Rechtskonforme Gestaltung von Cloud-Services in Bezug auf die öffentliche Verwaltung

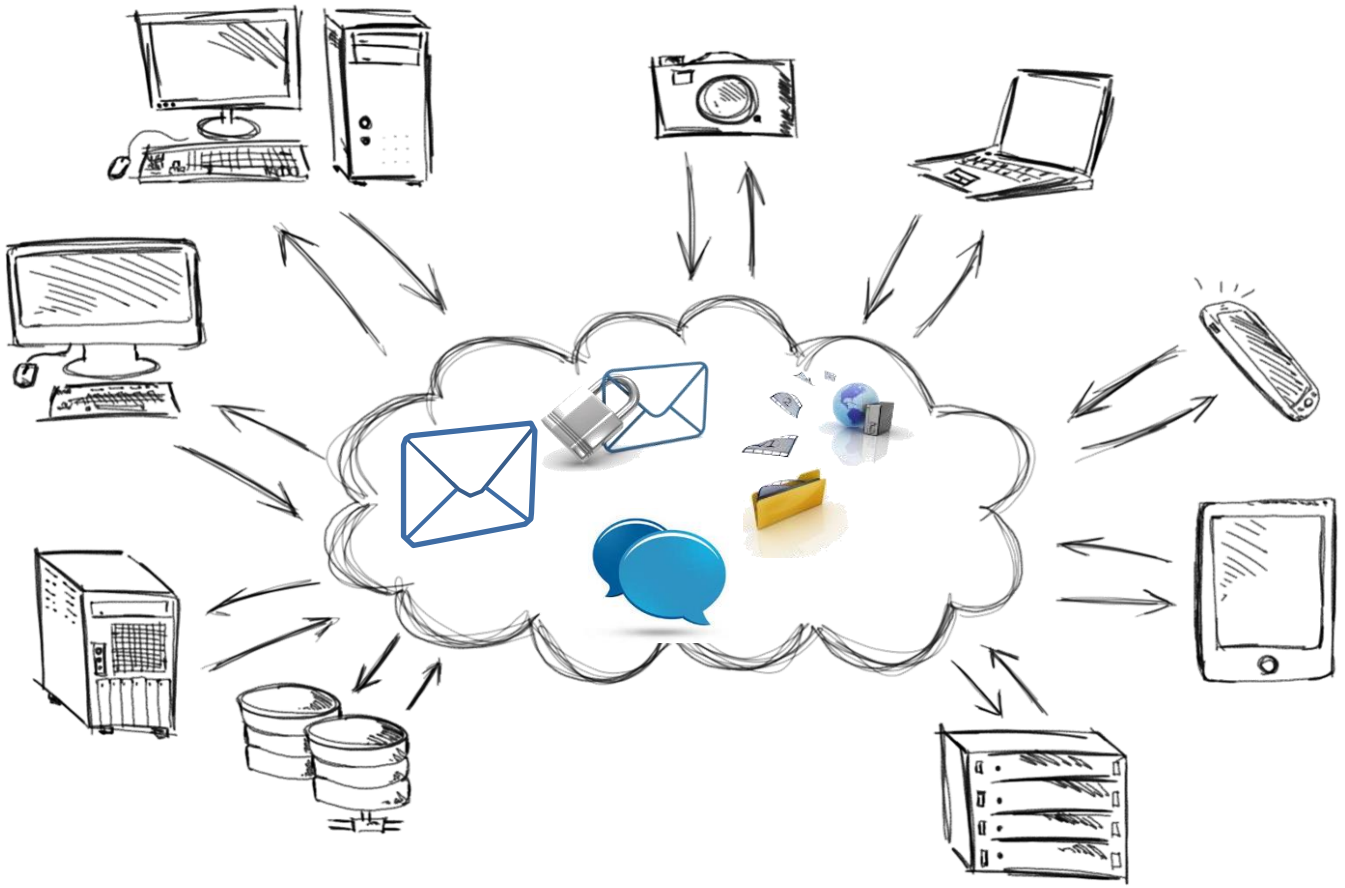
Where2B 2015 Konferenz, Bonn

Dr. Hubert Jäger
Uniscon GmbH

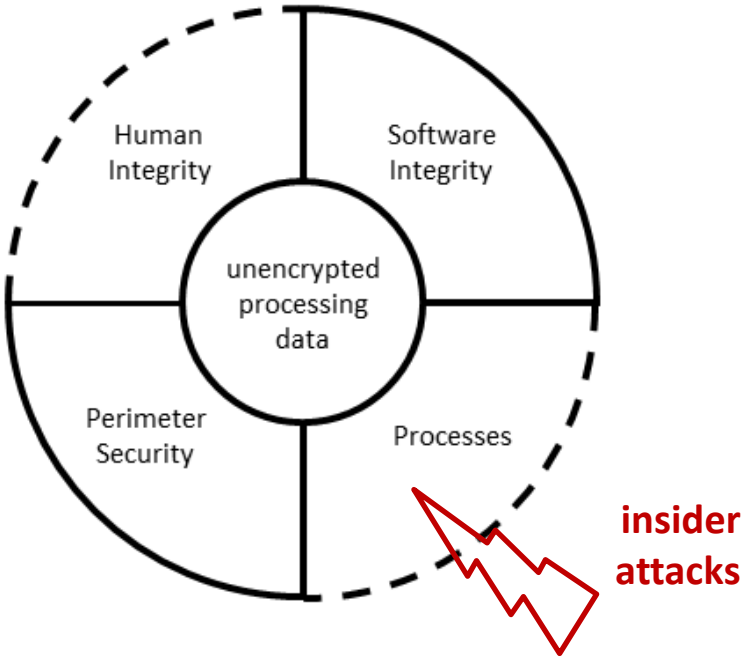
Agenda

- Die Datenschutz-Problematik beim Cloud-Computing
- Schutzziele der Datenschutzgesetze
- Schutzziele des Strafgesetzbuches
- Anforderungen um den Datenschutzgesetzen zu entsprechen
- Anforderungen um dem Geheimnisschutz zu entsprechen
- Technische Ansätze für rechtskonforme Nutzung von Cloud-Diensten in der öffentlichen Verwaltung
- Kriterien zur Auswahl geeigneter Dienste – Zertifikate

Web-/Cloud-Dienste sind verlockend...

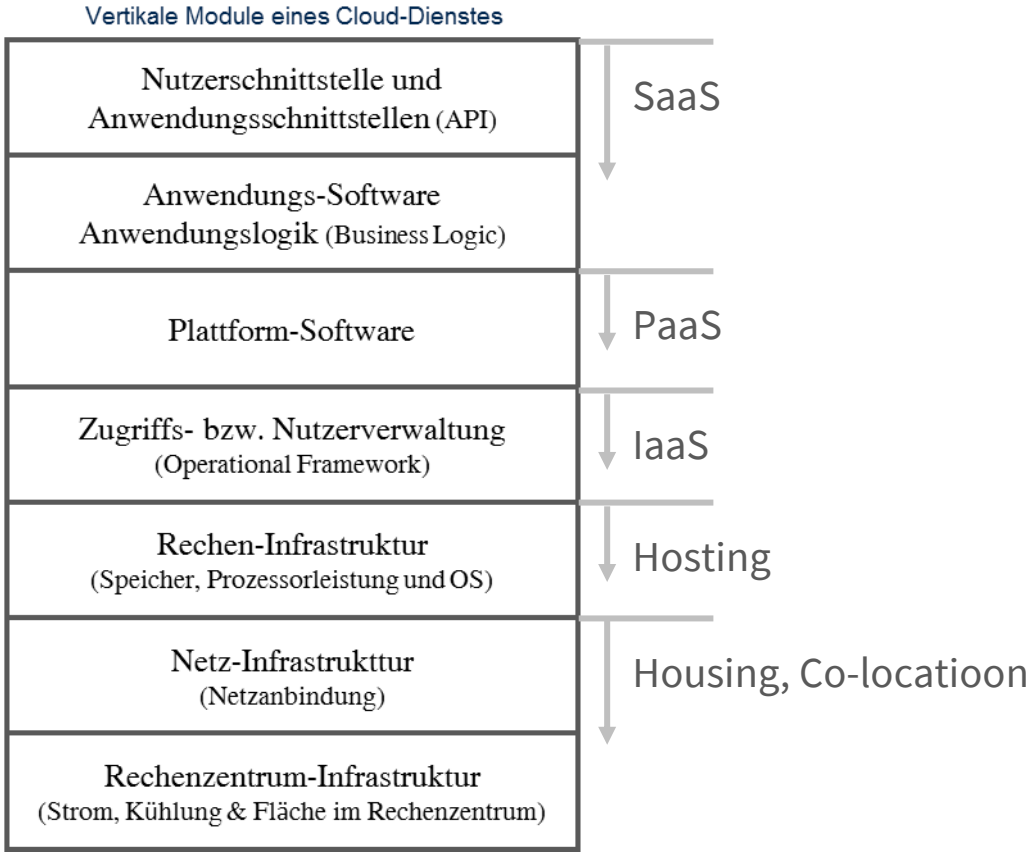


… aber nicht für sensible Daten!!



In der konventionellen Cloud können Betriebs- & Berufs-geheimnisse zur Kenntnis genommen werden.

Die Public Cloud



Die Public Cloud

- e.g. Passwort-Erneuerung via E-Mail
- e.g. Logging von Anwenderdaten, Service-Zugriff
- e.g. Systemschlüssel zur Datenbank vorhanden
- e.g. Nutzername und Passwort durch Betreiber verwaltet
- e.g. Zugriff zum Arbeitsspeicher möglich (z.B. Dump)

↓

Möglichkeiten der Kenntnisnahme durch den Betreiber

↓

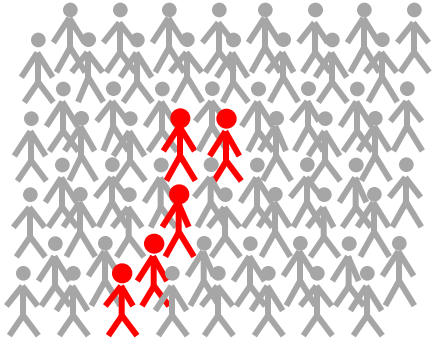
Offenbarung i.S.d. Gesetzes (§ 203 StGB u.a.)

↓

Oft kein verhältnismäßiger Schutz gemäß BDSG u.a.

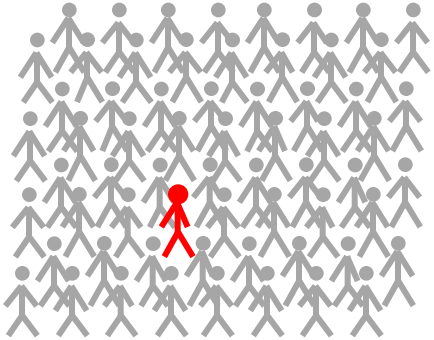
Ein Angreifer genügt .....

Datenmissbrauch
in klassischen Systemen



brauchte i.d.R. mehrere
untreue Daten-Verarbeiter

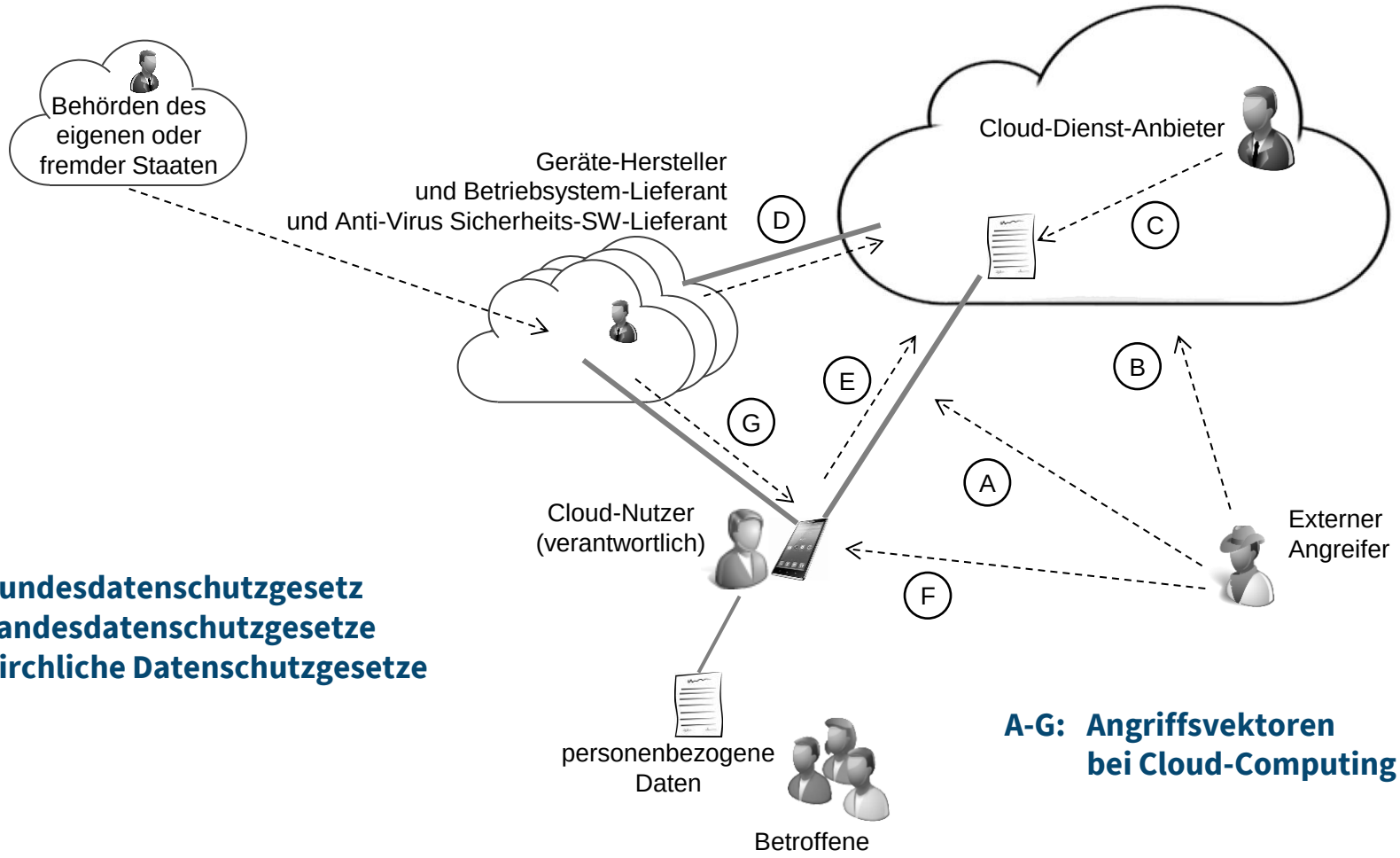
Datenmissbrauch
in vernetzten Systemen



braucht i.d.R. nur einen
untreuen Daten-Verarbeiter

Nur technische Maßnahmen können die notwendige Gewaltenteilung wieder herstellen.

Schutzziele der Datenschutzgesetze



Bundesdatenschutzgesetz
Landesdatenschutzgesetze
Kirchliche Datenschutzgesetze

A-G: Angriffsvektoren bei Cloud-Computing

Datenschutzgesetze schützen die informationelle Selbstbestimmung der Betroffenen

Schutzziele des Strafgesetzbuchs

§ 203 StGB

(1) … Ärzte, Anwälte, …
(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten
2. …

Geheimnisträger **Privatperson**

§ 203 StGB schützt das Vertrauensverhältnis zwischen Privatperson und Geheimnisträger (Katalogberuf oder öffentlicher Dienst)

§ 353b StGB

(1) Wer ein Geheimnis, das ihm als 1. Amtsträger, 2. für den öffentlichen Dienst besonders Verpflichteten oder 3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt, anvertraut worden oder sonst bekanntgeworden ist, unbefugt offenbart und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. …

Staat **Gesellschaft**

§ 353b StGB schützt das Vertrauensverhältnis der Gesellschaft in den Staat

Datenschutz-Anforderungen

- Technisch-organisatorische Maßnahmen nach einem Aufwand, der in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht
  -> Einzelfallprüfung oder Schutzklassen

- Vertragliche Regelung der Auftragsdatenverarbeitung

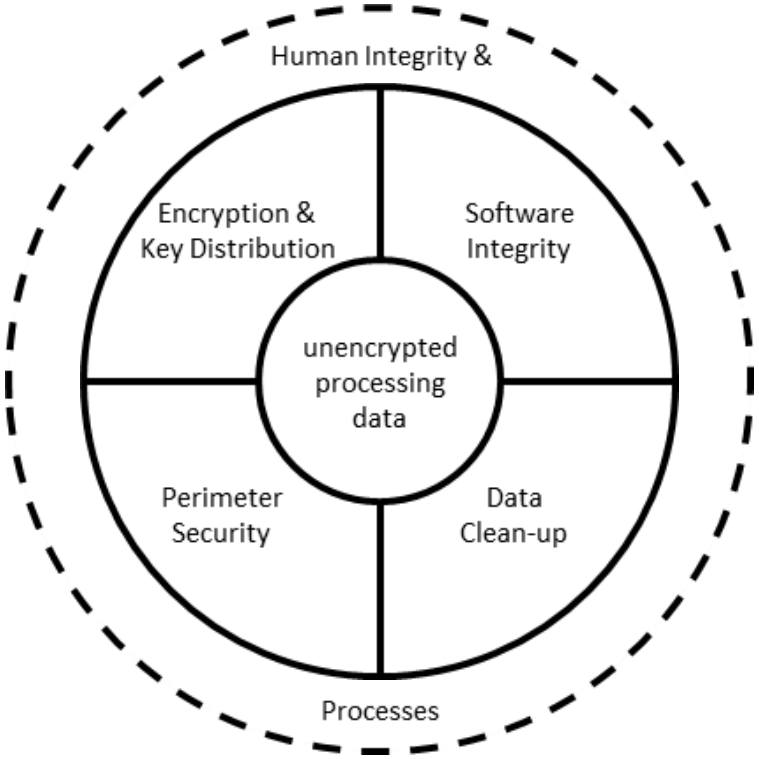
- Zertifizierungsstandard „Trusted Cloud Datenschutzprofil (TCDP)“ basierend auf ISO/IEC 27018

Geheimnisschutz-Anforderungen

- Bereits die theoretische Möglichkeit zur Kenntnisnahme von Privatgeheimnissen wird als Tatbestand der Offenbarung i.S.d § 203 StGB angesehen.
- Technischer Ausschluss der Möglichkeit der Kenntnisnahme
  -> Verschlüsselung
- Problem der Metadaten und Verbindungsinformationen
  -> Verschlüsselung + Versiegelung (Sealed Cloud)
- Problem der Langzeitverschlüsselung
  -> noch keine gute Lösung vorhanden
  (Potential: Post-Quantum-Computing-Kryptographie)

Das Konzept der „Betreibersicherheit“

Entlang der ersten Verteidigungslinie
werden organisatorische Maßnahmen durch innovative technische ersetzt



- Segmentierung des Datenzentrums
  Mitarbeiter haben nur zu Teilen Zugriff
- Bei geplantem oder ungeplantem Zugriff
  Alarmierung ➔ Data Clean-Up
- Schlüsselverteilung so,
  dass Betreiber nicht lesen kann
- Bei Wiederanlauf
  vollständiger Integritäts-Check
- Statischer und dynamischer Audit

Keine Möglichkeit der Kenntnisnahme von Nutzerdaten durch den Betreiber

Bedingungen für Rechtskonformität

Diese Module müssen dem Sealed Cloud Konzept entsprechen

Vertikale Module eines Cloud-Dienstes

- **u.a. voll automatisierter „Self-Service“**
- **u.a. kein Andenderdaten Logging, OWASP-Regeln**
- **u.a. keine Systemschlüssel**
- **Schlüsselverteilung so, dass kein Leseschlüssel beim Betreiber**
- **u.a. wird bei Alarm der „Data-Clean-Up“-Prozess ausgelöst**

Keine Möglichkeit der Kenntnisnahme durch den Betreiber

Digitale Transformation rechtskonform gestalten

Alternative zu
FTP-& Filesharing-Diensten

Projekt- &
Datenräume

Mobiler
Datenabruf

Industrie 4.0
machine2machine

Kalender &
Abstimmungen

Sicher E-Mail-
Anhänge versenden

Alleinstellungsmerkmale / USP

(a) Zugriff im Rechenzentrum technisch ausgeschlossen – patentiert

(b) Einzigartiger Schutz von Inhalten & Verbindungsinformationen – zertifiziert

- Patente bereits erteilt in EU und U.S.
- Betrieb in deutschen iDGARD-Rechenzentren
- vom TÜV-IT mit der höchsten Schutzklasse bewertet

→ Dadurch sogar auch für öffentlichen Dienst einsetzbar

→ Zukunftsweisende Technologie für sicheres Cloud Computing: Chats, Nachrichten, Abstimmungen, Wasserzeichen, gemeinsame Bearbeitung, etc.

Bundesministerium für Wirtschaft und Energie

Technologie hinter iDGARD gefördert durch das BMWi

Trusted Cloud

Schutzklasse III - Trusted Cloud Datenschutzprofil

Trusted Cloud Datenschutz-Zertifikat: Vergleichbare Sicherheit & Entlastung des Nutzers

- **Bisher:** Sicherheitsniveaus verschiedener Cloud-Angebote nicht vergleichbar
- **Jetzt:** TCDP mit Schutzklassen, Vergleichbarkeit und verbindlicher Rechtsfolge

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

TÜV-iT-Bewertung: iDGARD erfüllt Schutzklasse III

Zertifizierung und Ergebnis

Deutsches „Trusted Cloud Datenschutzprofil“ (TCDP) Bisherige Empfehlungen werden obligatorisch: ISO/IEC 27002:2013, ISO/IEC 29100:2011, ISO/IEC27018:2014	Schutzklasse III Schutzklasse II Schutzklasse I	⇨ Ergebnis: (a) Schutzbedarf erfüllt (b) Kontrollpflichten des Cloud-Nutzers erfüllt
ISO/IEC 27001:2013 oder BSI IT-Grundschutz		⇨ Ergebnis: Anbieterorganisation arbeitet sorgfältig

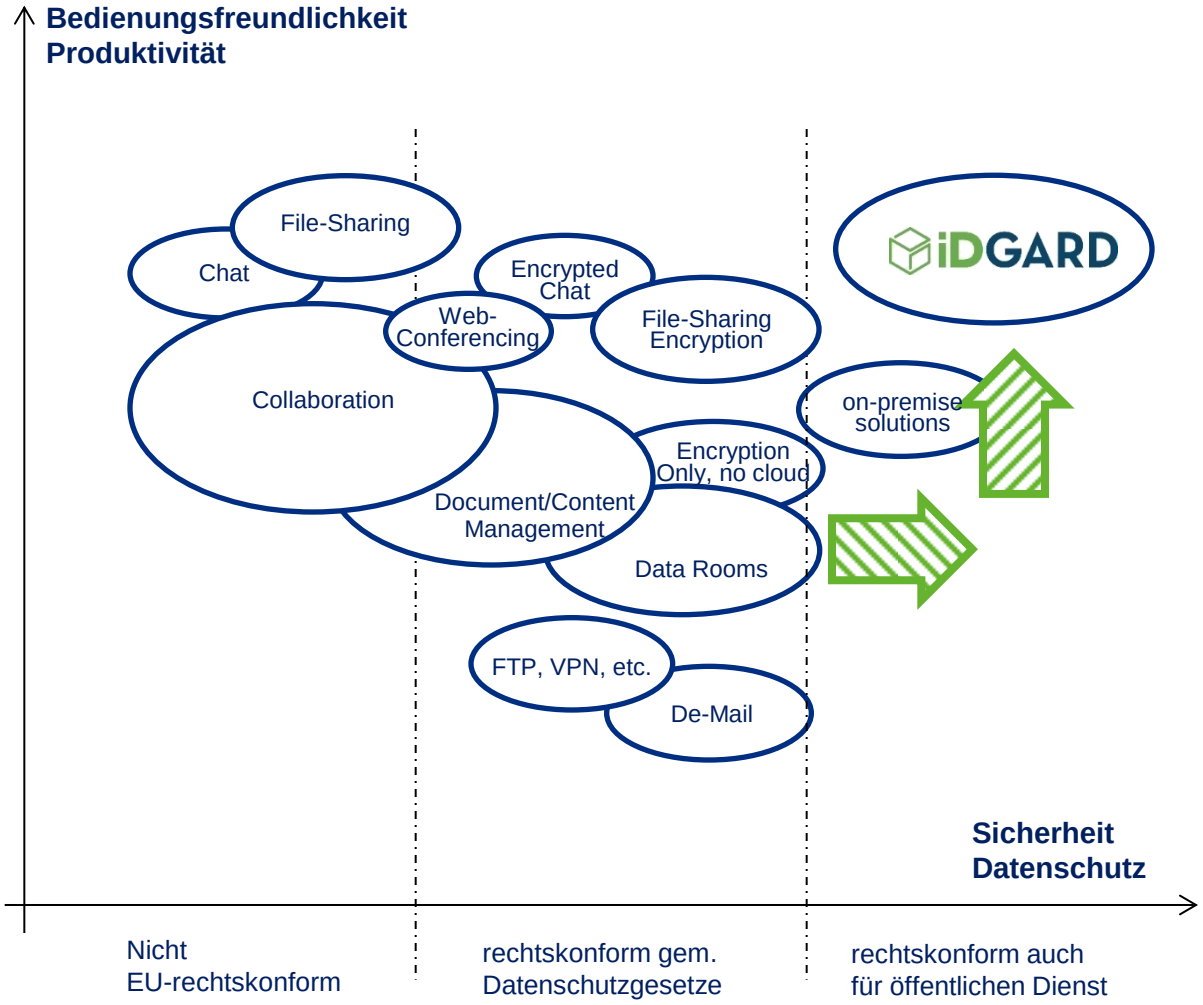
Rahmenbedingungen

- Gesetzlichen Anforderungen (BDSG, später DS-GVO -EU-)
- Schutzklassenkonzept Bedarfsklassen I – III Anforderungsklassen I - III

BSI-Anforderungskatalog Cloud-Computing

- **Entwurf:** Veröffentlichung 4.12. 2015
- **Final:** Januar 2016
- **WP-Testat:** gemäß ISAE 3000

Positionierung und Wettbewerb



Größe der Felder zeigt Funktionsumfang an

Ideale Ergänzung zu Office 365

standard
Office 365
non-compliant

EU-trustee model
Office 365
potentially compliant

Microsoft on premise
potentially compliant

fully compliant

- **Office always up-to-date**
- **Office everywhere available**

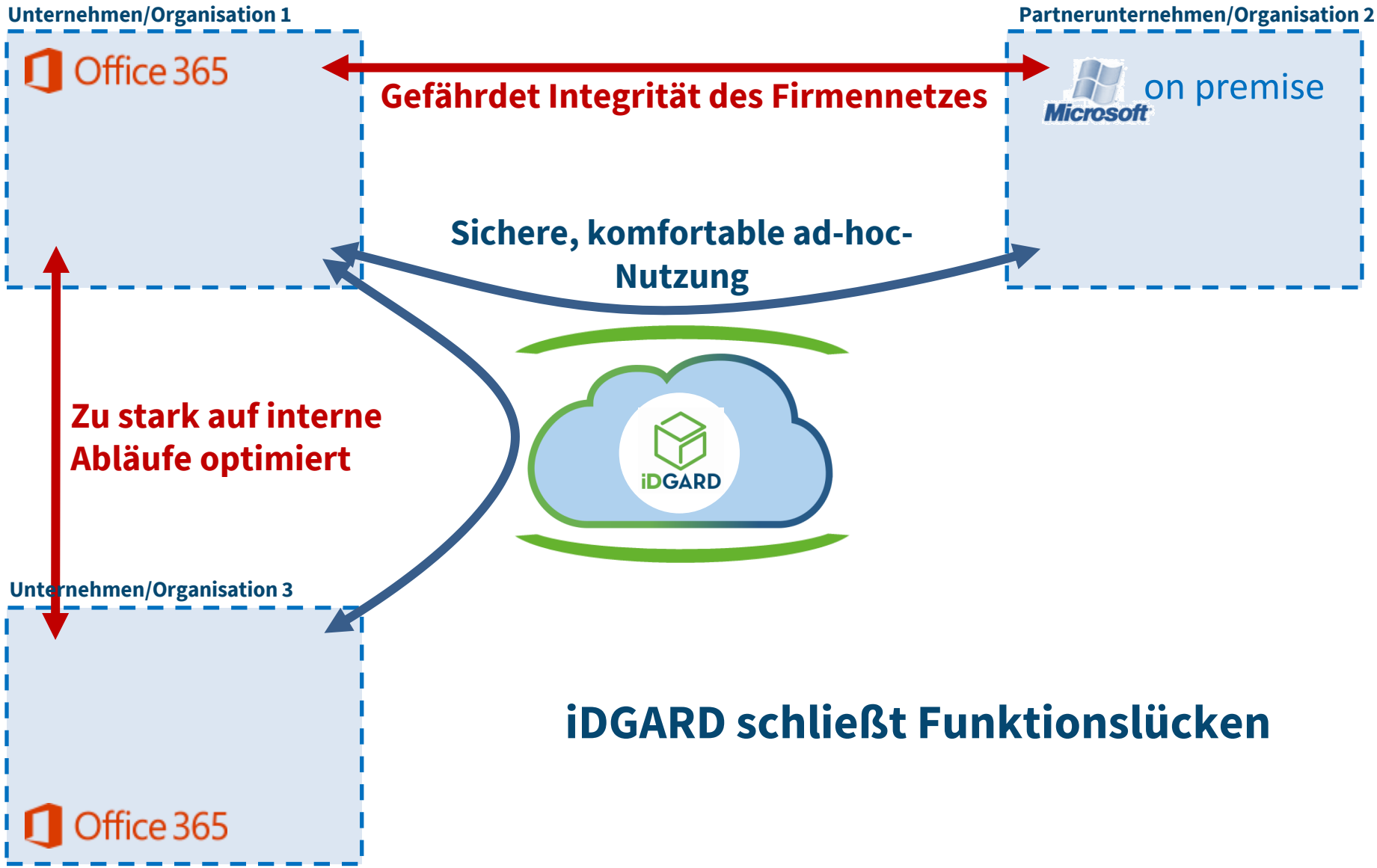
<u>Funktionslücken, die iDGARD schließt:</u>

- **Datenaustausch & Zusammenarbeit über Organisationsgrenzen hinweg**
- **Datenraum-Funktionen**
- **Medium für Dienst- und Privatgeheimnisse**

iDGARD Productivity Tool

iDGARD Sharepoint App

Ideale Ergänzung zu Office 365



iDGARD schließt Funktionslücken

Ideale Ergänzung zu Office 365

Unternehmen/Organisation 1

Office 365

Partnerunternehmen/Organisation 2

Microsoft on premise

- Einfaches Sharing auf einzelne Dateien beschränkt
- Aufwändiges Firewall- & DMZ Handling
- Fehleranfälliges Zertifikats-Handling

- Ad-Hoc Nutzung möglich
- Entlastung der IT durch einfache Selbstadministration
- Volle Kontrolle dennoch bei Admin + hohe Sicherheit

- Zentrales Gruppenmanagement umständlicher, langsamer Prozess
- Rechtemanagement auf interne Abläufe optimiert
- Integration mit 3rd Party schwierig

iDGARD

Unternehmen/Organisation 3

Office 365

Funktionslücken, die iDGARD schließt:

- Datenaustausch & Zusammenarbeit über Organisationsgrenzen hinweg
- Datenraum-Funktionen
- Medium für Dienst- und Privatgeheimnisse

Kontakt

Dr. Hubert Jäger
Geschäftsführer

Uniscon GmbH – The Web Privacy Company

Agnes-Pockels-Bogen 1
80992 München

E-Mail: contact@uniscon.de
Telefon: (089) 41615988-100
www.idgard.de