"Sicher? Sicher nicht! Das Dilemma mit der digitalen Souveränität."

Vorstellung & Zielsetzung

Stefan Pilarczyk

Head of Cybersecurity

- 15 Jahre Erfahrung in
  - IT
  - Cyber-Security
  - Advisory
- starker technischer Hintergrund
- Hands-on-Mentalität

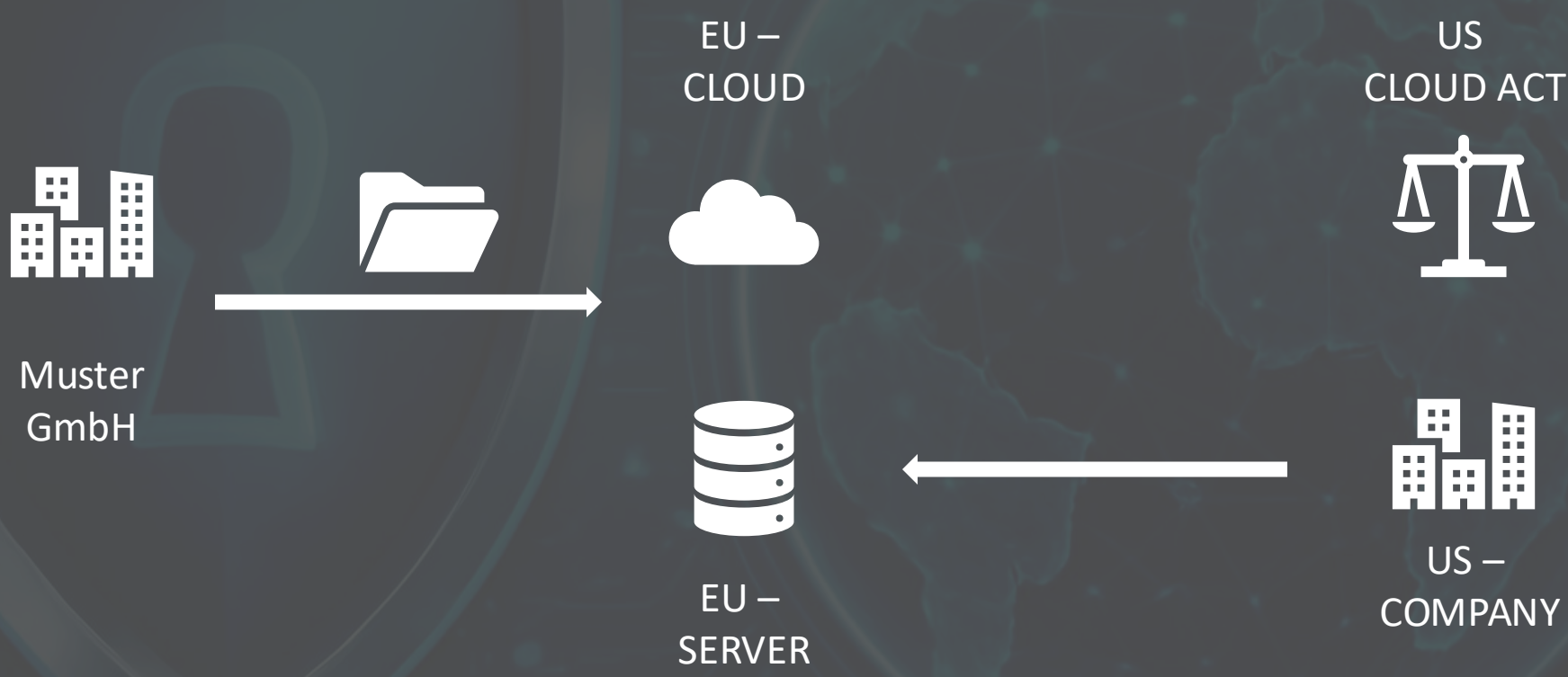
- Beratung von CxO und IT-Abteilungen
- Erfahrung in der Einführung zahlreicher ISMS-Systeme mit unterschiedlichen Standards (DORA, BAIT, VAIT, ISO27001, BSI-Grundschutz, TISAX, NIST)
- Entwicklung und Umsetzung von Sicherheitsstrategien und Sicherheitskonzepten
- Durchführen und Begleiten von Cybersicherheitsaudits (z.B. PenTests, Social Engineering)
- Notfallmanagement und Incident Response

Agenda

Einleitung	01
Begriffserklärung & Relevanz	02
Blickwinkel: ➢ Technik ➢ Recht ➢ Wirtschaft ➢ Ethik	03
Eure Meinung	04
Fragen	05

„Wer kontrolliert eigentlich wirklich Ihre Daten, sobald sie auf einer Cloud liegen?“

Dilemma



Digitale Souveränität vs. Extraterritorialen Rechtsvorschriften

Dilemma

US CLOUD Act = Clarifying Lawful Overseas Use of Data Act

Ziel: US-Strafverfolgungsbehörden erlauben, auf Daten zuzugreifen, die bei US-Unternehmen gespeichert sind – auch wenn diese Daten außerhalb der USA liegen.

Geltungsbereich: Betrifft Cloud-Dienste und andere IT-Dienstleister mit Sitz in den USA, unabhängig davon, wo die Server stehen.

Rechtliche Folge: US-Behörden können per Gerichtsbeschluss Daten von US-Firmen verlangen – auch wenn die Daten in Europa oder anderswo gespeichert sind.

Konflikt mit EU-Datenschutz: Trotz DSGVO und europäischer Datenschutzgesetze müssen Cloud-Anbieter US-Recht befolgen, was zu Rechtsunsicherheiten für europäische Nutzer führt.

Keine Herausgabe verweigert: US-Unternehmen dürfen die Datenübergabe nicht ablehnen, auch wenn das im Zielstaat illegal wäre (Umweg über amerikanische Staatsbürger möglich)

Auswirkungen: Einschränkung digitaler Souveränität und Datenschutz der Nutzer, da Daten theoretisch von US-Behörden eingesehen werden können.

-> CLOUD Act hat zwar die rechtliche Grundlage für US-Datenzugriffe auf global verteilte Daten geschaffen, konkrete Einzelfallentscheidungen sind in der Öffentlichkeit aber kaum transparent.

Dilemma

US Cloud Act ends Microsoft Dublin email case with a whimper

Act gives US 'nearly unchecked' power over global digital privacy rights, say critics

Expand

At the end of March, President Donald Trump signed into law the Cloud Act, which removed the ambiguity over whether a US court could demand data held extraterritorially. Photograph: Jim Lo Scalzo/EPA

Dilemma

Nur digitale Souveränität kann uns vor IT-Zusammenbrüchen schützen

Immer mehr Softwareprogramme werden von immer weniger Firmen bereitgestellt. Auch deshalb erfasste die IT-Panne die halbe Welt. Digitale Emanzipation ist nötig

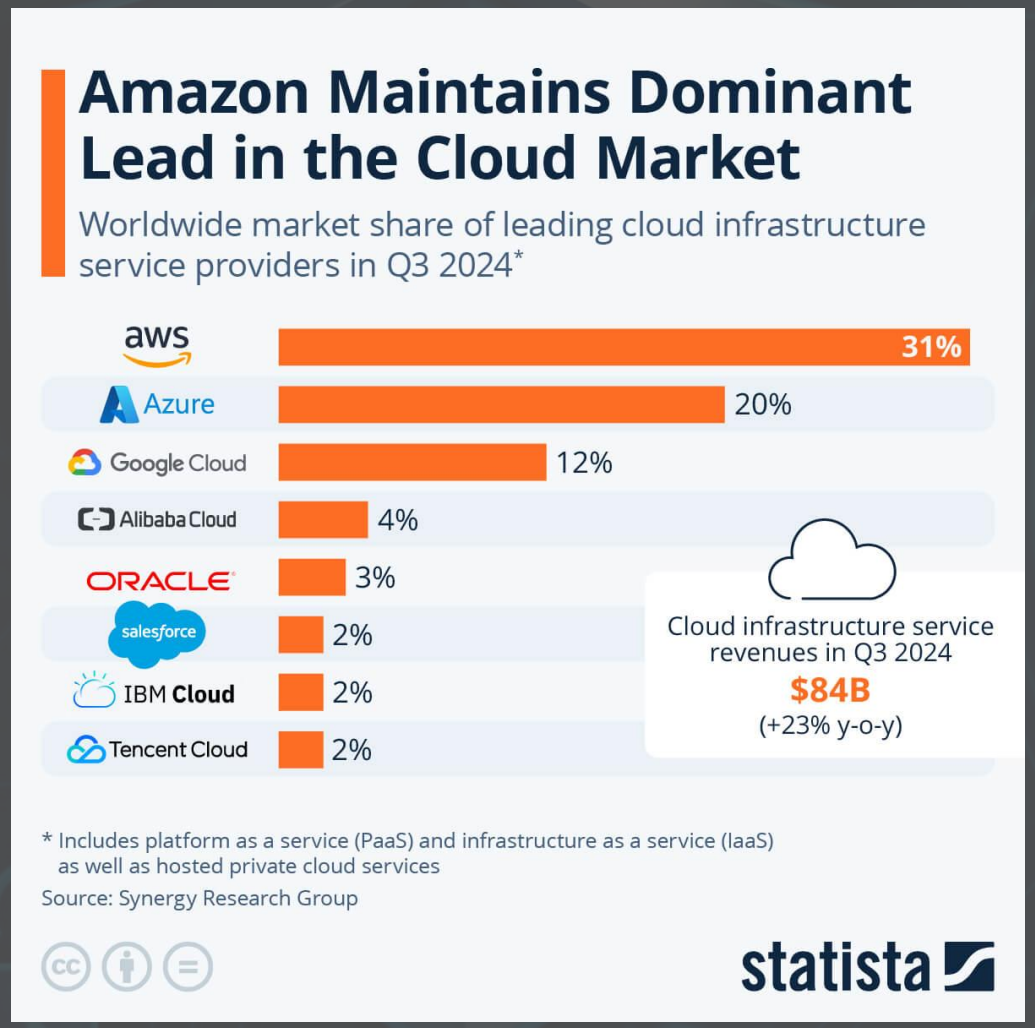
Michael Andrick

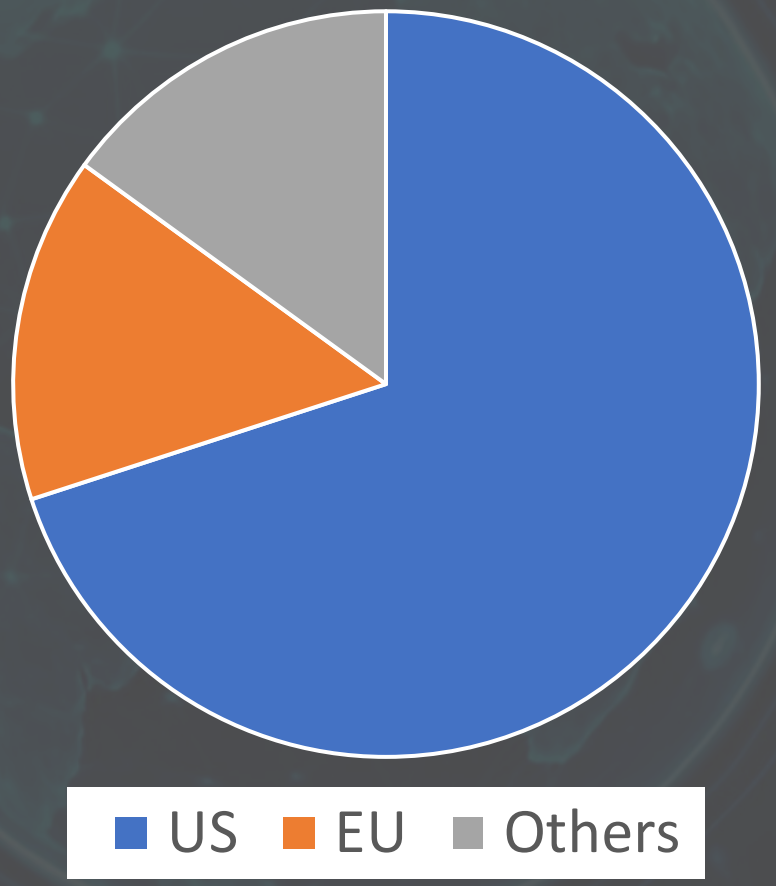
20.07.2024 · 20.07.2024, 14:51 Uhr

13

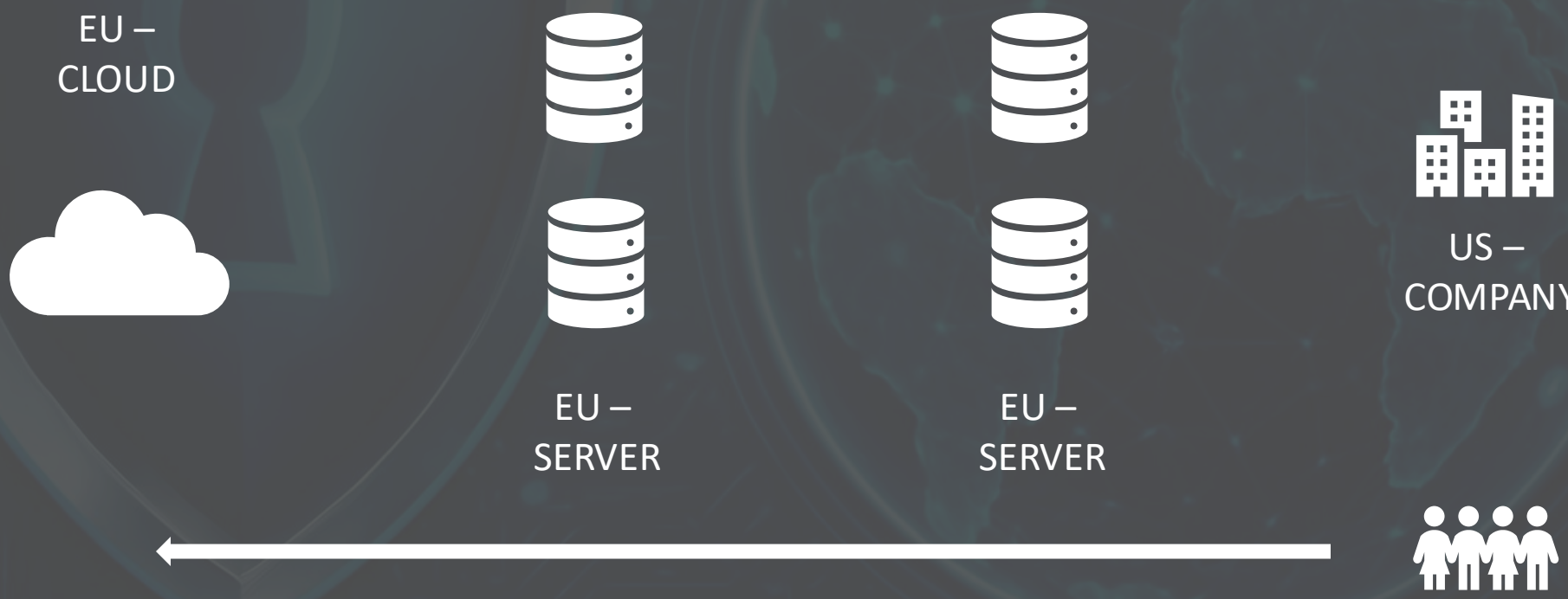
Die globale IT-Panne am 19. Juli 2024 ist auf ein fehlerhaftes Update zurückzuführen.

Fotoillustration: BLZ. Foto: Hartono Creative Studio/Unsplash


Amazon Maintains Dominant Lead in the Cloud Market
Worldwide market share of leading cloud infrastructure service providers in Q3 2024*
aws 31%
Azure 20%
Google Cloud 12%
Alibaba Cloud 4%
ORACLE 3%
salesforce 2%
IBM Cloud 2%
Tencent Cloud 2%
Cloud infrastructure service revenues in Q3 2024
$84B
(+23% y-o-y)
* Includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services
Source: Synergy Research Group
statista


US
EU
Others

Kann Technik wirklich digitale Souveränität sicherstellen, wenn internationale Gesetze wie der US CLOUD Act extraterritorial wirken und Zugriff auf Daten fordern?



Sind europäische Datenschutzregelungen nur theoretisch wirksam, solange US-Gesetze weltweit Datenzugriff erzwingen können?

Die Lösung – Data Privacy Framework (DPF)

Das DPF beruht auf der US-Executive Order 14086 (Joe Biden vom 7. Oktober 2022), die Grundsätze zur Beschränkung von US-Geheimdienstzugriffen und ein unabhängiges Kontrollgremium (Privacy and Civil Liberties Oversight Board – PCLOB) einführte.


Government Surveillance

What the PCLOB Firings Mean for the EU-US Data Privacy Framework

February 14, 2025 / Silvia Lorenzo Perez

Widersprüchliche Anforderungen schaffen Unsicherheiten:

- Europäische Unternehmen sind hin- und hergerissen zwischen DSGVO-Konformität und US-Gesetzen mit extraterritorialer Wirkung.
- Dies führt zu rechtlicher Unsicherheit, erhöhten Compliance-Kosten und erschwert klare Strategien.

Ist digitale Souveränität wirtschaftlich tragbar – und für welche Unternehmen lohnt sich der Aufwand wirklich?

- Datenschutz
- Compliance
- Transparenz
- Kontrolle
- Rechtliche Klarheit

- Skalierbarkeit
- „Kosten“
- Breit aufgestellt
- Renomiert
- Innovation und KI 😁

Wer wäre bereit, Mehrkosten oder Einschränkungen in Komfort zu akzeptieren, wenn dadurch echte digitale Souveränität und Datenschutz gewährleistet wäre?

- Wunsch nach Privacy, Transparenz und Sicherheit ihrer digitalen Daten
- Gleichzeitig ist der Wunsch nach bequemen, kostengünstigen und funktionalen digitalen Diensten sehr hoch.
- Balance zwischen Datenschutz und Innovation: Wie viel Kontrolle über Daten ist notwendig, ohne Innovationshemmnis zu sein?
- Digitale Souveränität wird häufig als abstraktes Ziel gesehen.

Fazit

„Wie viel Komfort und Kostenvorteil sind wir als Gesellschaft bereit aufzugeben, um echte digitale Souveränität zu erreichen?“

„Sollte Europa in Kauf nehmen, technologisch langsamer zu sein, wenn dadurch mehr Datenschutz und Unabhängigkeit gesichert werden?“

„Können wir internationalen Cloud-Anbietern jemals wirklich vertrauen – oder brauchen wir 100 % europäische Lösungen?“

„Wie lässt sich digitale Souveränität mit globaler Zusammenarbeit und Datenaustausch vereinbaren, ohne Sicherheit einzubüßen?“

„Wer trägt letztlich die Verantwortung für digitale Souveränität – Politik, Unternehmen oder jede/r Einzelne?“

LinkedIn

/stefan-pilarczyk

Vielen Dank!

Fragen?