DSGVO und Cloud

Die Quadratur des Kreises?

Dr. -Ing. Sybe Izaak Rispens

Art. 32 DSGVO

Sicherheit der Verarbeitung

- (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
  - die Pseudonymisierung und **Verschlüsselung** personenbezogener Daten; (1)
  - die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**;
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (2)

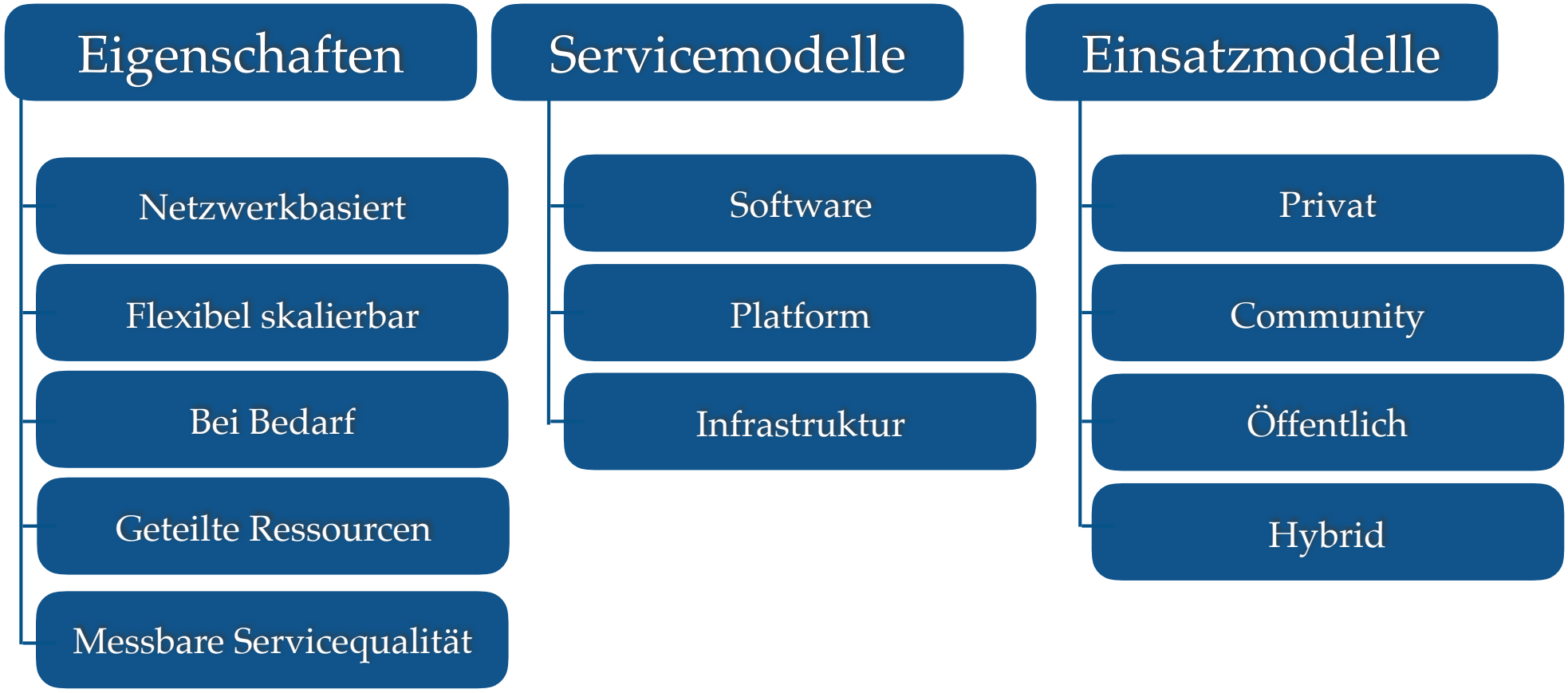
Art. 32 DSGVO

Sicherheit der Verarbeitung

- (1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
  - die Pseudonymisierung und **Verschlüsselung** personenbezogener Daten; (1)
  - die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
  - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**;
  - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (2)

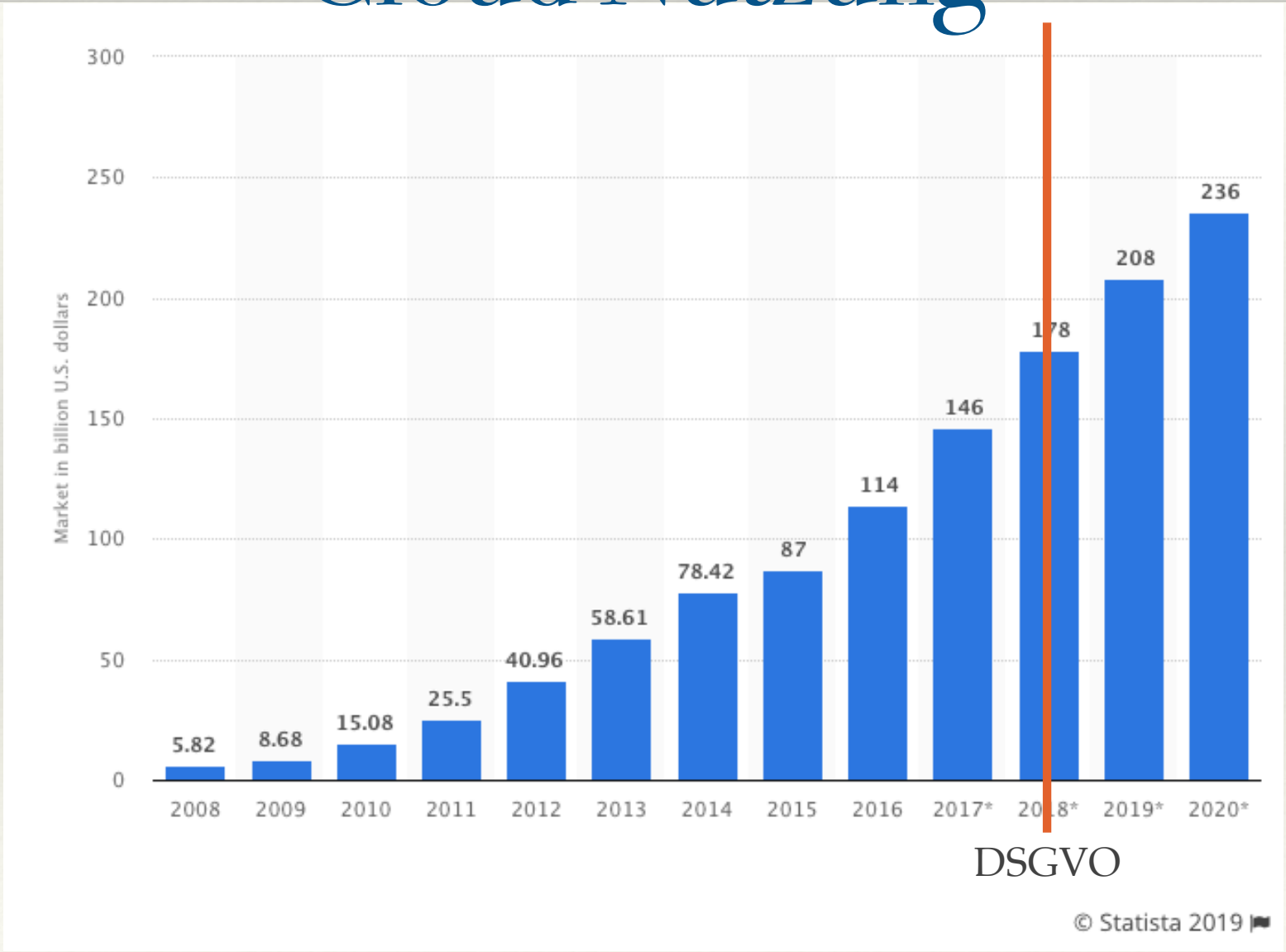
—> Massive Änderungen durch Cloud-Nutzung

Was heißt "Cloud"?

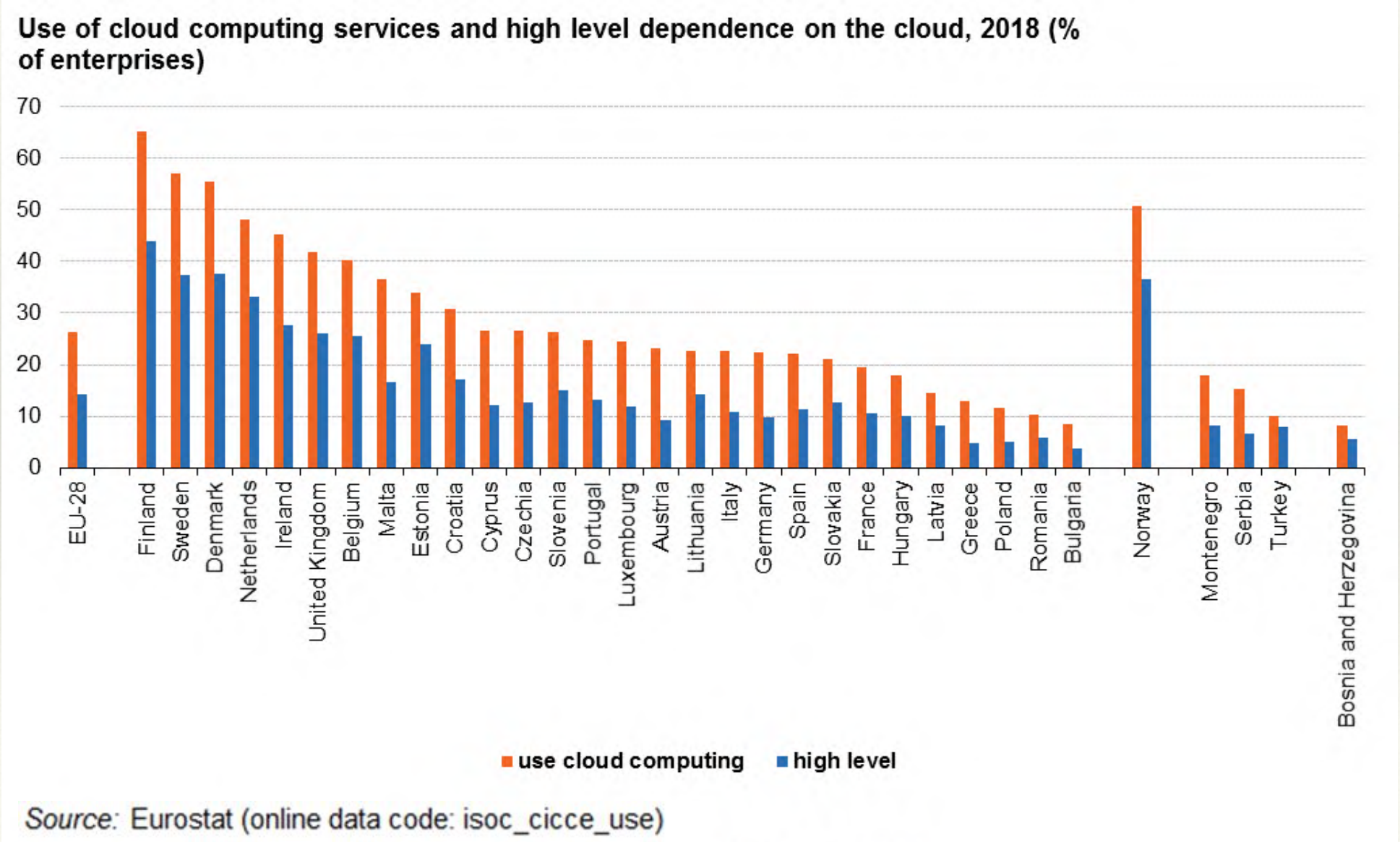


Quelle: The NIST Definition of Cloud Computing
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

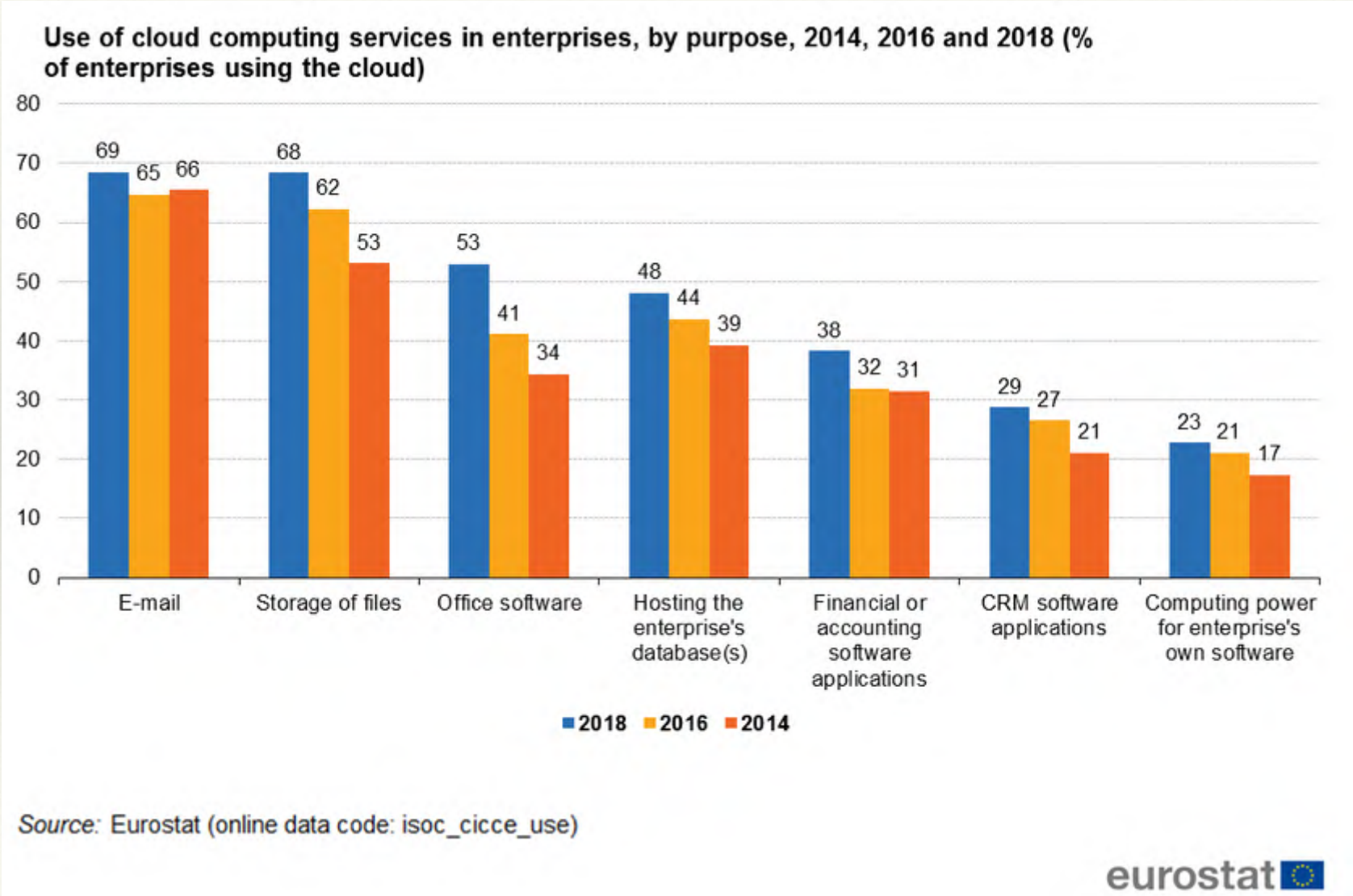
Cloud Nutzung



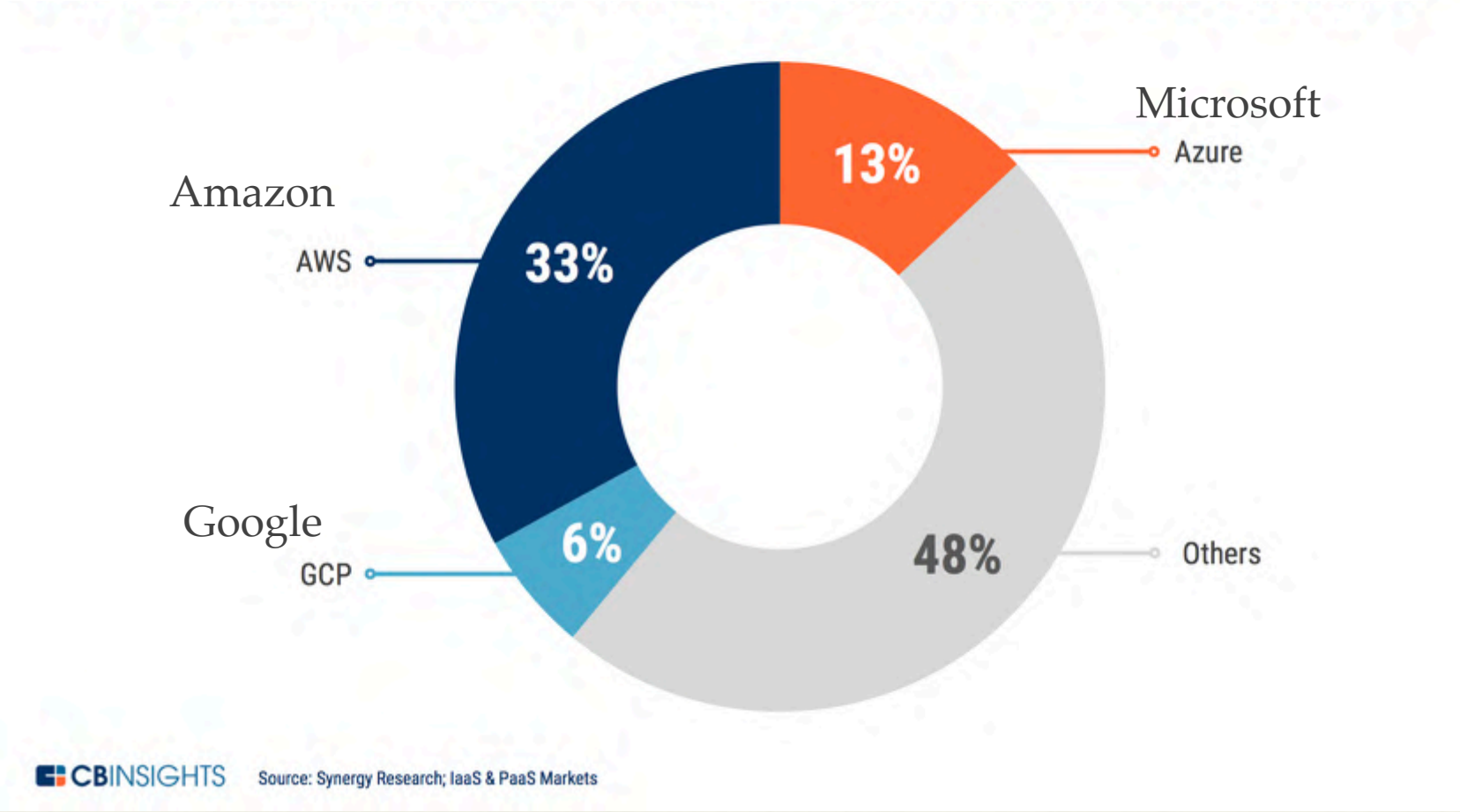
Cloud Nutzung

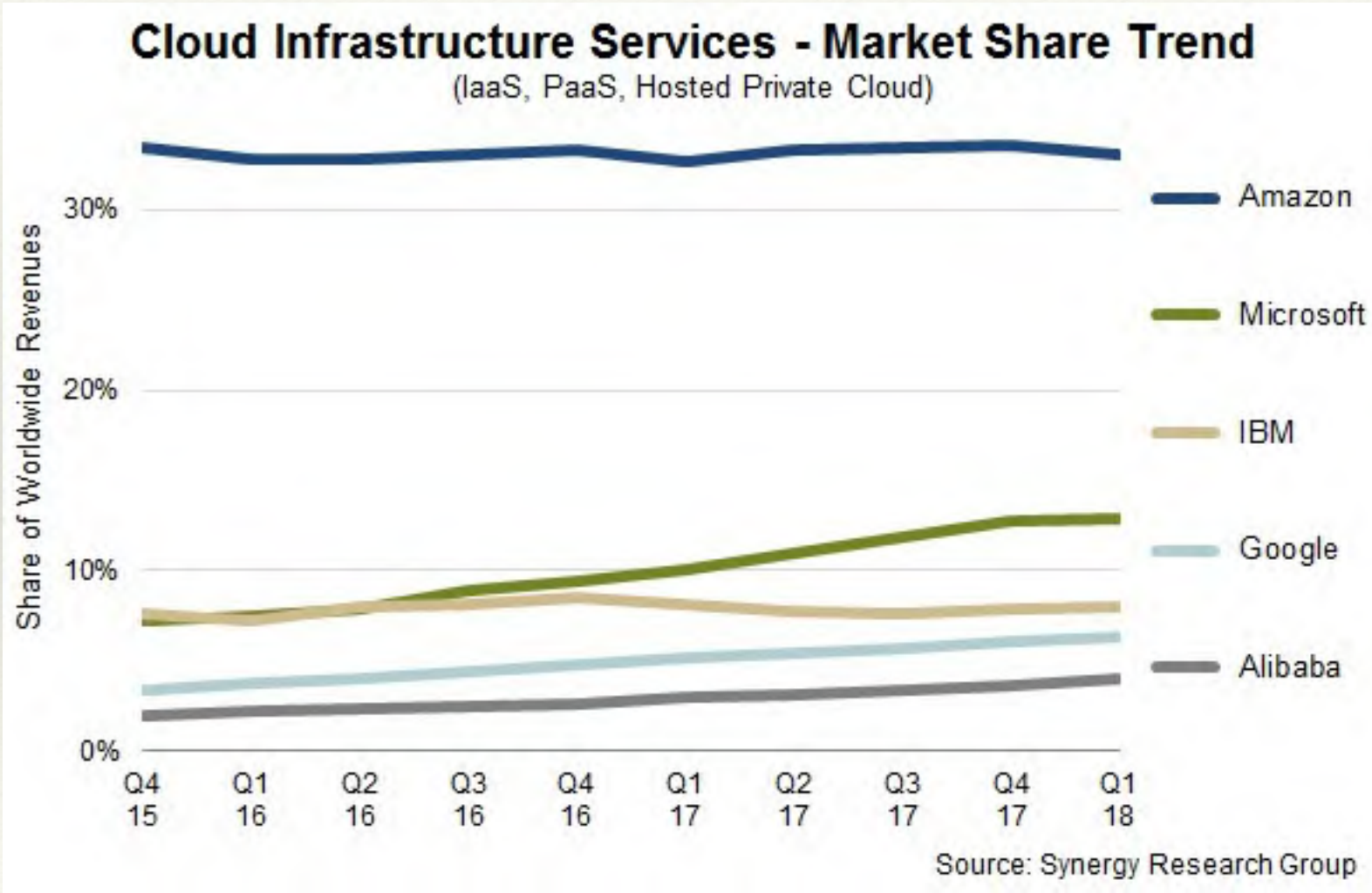


Cloud Nutzung



Cloud Anbieter




Cloud Infrastructure Services - Market Share Trend
(IaaS, PaaS, Hosted Private Cloud)
Share of Worldwide Revenues
30%
20%
10%
0%
Q4 15
Q1 16
Q2 16
Q3 16
Q4 16
Q1 17
Q2 17
Q3 17
Q4 17
Q1 18
Amazon
Microsoft
IBM
Google
Alibaba
Source: Synergy Research Group

Bedrohungen DSGVO & Nutzung der Cloud

1. Bedrohungen bei der **Einführung** von Cloud Services
2. Bedrohungen bei der Nutzung Cloud-Infrastrukturen
3. Bedrohungen bei der **Nutzung** von Cloud Services

1. Bedrohungen bei Einführung der Cloud

1. Der großer Wille, Cloud Computing auf jeden Fall einzusetzen, führt zu komplett illusorischen Annahmen

1. Bedrohungen bei Einführung der Cloud

1. Der großer Wille, Cloud Computing auf jeden Fall einzusetzen, führt <u>zu komplett illusorischen Annahmen</u>

    - Cloudanbieter in Deutschland - Alles OK?
        - Cloud Anbieter haben Wachstumsraten von 30% / Jahr und mehr.
        - Sicherheit bleibt auf der Strecke.
    - Da Clouds im Vergleich zu privaten Rechenzentren einen massiven Umfang haben, sind sie für Hacker viel größere Ziele.
    - Datenschutzverantwortung wird leichtsinnig einen Drittanbieter übertragen. Stichwort: <u>Shared Responsibility Model</u>

    - Mangelhaftes Cloud-Management: **Nicht-technische Probleme werden häufig übersehen**.
        - Unzureichende Sicherheitsaudits
        - Mangelhafte Backup-Verfahren
        - Administratoren mit unsachgemäße Zugriffsrechte

1. Bedrohungen bei Einführung der Cloud

2. Der Weg in die Cloud kann sehr schwierig sein und dabei wird übersehen, dass auch an einen **Weg aus der Cloud heraus gedacht werden muss**

1. Bedrohungen bei Einführung der Cloud

3. Cloud-Anbieter beziehen selbst häufig Dienste (z. B. Administration oder Backup von Daten) von Unterauftragnehmern.
    1. personenbezogene Daten geraten an nicht erlaubte Stellen
    2. Sicherheitszertifikate gefährdet
4. Mangelhafte Planung, insbesondere fehlende Notfallplanung

2. Bedrohungen bei der Nutzung Cloud-Infrastrukturen

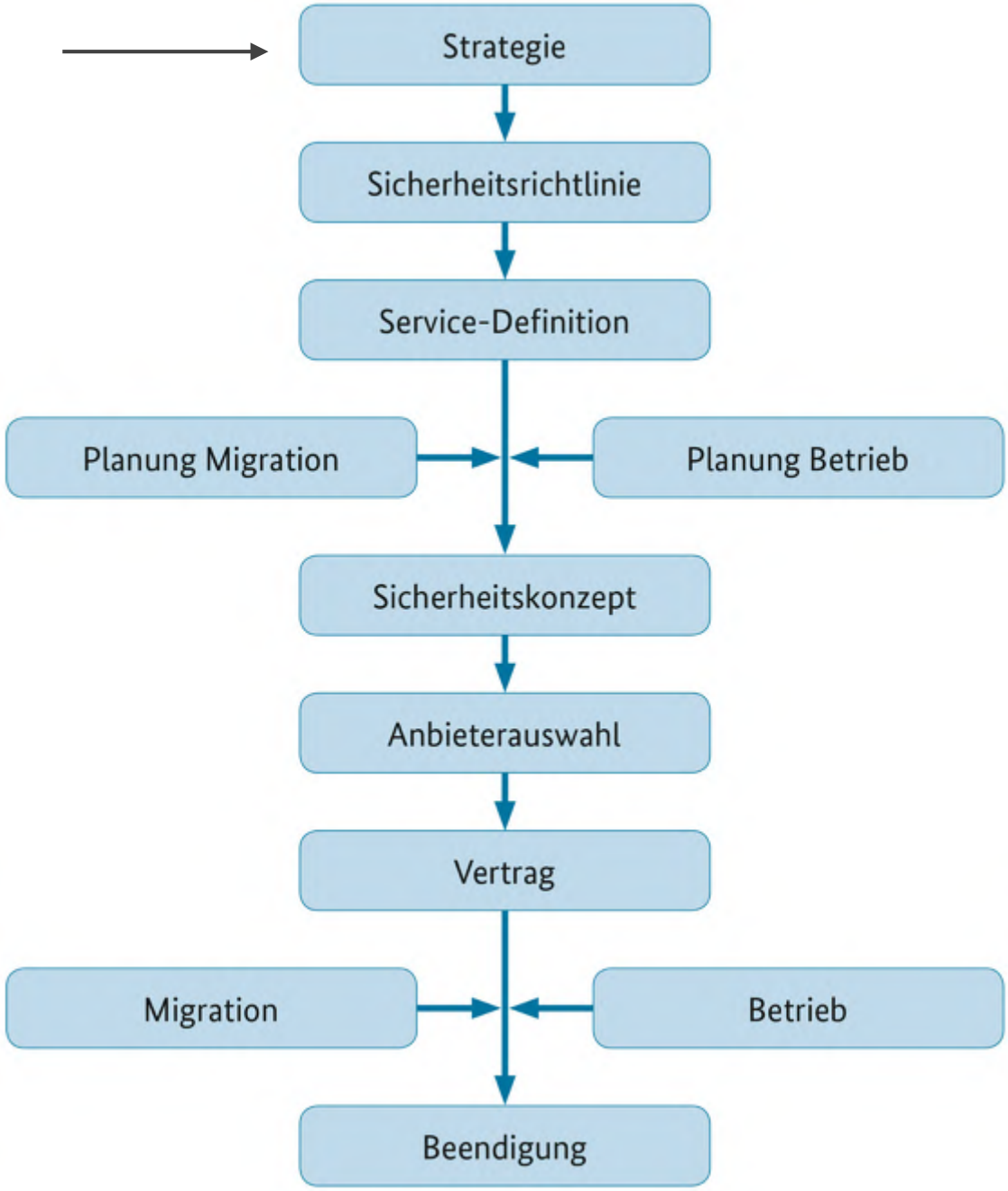
1. Datenverlust bzw. Informationsabfluss
2. Beeinflussung der verschiedenen Nutzer in der gemeinsamen (shared) Cloud-Infrastruktur bis hin zu Angriffen aus der Cloud heraus.
3. Ausfall der Internet- oder Netzverbindung, der den Zugriff auf Daten bzw. Anwendungen unmöglich macht.
4. Denial-of-Service Angriffe auf Cloud-Anbieter, die sicher noch zunehmen werden.
5. **Fehler in der Cloud-Administration, die aufgrund der sehr hohen Komplexität zu erheblichen Sicherheitsproblemen führen**

3. Bedrohungen bei der Nutzung von Cloud-Diensten

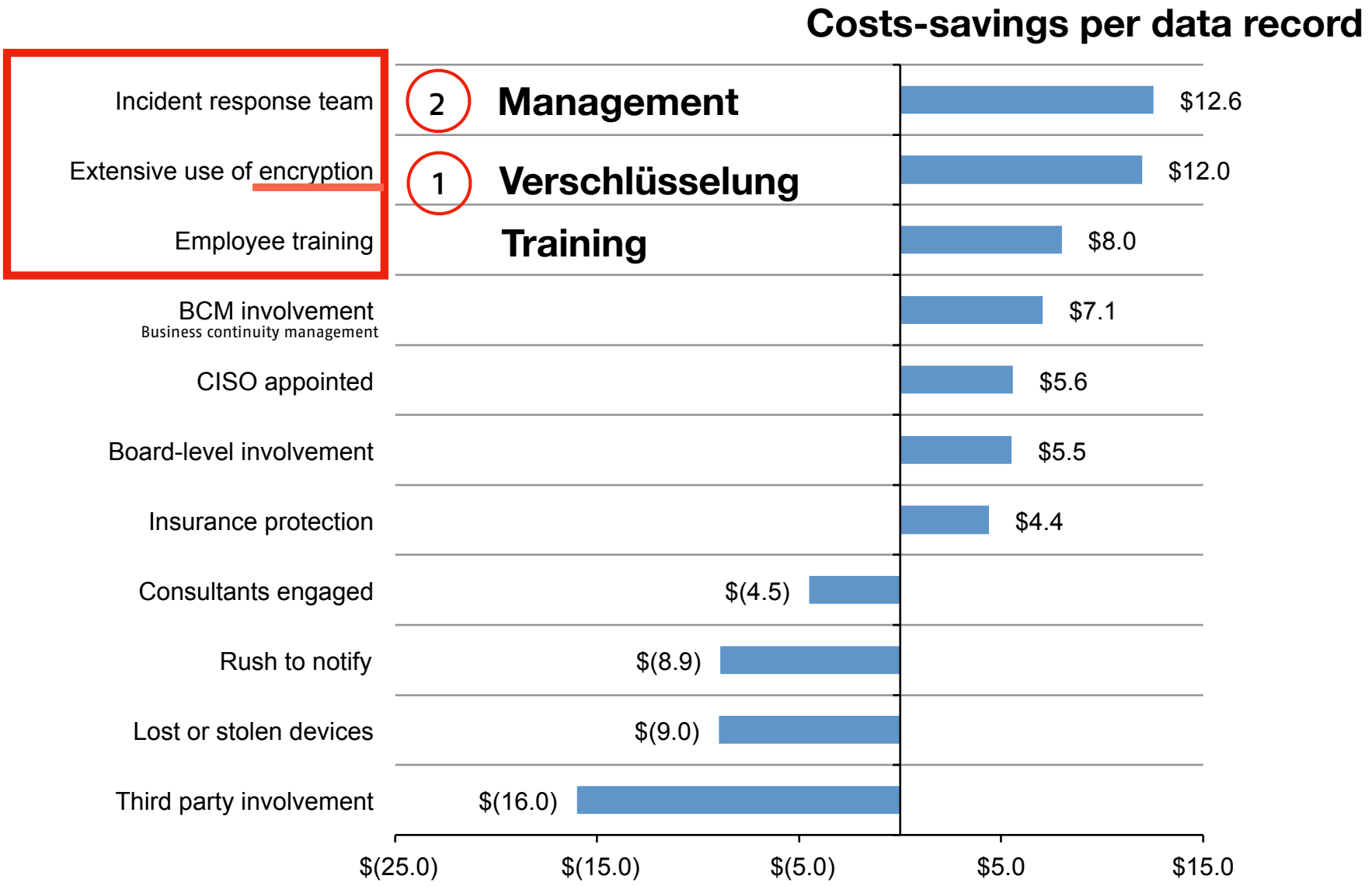
- Identitätsdiebstahl bzw. Missbrauch von Accounts
- Verlust der Kontrolle über die Daten und Anwendungen
- Verletzung geltender Vorgaben und Richtlinien (z. B. Datenschutzanforderungen)
- Sicherheit der Endgeräte, mit denen die Cloud- Dienste verwendet werden.
- Daten können über das Netz abgefangen und (bei schlechter oder nicht vorhandener Verschlüsselung) ausgespäht werden.

> "To cloud computing, the possibilities of **law enforcement authorities** to force cloud provider to hand over data of their customers without informing them about this and be allowed to make a statement about this at all are particularly relevant.
>
> BSI, Secure Cloud computing

DSGVO + Cloud=



Quelle: BSI



Source: 2015 Cost of Data Breach Study: Impact of Business Continuity Management

Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC June 2015

Takeway message:

“Shared Responsibility Model”

=

verlassen sich NIE nur auf die Schutzmaßnahmen ihres Cloud-Providers!

Was können wir für Sie tun?

1. Awareness Schulungen für Ihre Mitarbeiter
2. Ausbildung der internen Datenschutzbeauftragten
3. Übernehmen der Rolle des Datenschutzbeauftragten (Ständig oder als Interimslösung)
4. Technische Prüfungen / Trainings / Beratungen
5. Begleitung von Zertifizierungsprozesse

Termine

Seminare für Datenschutzbeauftragten – Einführung

12. 6.2019

14.8.2019

11.9.2019

Seminare für Mitarbeiter – Einführung

13.6.2019

15.8.2019

12.9.2019

Alle Seminare finden statt in der Bibliothek der Kanzlei von von Zanthier und Schultz:

Kurfürstendamm 217

10719 Berlin

Telefon: +49 30 88 03 59 0

Fax: +49 30 88 03 59 99

Mail: info@meine-dsgvo.eu

Mehr info: www.meine-dsgvo.eu

Vielen Dank!

Dr. Sybe Izaak Rispens
Oliver Lindemann
info@lindemann-rispens.de

Lindemann | Rispens
IT-Sicherheitsberatung / ISO27001