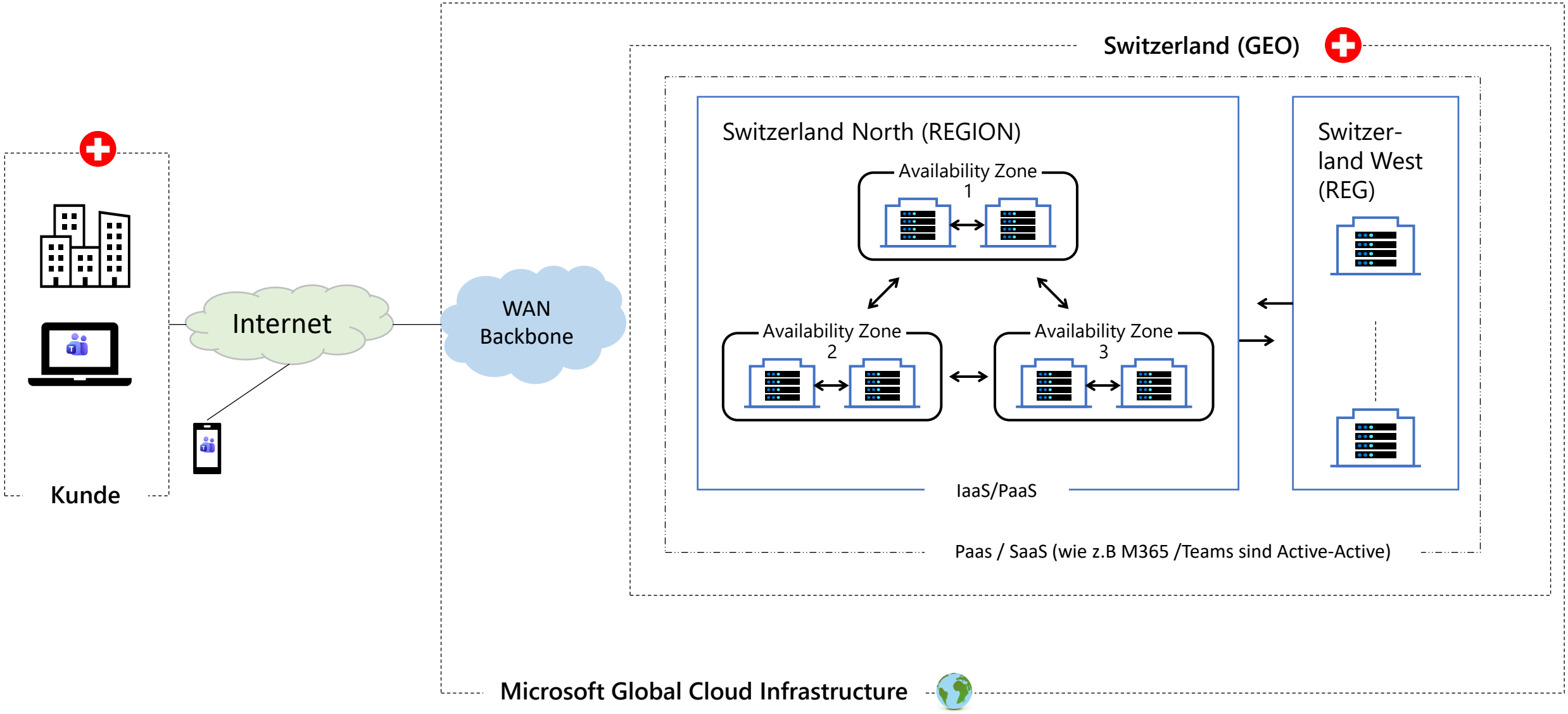
Der Internet-Übergabepunkt der Verwaltung sitzt beim lokalen Carrier — derselbe Carrier, dessen Mobilfunk- und Festnetzschicht ausfällt.

3

Identitäts-Edge

ADFS, Federation und alle on-prem-IdPs sind mit dem RZ tot. Authentifizierung an die Cloud — wenn überhaupt erreichbar — bricht.

Grundlagen Cloud Architektur



Microsoft

Microsoft global infrastructure

80+

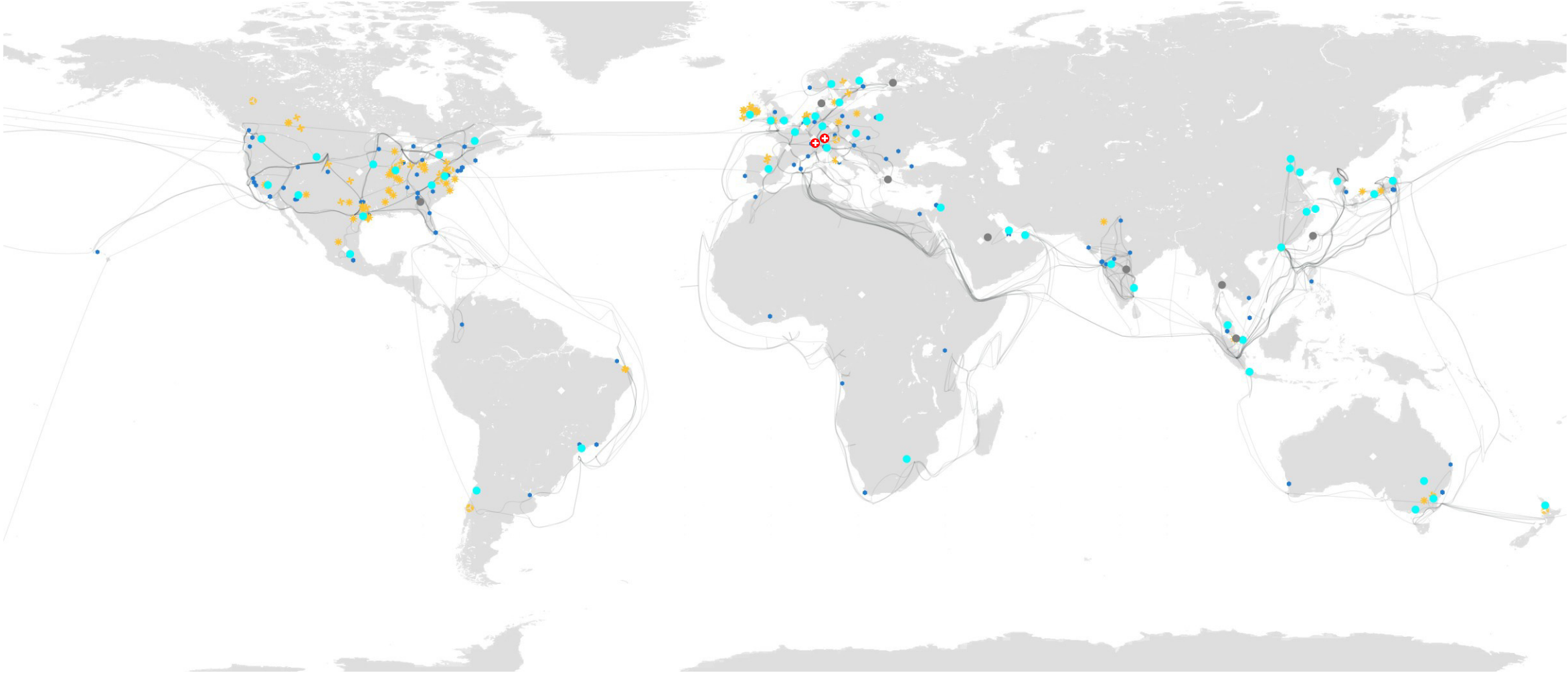
Azure regions

500+

Datacenters

Teams (und M365) ist ein globaler Dienst

Teams läuft verteilt, über anycast- und/oder GeoDNS gerouted, regional gespiegelt und mit Failover Mechanisms ausserhalb der Region, wo erlaubt/vorgesehen



Microsoft Azure Backbone-Architektur — https://datacenters.microsoft.com/globe/explore?view=globe

Resilienz by Design - Teams

Active-Active Multi-Region — Microsoft-managed, kein Kunden-Failover.

Innerhalb einer Region

Active-Active über mehrere Verfügbarkeitszonen

Datacenter sind redundant gepaart; ein Ausfall eines Standorts wird automatisch absorbiert.

Lastverteilung anycast / DNS-gesteuert

Clients verbinden sich zum nächsten gesunden Front-End — Re-Routing geschieht im Hintergrund.

Daten mehrfach repliziert

Chats, Channel-Nachrichten und Dateien sind synchron innerhalb der Region gehalten.

Zwischen Regionen

Cross-Region-Replikation für Kerndienste

Kontinuierliche, asynchrone Spiegelung über Regions-Grenzen — schützt vor regionalen Vorfällen.

Failover ohne Kundeneingriff

Microsoft steuert das Routing — keine Runbooks, kein DR-Drill auf Kundenseite.

Vertraglich: 99,9–99,999 % SLA

Microsoft veröffentlicht keine RTO/RPO pro Workload — nur die finanziell hinterlegte Verfügbarkeit.

Beispiele:

Schadenorganisation Erdbeben revolutioniert Krisenmanagement mit Microsoft Azure | Microsoft Customer Stories

How technology helped Ukraine resist during wartime - CEE Multi-Country News Center

Identität trägt mit

Microsoft Entra ID — die Resilienzschicht, die der Nutzer nie sieht.

99,99 %

SLA-Ziel für die Authentifizierung

Mehrstufige Resilienz

Entra ID nutzt georedundante und resiliente Authentifizierungsdienste

Architektur entscheidet im Blackout

✓ **Cloud-only Entra ID**

Beste Resilienz, keine On-Prem-Abhängigkeit

✓ **Hybrid mit Password Hash Sync**

Cloud-Auth funktioniert auch bei totem On-Prem-AD

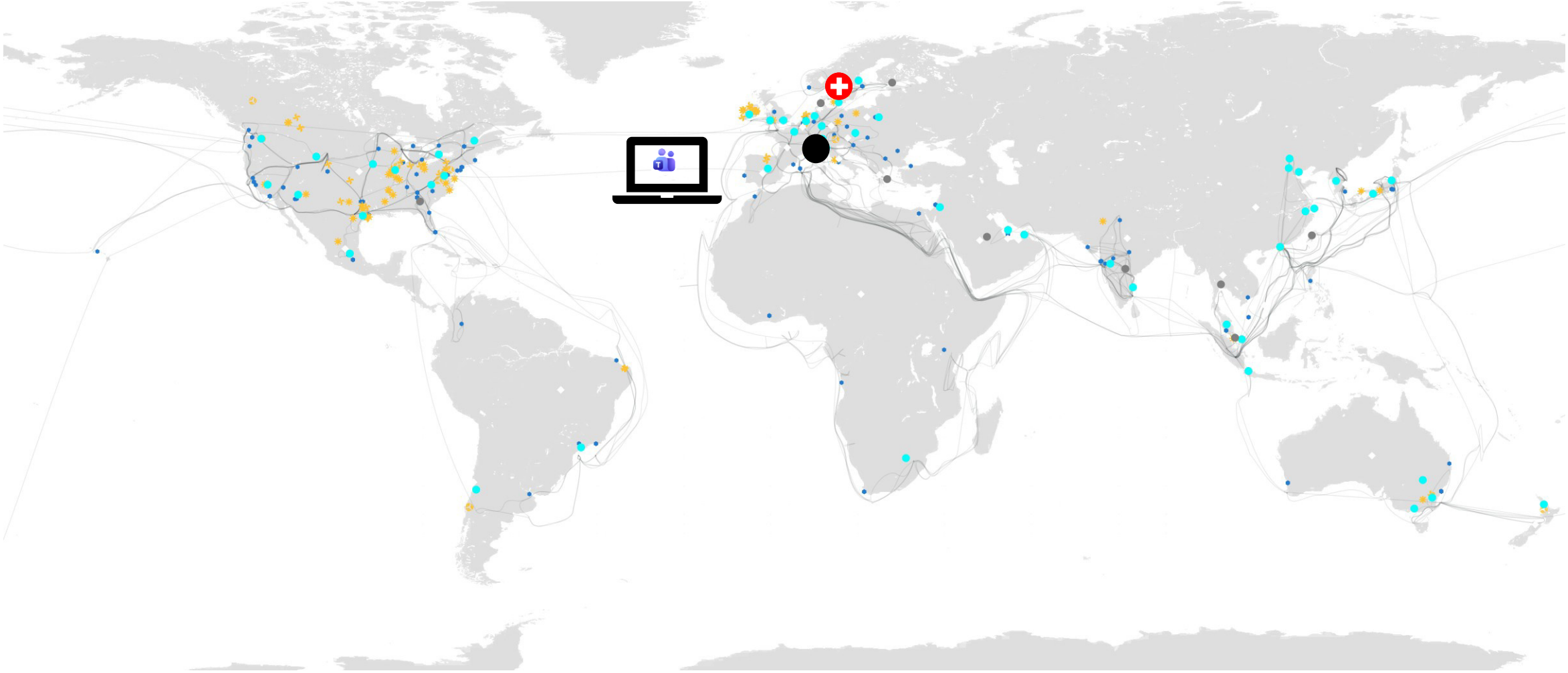
✗ **Pass-Through Authentication**

On-Prem-Agent unerreichbar — Auth bricht

✗ **Federation**

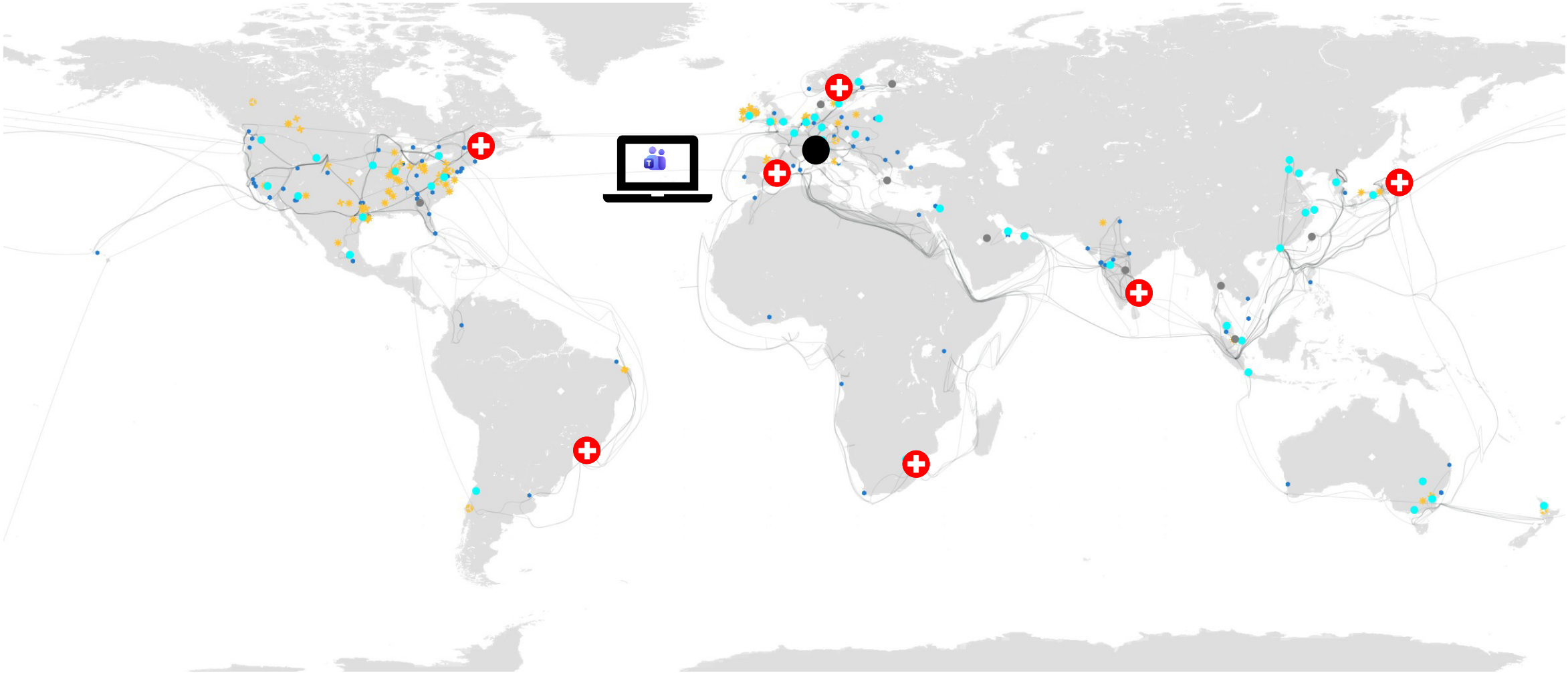
IdP im Ausfallgebiet — Auth bricht

Tenant-Strategie für den Notfall – Single Tenant



Microsoft Azure Backbone-Architektur — https://datacenters.microsoft.com/globe/explore?view=globe

Tenant-Strategie für den Notfall - Multitenant

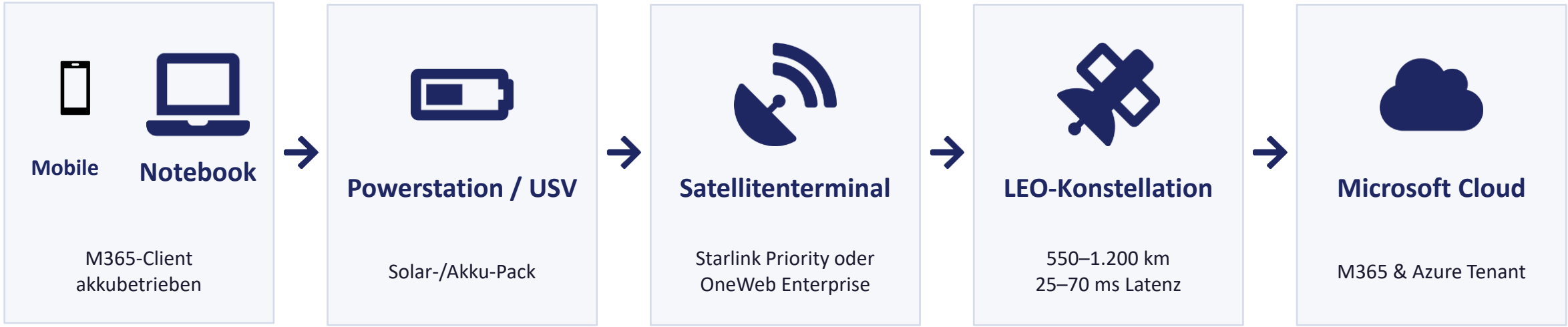


Microsoft Azure Backbone-Architektur — https://datacenters.microsoft.com/globe/explore?view=globe

Microsoft 365 inter-tenant collaboration - Microsoft 365 Enterprise | Microsoft Learn

Der Last-Mile-Plan – Sicht Infrastruktur Behördenkommunikation

Die Cloud läuft. Der Pfad zur Cloud ist das, was wir sicherstellen müssen.



Satcom-Tiering für Teams

Eine Klasse ersetzt nicht die andere — bewusste Schichten.

Operator	Orbit	Down / Up	Latenz	Eignung für Teams
Starlink Priority	LEO 550 km	135–310 / 20–44 Mbps	25–60 ms	**Chat, Files, Calling, Video — voll**
Eutelsat OneWeb	LEO 1.200 km	50–195 / 10–32 Mbps	30–70 ms	**Chat, Files, Calling, Video — voll, EU-Souverän**
Iridium Certus 700	LEO 780 km (L-Band)	704 / 352 Kbps	~395 ms	**Chat + Sprache, Out-of-Band-Lagekanal**
Inmarsat BGAN	GEO 36.000 km	bis 492 Kbps	600–1.500 ms	**Sprache + SMS, Notfall-IP**

Tier 1

Primärbackhaul für M365 inkl. Teams Audio/Video

Tier 2

Out-of-Band-Lagekanal und Notfall-Sprache

Tier 3

Sprache + SMS — letzte Resilienzschicht

Tenant-Notfall-Szenario

Ein Sekundär-Tenant ausserhalb der Schweiz als ‚digitale Ausweich-Location'.

Primär-Tenant (Verwaltung)

- Identitäten
  Alle Mitarbeitenden
- Tägliche Daten
  Teams/SharePoint/OneDrive
- Geo: Switzerland / EU-EFTA

B2B / Cross-Tenant Access

Integrierte Emergency-Tenant(s)

- Notfall-Identitäten
  Krisenstab + Schlüsselfunktionen
- Krisen-Lagebibliothek
  Kopien / Read-Replicas
- Geo: EU, Weltweit
  Ausserhalb CH-Ausfallzone

Autonome mergency-Tenant(s)

- Notfall-Identitäten
  Krisenstab /Schlüsselfunktionen
- Krisen-Lagebibliothek
  Kopien / Read-Replicas
- Geo: EU, Weltweit
  Ausserhalb CH-Ausfallzone

Wie es funktioniert

1. Pre-staging der Schlüsselrollen als Gäste im Emergency-Tenant über B2B-Federation.
2. Krisen-relevante Lagebibliotheken werden regelmässig in den Emergency-Tenant repliziert.
3. Im Notfall: via Satcom-Backhaul direkter Zugriff auf den Emergency-Tenant — bei Bedarf ohne Heim-Tenant-Round-Trip.

Architektur-Empfehlungen

Fünf Stellschrauben — alle vor dem Ereignis zu drehen.

1	**Identität sanieren**	Cloud-only Entra ID oder Hybrid mit Password Hash Sync. Federation aus dem kritischen Pfad.
2	**Tenant-Geographie bewusst wählen**	EU/EFTA-Default, Multi-Geo.
3	**Emergency-Tenant aufsetzen**	Sekundär-Tenant ausserhalb CH, B2B-Federation, regelmässige Replikation
4	**Last-Mile-Kit pre-stagen**	Powerstation/USV, Starlink Priority oder OneWeb Enterprise, Iridium als Out-of-Band, BAKOM-Bewilligungen.
5	**Üben**	Architektur ohne Drill ist Theorie. Mindestens einmal jährlich ein realer Last-Mile-Drill mit Stab und IT.

Die Cloud kippt nicht.

Der Pfad zur Cloud kippt.

Teams-Backbone

trägt — global, active-active

Last-Mile

Notebook + USV + Satellit + Cloud-only Identität.


OFF
ON

Over the past decade, Microsoft has invested extensively in data privacy, compliance and security

2016

- **Launched German sovereign cloud** with local trustee
- **Invested $3B to double European cloud capacity**
- **Challenged U.S. gag order** on customer data for transparency
- **30 Azure regions** live

2017

- **Committed to full GDPR compliance for all cloud services** by 2018 enforcement
- **Secured policy win** as U.S. Justice Department limited indefinite gag orders
- **Revised contracts and privacy controls** to support customer compliance

2018

- First major tech company to **apply GDPR data rights to customers globally**
- Met the **GDPR deadline**

2019

- Launched first cloud datacenters in Africa and the Middle East, enabling local data storage
- **Extended California's CCPA privacy rights to all U.S. customers,** adopting a "beyond compliance" stance
- **54 Azure regions** live

2020

- **Launched "Defending Your Data"** to legally oppose government data requests
- **Committed to compensation** if personal data is disclosed in violation of GDPR
- Reaffirmed **opposition to government encryption backdoors**

2021

- **Announced EU Data Boundary** for Microsoft Cloud
- Committed to **storing and processing all EU customer data within EU** datacenters by end of 2022

2022

- **Launched Microsoft Cloud for Sovereignty** with enhanced data residency, privacy, and compliance
- Introduced **Advanced Data Residency add-on**
- **60+ Azure regions** live
- Expanded Go Local program to **15 countries**
- Over **100 compliance certifications,** including **50+ region-specific ones**

2023

- **Launched EU Data Boundary Phase 1,** storing core customer data in European datacenters
- Expanded Go Local program to **25+ countries**

2024

- **Expanded EU Data Boundary** to Phase 2, adding pseudonymized personal data and telemetry in-region
- **Reduced data transfers outside the EU** by keeping Microsoft cloud service data and metadata within Europe

2025

- **Completed EU Data Boundary** (Phase 3) with all EU customer data in European datacenters
- **Announced expansion of Microsoft Sovereign Cloud to Public and Private cloud environments**
- **Launched** Bleu (France) and Delos (Germany) **national cloud providers**
- **Announced 5 European digital commitments**
- **Over 70 Azure regions** live
- **Invested $20B+ in European cloud infrastructure** since 2023

2026

Major milestone

Vertragsauszug (DPA) Microsoft<->Kunde

Anhang D – Anfechtung einer Anordnung oder einer verbindlichen rechtlichen Verpflichtung zur Aussetzung von Onlinediensten

Mit diesem Anhang geht Microsoft gegenüber nationalen, bundesstaatlichen und regionalen Behördenkunden der Mitgliedstaaten der Europäischen Union („EU“) sowie der EU-Beitrittsländer, der Mitglieder der Europäischen Freihandelsassoziation, des Vereinigten Königreichs, Monacos, des Vatikans und der Europäischen Kommission („Geschützte Behördenkunden“) die folgenden Verpflichtungen ein.

1. Für den Fall, dass gegenüber Microsoft eine Anordnung ergeht oder Microsoft anderweitig einer verbindlichen rechtlichen Verpflichtung einer staatlichen Stelle, Behörde, Kommission oder quasi-staatliche Einrichtung unterliegt, die Microsoft dazu verpflichtet, die Bereitstellung von Onlinediensten (einschließlich, aber nicht beschränkt auf die Bereitstellung von Microsoft Azure-Diensten, Microsoft Dynamics 365-Diensten oder Office 365-Diensten) für den Geschützten Behördenkunden ganz oder teilweise auszusetzen oder einzustellen, wird Microsoft im eigenen Namen und im Namen seiner verbundenen Unternehmen:
    a. alle verfügbaren Mittel einzusetzen, um die freiwillige Rücknahme, Aufhebung oder Rückgängigmachung einer solchen Anordnung zu erreichen; und
    b. alle rechtmäßigen Anstrengungen unternehmen, um die Anordnung vor den Gerichten des Lands anzufechten, dessen Behörde die Anordnung erlassen hat, und zwar auf der Grundlage von Rechtsmängeln nach dem Recht der anfordernden Partei oder von relevanten Konflikten mit dem Recht der Europäischen Union oder dem anwendbaren nationalen Recht der oben aufgelisteten Staaten.

    Microsoft wird bei Bedarf eine einstweilige oder dauerhafte Unterlassungsanordnung erwirken, um die kontinuierliche und ununterbrochene Bereitstellung der entsprechenden Onlinedienste sicherzustellen, bis eine rechtskräftige Entscheidung über die rechtmäßigen Anstrengungen zur Anfechtung der Anordnung oder der sonstigen oben genannten verbindlichen rechtlichen Verpflichtung ergangen ist.

https://www.microsoft.com/licensing/docs/documents/download/MicrosoftProductandServicesDPA(WW)(German)(September2025)(CR).docx

Lawful Access – Reality Check…

- Context **criminal prosecution** (!), independent judicial decision required as a basis, clearly defined framework conditions and processes.
- Law provides that providers can take legal action in case of violations of local laws of affected third countries. (see also "Gutachten des Bundesamts für Justiz - Bericht zum US CLOUD Act")
- No focus on enterprise organizations, or even on governments. Focus is on individual persons aka "consumers."
- No direct access, only the possibility to request providers…
- The "CLOUD Act" is not a US-specific law, it exists in many other countries in comparable form (e.g. e-Evidence, etc.)

Global

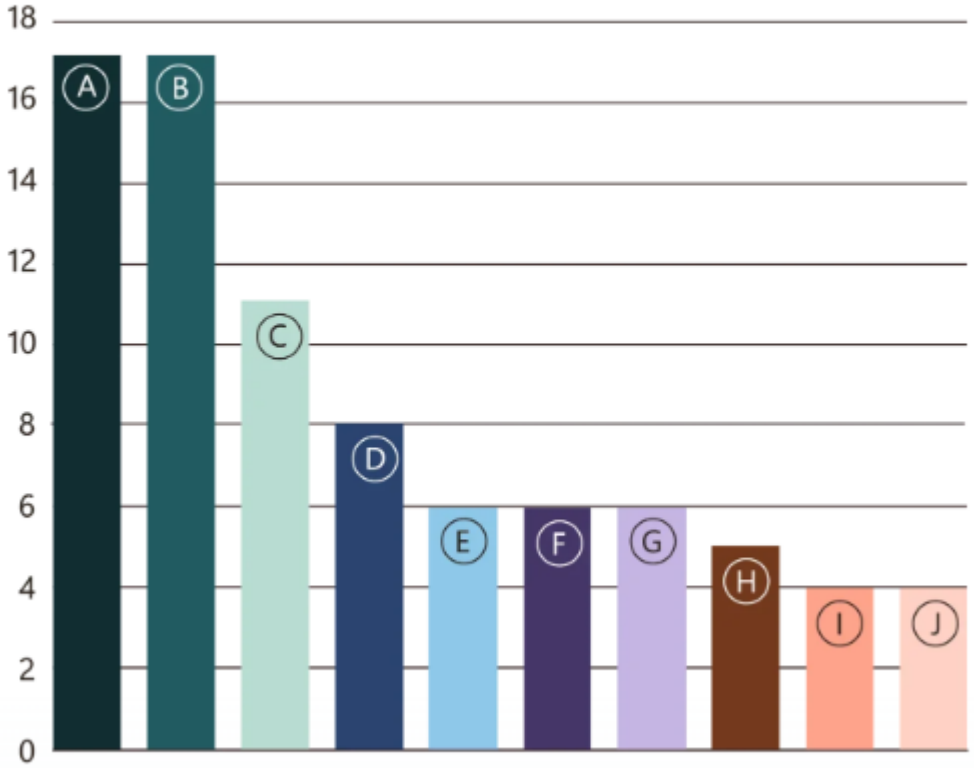
EU & CH Governments

Global
~450 Mio
kommerzielle Nutzer

*Government Requests for Customer Data Report | Microsoft CSR (H1/2025)

Unlawful Access ….

Most cyberattacks targeted industries with vast amounts of sensitive data, incl
academia. Below are the sectors most impacted by cyber threats in 2025.



Source: Microsoft Threat Intelligence

Top ten global sectors m
by threat actors

January - June 2025

A. Government agencies & services	18
B. Information technology	17
C. Research and academia	11
D. Non-governmental organizations	8
E. Critical manufacturing	6
F. Transportation systems	6
G. Consumer retail	6
H. Communications infrastructure	5
I. Financial services	4
J. Healthcare & public health	4

Cybersicherheit

Darum schützen sich Gemeinden unzureichend gegen Hacker

Jede zweite Gemeinde
Cyberangriffe vorbereit

Eliane Leiser
19.06.2025, 06:01 Uhr

Im Visier von Akira

Walliser Gemeinde Vétroz erholt sich von einem Cyberangriff

Mo 27.04.2026 - 1
von Yannick Chava

Ein IT-Dienstleis
geworden. Tage
Betriebsstörung

Bundesrat warnt

Das sind die 6 grössten Bedrohungen für die Schweiz

Der Bundesrat warnt: Die Sicherheitslage der Schweiz hat sich stark verschlechtert. Russland, der Terrorismus und Cyberangriffe könnten das Land gefährden. Eine umstrittene Steuererhöhung soll helfen, die Landesverteidigung zu stärken.

Publiziert: 06.05.2026 um 17:13 Uhr | Aktualisiert: 05:16 Uhr

[Microsoft Digital Defense Report 2025 | Microsoft]

Statement on current media reports regarding data disclosure in the context of the Dutch Consumer and Markets Authority (ACM) / Digital Services Act (DSA)

Microsoft is committed to complying with the laws and regulations in the markets where we operate.
This includes our obligations under EU frameworks such as the Digital Services Act, as well as responding appropriately to lawful requests from authorities in the United States.
This specific request required Microsoft business records, **not** **customer data.**
We cannot comment on ongoing legal or congressional processes. We do, however, value our continued engagement with policymakers, regulators, and civil society on issues related to digital safety and fundamental rights globally.

This is not a CLOUD Act matter. Requests under the U.S. CLOUD Act relate to serious criminal investigations by law enforcement. The documents referenced in the reporting relate to a U.S. congressional inquiry into the EU Digital Services Act and consisted of a limited set of Microsoft business records.
Microsoft did not share customer information with the U.S. government.
We are committed to protecting customer data and complying with the laws and regulations in the countries where we operate, including Europe as well as the United States.

International Criminal Court Case

Microsoft didn't cut services to International Criminal Court, its president says

Chief prosecutor's email issues have spurred fears in Europe that Trump could trigger a "kill switch" through U.S. tech giants abroad.

SHARE

POLITICOPRO Free article usually reserved for subscribers

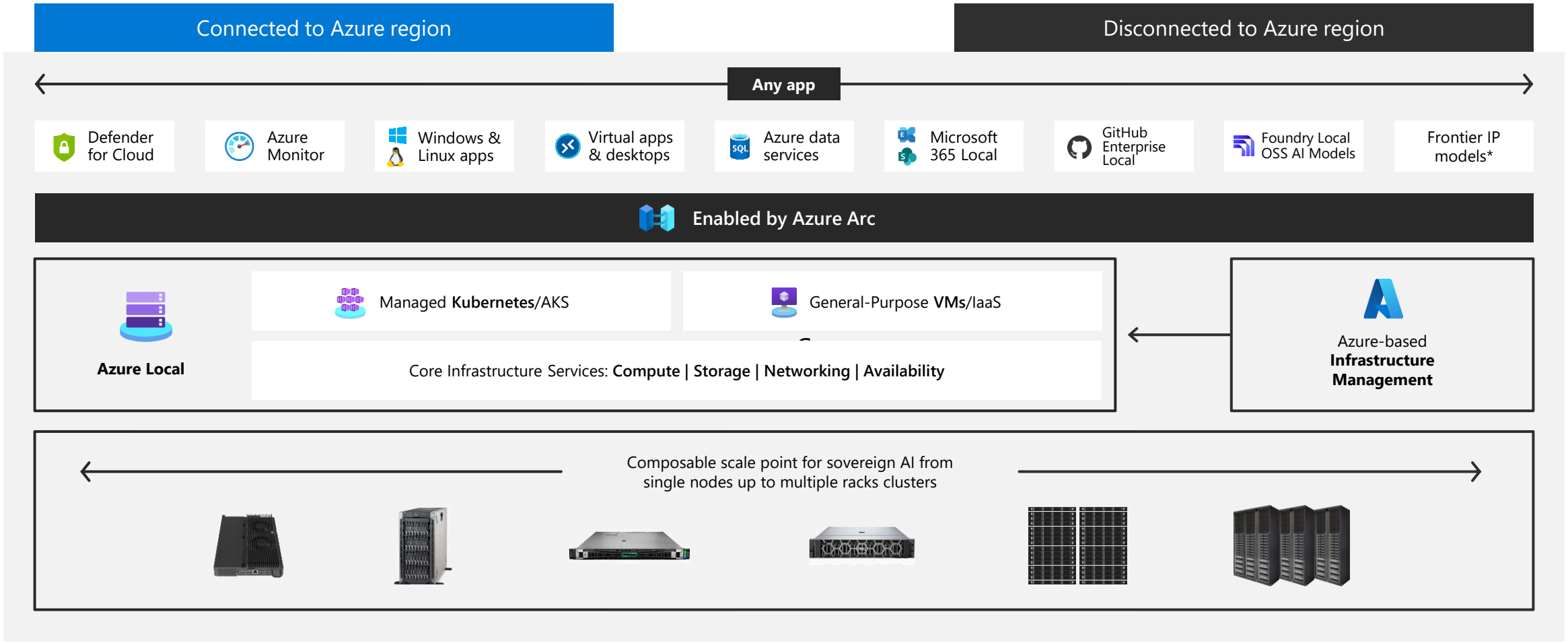
The company's President Brad Smith told reporters that Microsoft's actions "did not in any way involve the cessation of services to the ICC." | Michael Reynolds/EFE via EPA

JUNE 4, 2025 12:45 PM CET
BY SAM CLARK

Source: Microsoft didn't cut services to International Criminal Court, its president says – POLITICO

Azure Local

AI-ready infrastructure, anywhere



* For qualified customers

Microsoft

Danke!

Cyril Hollenstein
Senior Account Technology Strategist · Public Sector Schweiz
cyhollen@microsoft.com

Jürg Stadelmann
Senior Cloud Solution Architect
juerg.stadelmann@microsoft.com