TeleTrusT-EBCA "PKI-Workshop" 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 18.06.2019

Technisch gekapselte Verarbeitung schützt hochsensible Anwendungen mit rein technischen Maßnahmen

Dr. Ralf Rieken, COO

Dr. Hubert Jäger, CTO

Uniscon GmbH

Uniscon auf einen Blick

UNiSCON
Sealed Cloud Technologies
A member of TÜV SÜD

Über die Uniscon GmbH

- Gegründet 2009 (Münchner Technologiezentrum)
- Technologieführer bei Cloud Security
- Entwicklung und Rechenzentren in Deutschland
- Team von 60+ Mitarbeitern
- Kunden in allen Branchen
- Uniscon ist seit dem 31.07.2017 Teil des TÜV SÜD:
  - Mehr als 25.000 Mitarbeiter
  - € 2,6 Mrd. Umsatz in 2017

Entwicklung / Betrieb sicherer Cloud-Lösungen & Dienste:

- international patentierte Sicherheitstechnologie für Cloud Computing (IaaS, PaaS, SaaS)
- Technischer Ausschluss von Softwareanbieter und Hoster (Betreibersicherheit)
- Daten sind auch während der Verarbeitung im Data Center geschützt
- Inhalte und Verbindungsinformationen (Metadaten) technisch geschützt.

UNiSCON
Sealed Cloud Technologies
member of TÜV SÜD

Wie sicher sind meine Anwendungen in einem RZ oder in einer Cloud?

Verarbeitung erfordert unverschlüsselte Daten

UNiSCON Sealed Cloud Technologies
A member of TÜV SÜD

Das Betriebspersonal hat privilegierten Zugang zu Systemen und somit prinzipiell zu unverschlüsselten Daten:

Probleme klassischer Systeme:

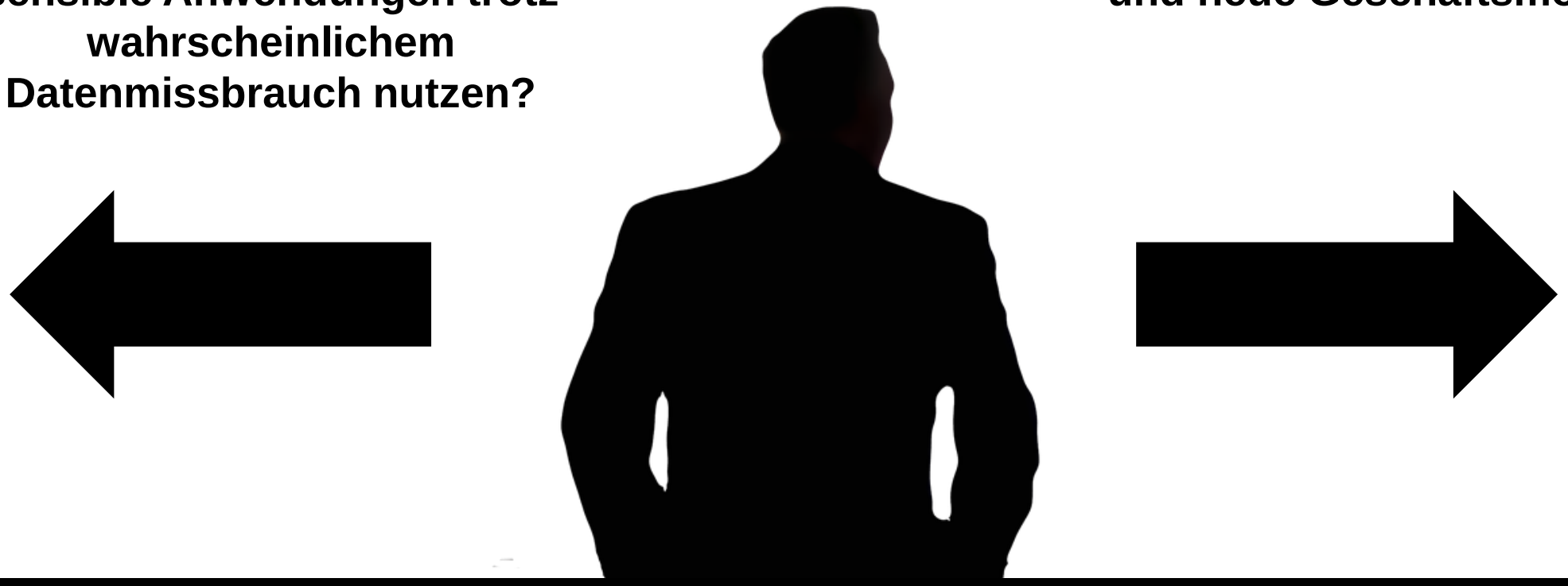
- Datensicherheit hängt vom Faktor „Mensch“ ab
- Solange Einzeltäter unentdeckt kopieren können → mehrere „Hidden Breaches“ pro Jahr*
- Rollenkonzepte und Überwachung helfen, können Einzeltäter aber nicht stoppen

* Historische Werte zeigen bei technischen Administratoren 1/100 bis 1/10.000 Akte der Untreue per Admin und Annum.
Bei 10-100 Personen mit privilegiertem Zugriff je Cloud-Dienst und 10-100 solcher Dienste ergeben sich mehrere verborgende Datenvorfälle („Hidden Breaches“) p.a.

Sicherheitsdilemma

Hosting / Cloud auch für sensible Anwendungen trotz wahrscheinlichem Datenmissbrauch nutzen?

Verzicht auf Kosteneinsparungen und neue Geschäftsmodelle?



Lösung: Ausschluss des Betreibers und seines Personals durch rein technisch gekapselte Verarbeitung im RZ / in der Cloud

UNiSCON
Sealed Cloud Technologies
A member of TÜV SÜD

Sealed Cloud Technologie realisiert mit **rein technischen Mitteln:**

- Verschlüsselte Übertragung und Speicherung der Daten
- Schutz der Daten **auch während der Verarbeitung**

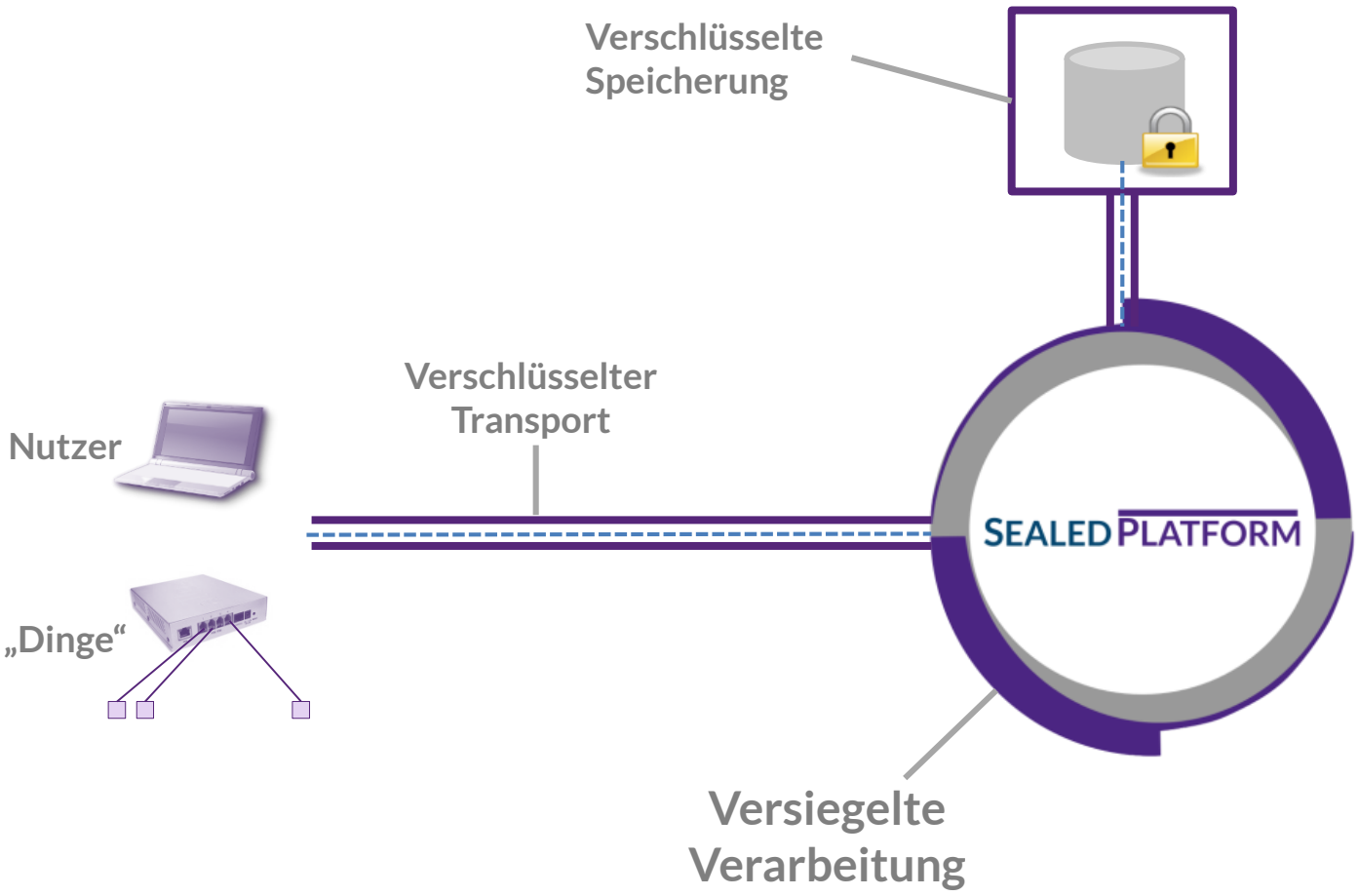
→ **Niemand, außer dem Nutzer selbst, kann auf seine Daten zugreifen.**

→ **Ein Daten-Zugriff von Betreibern und Administratoren ist technisch ausgeschlossen!**

SEALED CLOUD

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Wie funktioniert die technische Versiegelung / Kapselung?

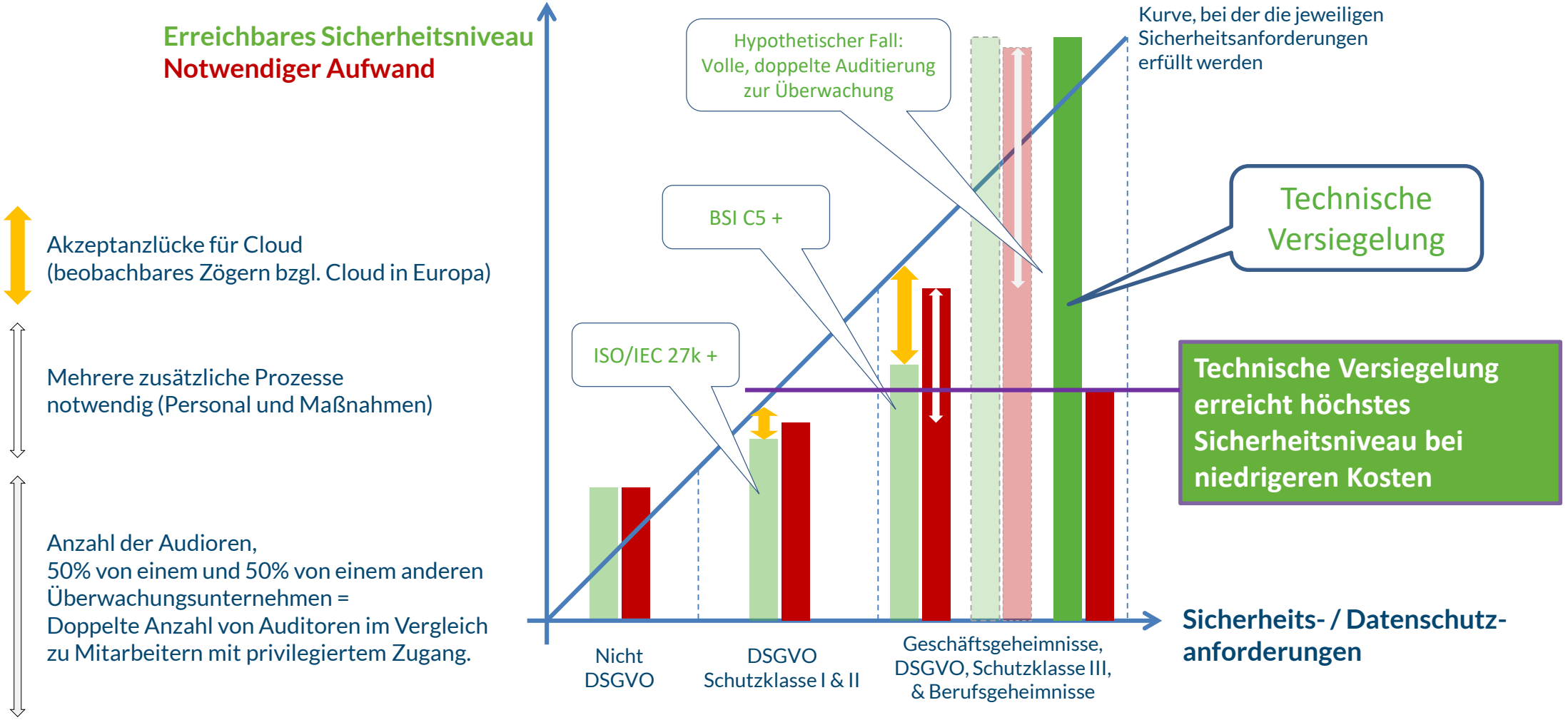


Die vier Maßnahmenpakete der Versiegelung

1. Physische & logische Kaspelung
   Bei Alarm -> Data Clean-Up
2. Schlüsselerzeugung und Haltung so, dass Betreiber kein Zugriff haben kann
3. Wartung ohne privilegierten Zugang, nur „white list“-Befehle
4. Vertrauenswürdiger „Bootstrap“ mit Shamir & „Sealing Trustees“

Zusammenhang von Sicherheitsniveau und Kosten

UNiSCON Sealed Cloud Technologies
A member of TÜV SÜD



Zusammenfassung

UNiSCON Sealed Cloud Technologies
A member of TÜV SÜD

- Rein technisch gekapselte Verarbeitung ist für beliebige Anwendungen nutzbar
- Anwendungen müssen dafür nicht angepasst werden
- Versiegelte Verarbeitung gestattet das Outsourcing hochsensibler, unternehmenskritischer Anwendungen

Kontakt

Uniscon GmbH – Sealed Cloud Technologies

Ridlerstraße 57
80339 München

eMail: contact@uniscon.de
Telefon: (089) 4161 5988-100

www.idgard.de