Sichere Kommunikation mit der Cloud

SLTA Basel und Advokatenkammer Basel

Heinz, Roland und Rainer Steinegger

26.01.2022

Motivation

- Mündig zu entscheiden welche Cloud-Dienste akzeptabel sind
- Beurteilung von Cloud-Diensten
- Beurteilung der Risiken

Inhalt

1. Generelle Gefahren/Risiken mit Cloud-Diensten
2. Gefahren bezüglich Zugriff erkennen
   a. Kommunikationswege und Verschlüsselung
   b. Drei Kategorien zur Einordnung von Cloud-Diensten
3. Risikoabschätzung für Cloud-Anbieter
4. Live Vorführung leguli
5. Quellen

Generelle Gefahren/Risiken mit Cloud Diensten

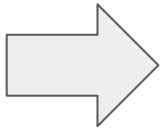
Qualitative Beurteilung der Datensicherheit für eine Verarbeitung in Europa

1. Mögliche Gefahren bezüglich Vertraulichkeit, Integrität und Verfügbarkeit von Daten
2. Gruppiert nach Themenbereichen die alle Gefahren abdecken
3. Klassifizierung nach
   a. Zukünftige Entwicklung der möglichen Gefahren
   b. Abhängigkeit von Art der Anwendung/Cloud
4. Reihenfolge nach Gefahrenpotential, hoch -> niedrig
5. Allgemeine Risikobeurteilung bei verschiedenen Anwendungsmöglichkeiten
   a. On Premise
   b. Cloud Hyperscaler
   c. CH Cloud
   d. Cloud mit Ende-zu-Ende Verschlüsselung und Schlüsselkontrolle

Mögliche Gefahren, 1. Eigene Mitarbeiter

Vertraulichkeit, Integrität und Verfügbarkeit von Daten

- Zukünftige Entwicklung



- Generell, unabhängig vom Einsatz in der Cloud

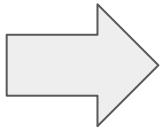
Eigene Mitarbeiter

- Social Engineering
- Geräte für unbefugte zugänglich
- Passwort für unbefugte zugänglich
- Schlüssel für unbefugte zugänglich
- Unbekannten Mailanhang öffnen
- Unbekannte USB Sticks benutzen
- Unverschlüsselten Internetseiten benutzen
- Benutzung unbekannter Programme

Mögliche Gefahren, 2. Inhouse IT, Organisation

Vertraulichkeit, Integrität und Verfügbarkeit von Daten

- Zukünftige Entwicklung



- Generell, unabhängig vom Einsatz in der Cloud

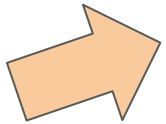
Inhouse IT, Organisation

- Benutzung veralteter Software und Bibliotheken
- Virenscanner nicht aktuell
- Firewall nicht aktuell
- Unverschlüsselte Datenübertragung
- Unverschlüsselte Datenspeicherung
- Schlüssel für andere zugänglich
- Zugangsmanagement (neue/ehemalige Mitarbeiter)
- Unsachgemässe Entsorgung von Speichern

Mögliche Gefahren, 3. Dienstleister

Vertraulichkeit, Integrität und Verfügbarkeit von Daten

- Zukünftige Entwicklung



- Abhängig vom Einsatz in der Cloud

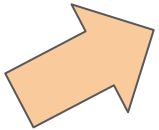
Dienstleister

- Ungenügender Schutz vor Datenverlust
- Ungenügender Schutz vor Datenzugriff von Dritten
- Unberechtigter Datenzugriff durch Mitarbeiter
- Ungenügender Schutz von Passwörtern
- Ungenügender Schutz von Schlüsseln
- Ungenügender Schutz der Integrität der Daten

Mögliche Gefahren, 4. Zukunftsfähigkeit

Vertraulichkeit, Integrität und Verfügbarkeit von Daten

- Zukünftige Entwicklung



- Abhängig vom Einsatz in der Cloud

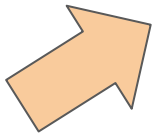
Zukunftsfähigkeit

- Zukunftsfähigkeit
  - Ungeeignetes Konzept
  - Ungeeignete Technologie
  - Ungeeignete Dienstleister
  - Keine Datentransparenz
  - Kein Potential für Weiterentwicklung
  - Keine Integration in neue Systeme
- Abhängigkeit vom Anbieter
  - Lock-in-Effekt
  - Keine Fehlerbehebung
  - Kein transparenter Zugang zu den Daten
  - Keine Weiterentwicklung

Mögliche Gefahren, 5. Staatlicher Zugang

Vertraulichkeit, Integrität und Verfügbarkeit von Daten

- Zukünftige Entwicklung



- Abhängig vom Einsatz in der Cloud

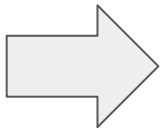
Staatlicher Zugang

- Staatlicher Zugang
  - US Cloud Act
  - Behördlicher Zugang
- Nachrichtendienste
  - US Nachrichtendienste wie NSA
  - Nachrichtendienste anderer Länder

Mögliche Gefahren, 6. Fehler in SW/HW

Vertraulichkeit, Integrität und Verfügbarkeit von Daten

- Zukünftige Entwicklung



- Abhängig vom Einsatz in der Cloud

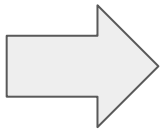
Fehler in SW/HW

- Softwarefehler
  - Fehler der Software vom Dienstleister
  - Schwachstelle in der Netzwerksoftware
  - Schwachstelle in verwendeten Bibliotheken
- Hardwarefehler
  - Physikalischer Netzwerkfehler
  - Schwachstelle im Netzwerk/Verkabelung
  - Defekte Speichermedium

Mögliche Gefahren, 7. Äussere Einflüsse

Vertraulichkeit, Integrität und Verfügbarkeit von Daten

- Zukünftige Entwicklung



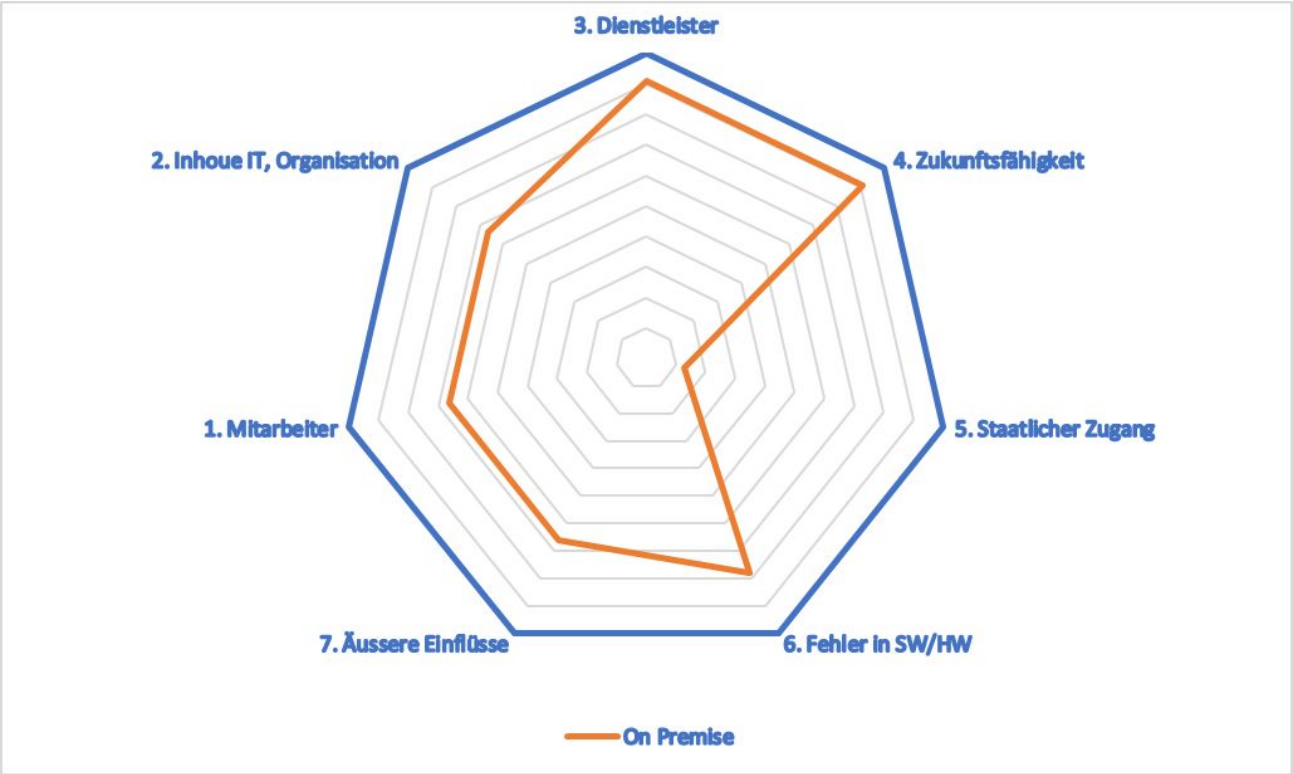
- Generell, unabhängig vom Einsatz in der Cloud

Äussere Einflüsse

- Erdbeben
- Hochwasser
- Blitzeinschlag
- Stromausfall
- Politische Unruhen

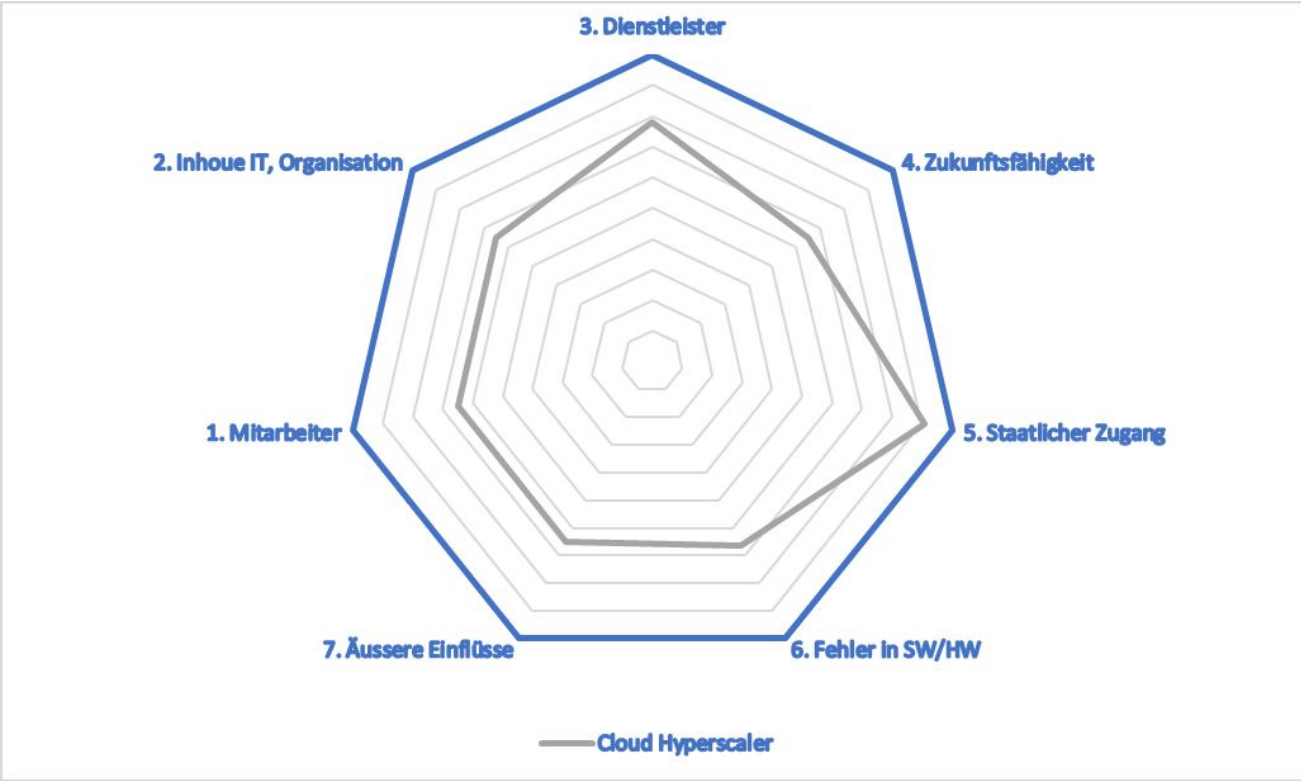
Allgemeine Risikobeurteilung bei Anwendungsarten

On Premise



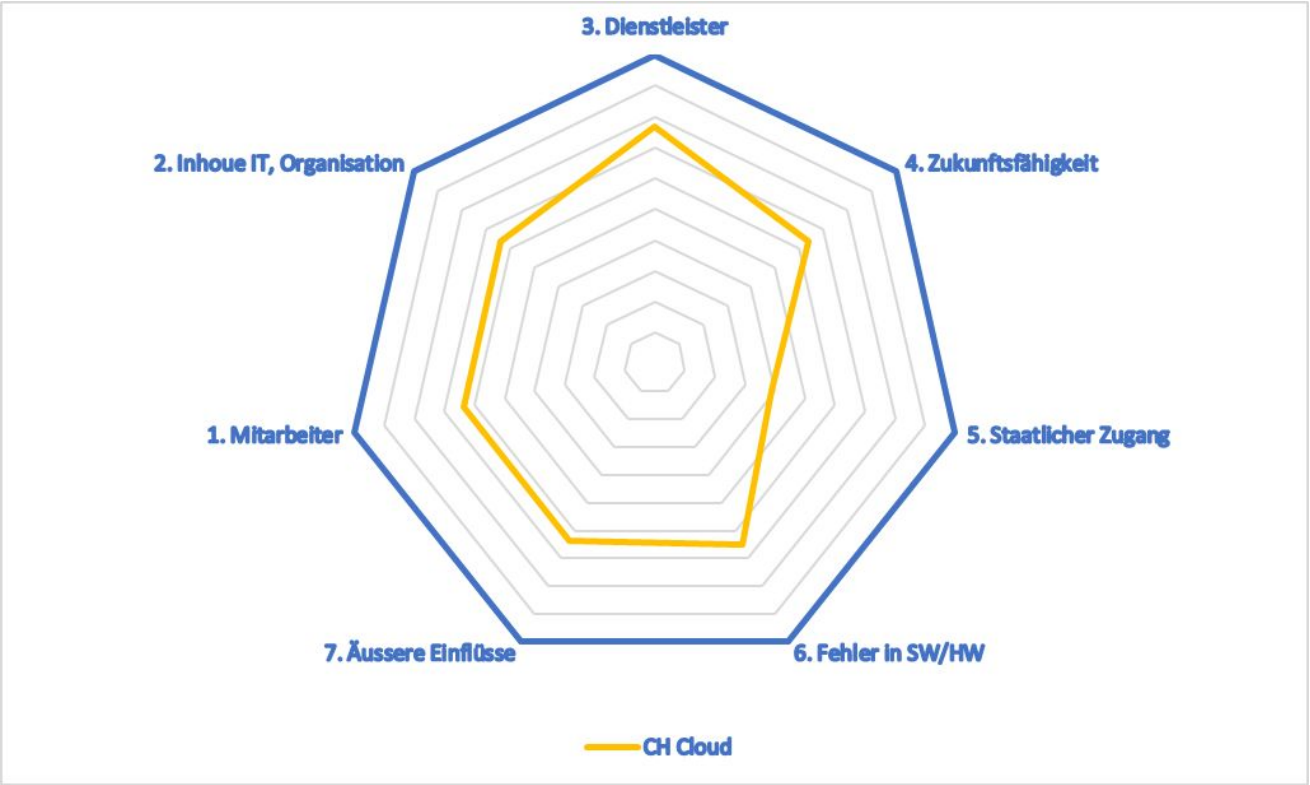
Allgemeine Risikobeurteilung bei Anwendungsarten

Cloud
Hyperscaler



Allgemeine Risikobeurteilung bei Anwendungsarten

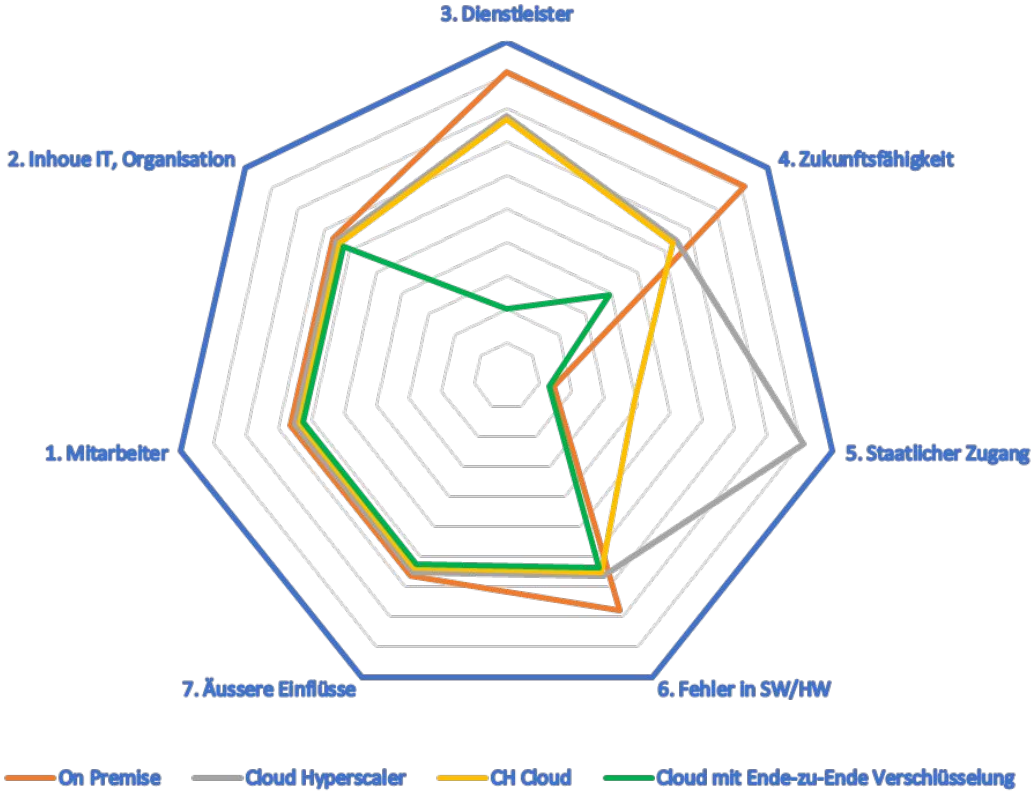
CH Cloud



Allgemeine Risikobeurteilung bei Anwendungsarten

Cloud mit Ende-zu-Ende Verschlüsselung und Schlüsselkontrolle

Allgemeine Risikobeurteilung bei Anwendungsarten



Kategorien zur Einordnung von Cloud-Anbietern

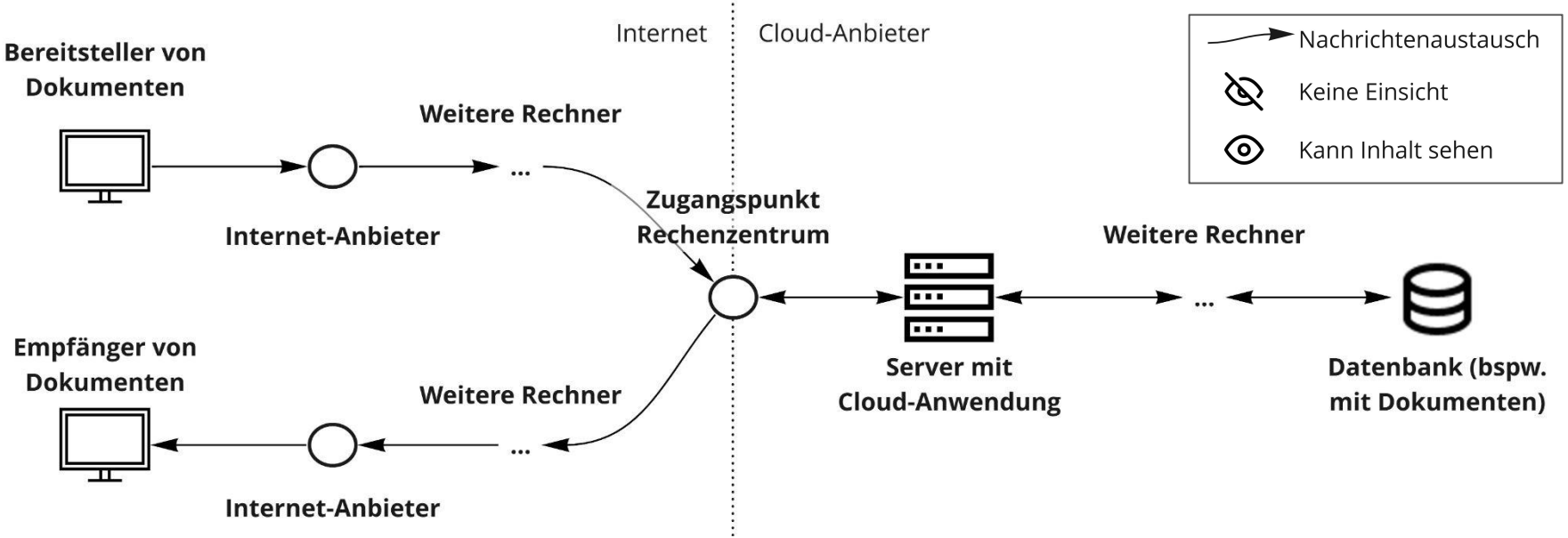
1. Daten sind vor Einsicht geschützt
   - Zugriff durch Dritte ausgeschlossen
   - Open-Source erhöht Vertrauen in Verschlüsselung
2. Kein Schutz vor Anbieter, aber EU/Schweizer Unternehmen
   - Einsichtnahme des Anbieters in Daten, die bspw. dem Anwaltsgeheimnis unterliegen
   - Anbieter (Entwickler, Support, ...), Rechenzentrum und evtl. Dritte Dienstleister könnten Daten einsehen
   - Personenkreis mit Zugriffsrechten nicht kontrolliert
3. Kein Schutz vor Anbieter und US-Unternehmen beteiligt
   - Unbemerkter Zugriff bspw. durch US-Geheimdienste möglich und bei Finanzen auch wahrscheinlich (Terrorismusabwehr)
     (Cloud Act, Patriot Act, FISA, Freedom Act)
   - Günstiger Preis → "Sie sind das Produkt" → Daten werden vermutlich automatisiert verarbeitet

Zugriff ausgeschlossen?
Ende-zu-Ende-Verschlüsselung?

- Warum ist fehlende Ende-zu-Ende-Verschlüsselung eine Gefahr?
  - Anwaltsgeheimnisse,
  - Personenbezogene Daten und
  - weitere Geheimnisse sind einsehbar
- Einsicht des Cloud-Dienstanbieters
  - Daten sind üblicherweise für (alle) EntwicklerInnen einsehbar, um bspw. die Fehlerbehebung zu erleichtern
  - Support hat üblicherweise Zugriff auf die Daten
  - Zugriffseinschränkungen à la "Daten nicht für Support freigeben" wirken nur in der Support-Software und können umgangen werden
- D.h. vertrauliche Informationen werden grossem, unbekanntem und unkontrollierbarem Personenkreis zugänglich gemacht

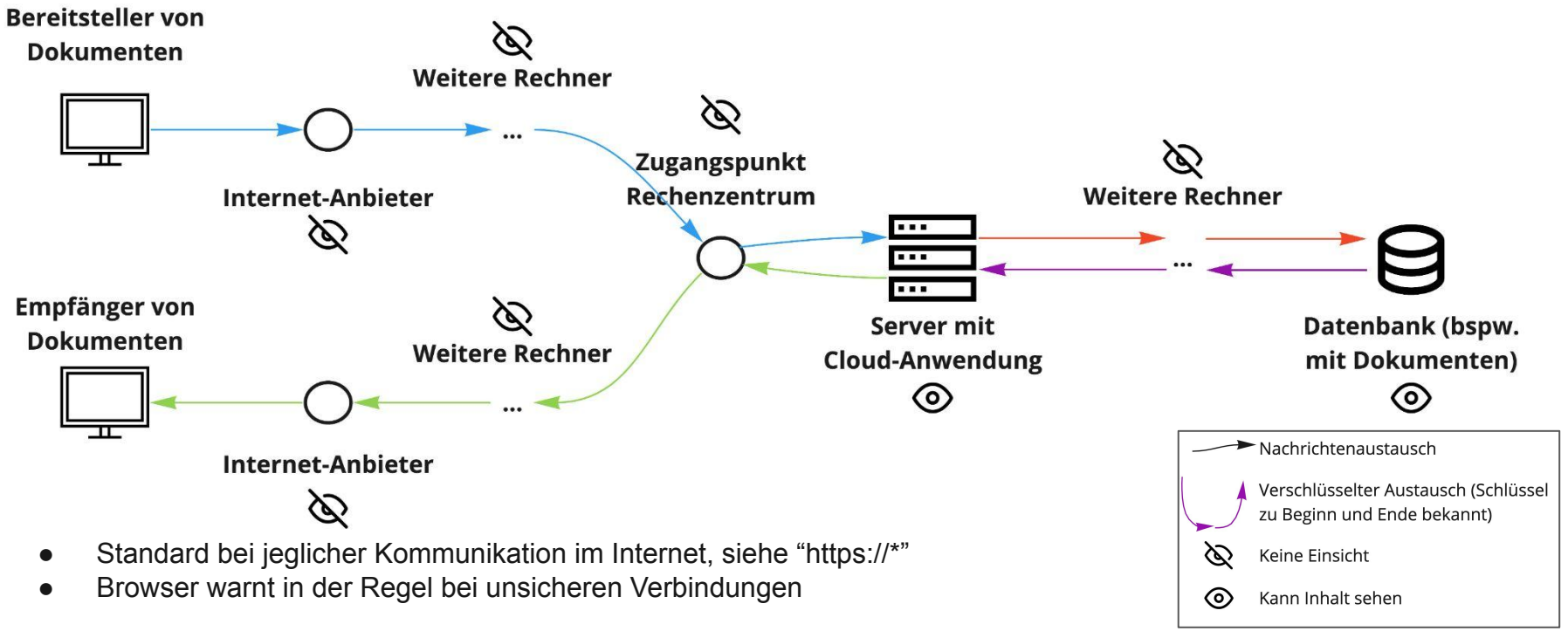
ⓘ Extremes Praxisbeispiel: Entwickler nutzen Produktionsdaten zur Entwicklung auf dem eigenen PC (nicht selten)

Verschlüsselung in Cloud-Anwendungen – Kommunikationswege



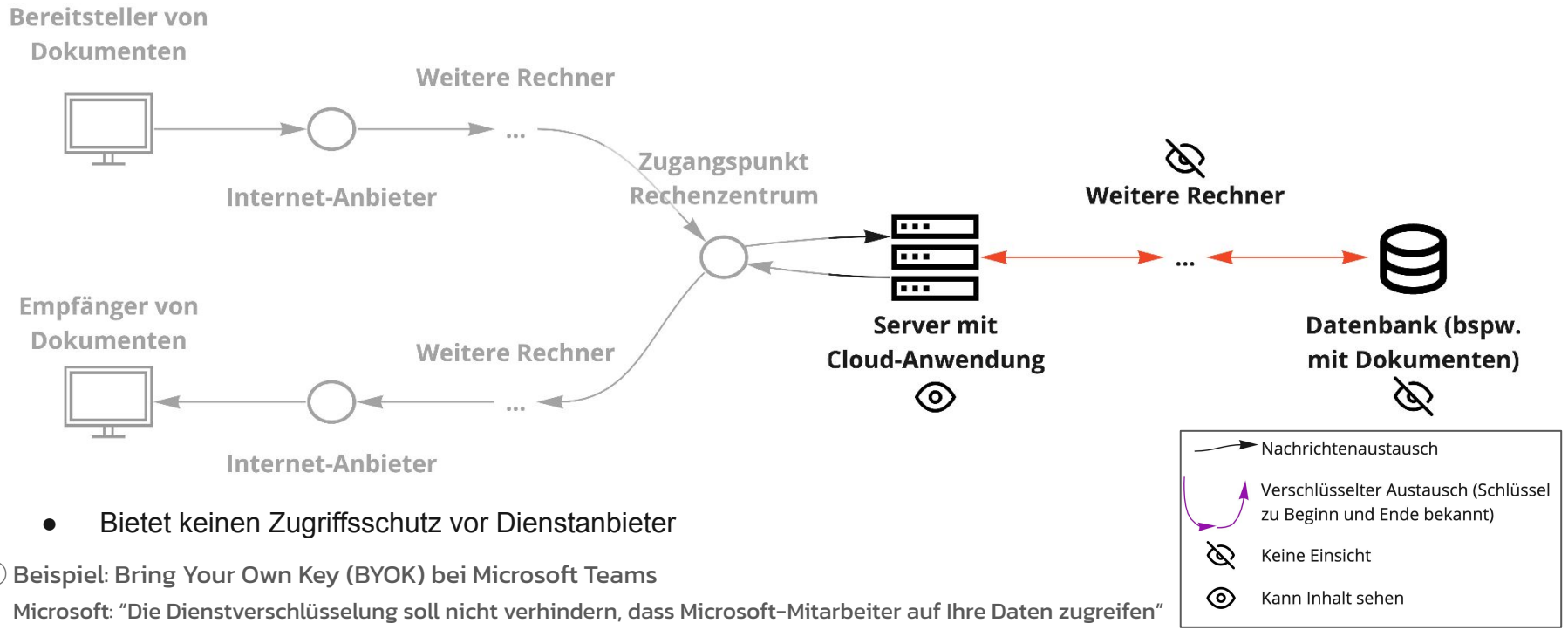
- Typische Beteiligte bei der Bereitstellung von Dokumenten
  - Bereitstellerin lädt Dokument bei Cloud-Anwendung hoch, welche diese in einer Datenbank speichert
  - Empfängerin greift auf Cloud-Anwendung zu und lädt Dokument herunter
  - Internet-Anbieter und weitere Rechner leiten Anfragen an die Kommunikationsparteien weiter

Transportverschlüsselung (data in transit)



- Standard bei jeglicher Kommunikation im Internet, siehe “https://*”
- Browser warnt in der Regel bei unsicheren Verbindungen

Verschlüsselte Datenablage (data at rest)

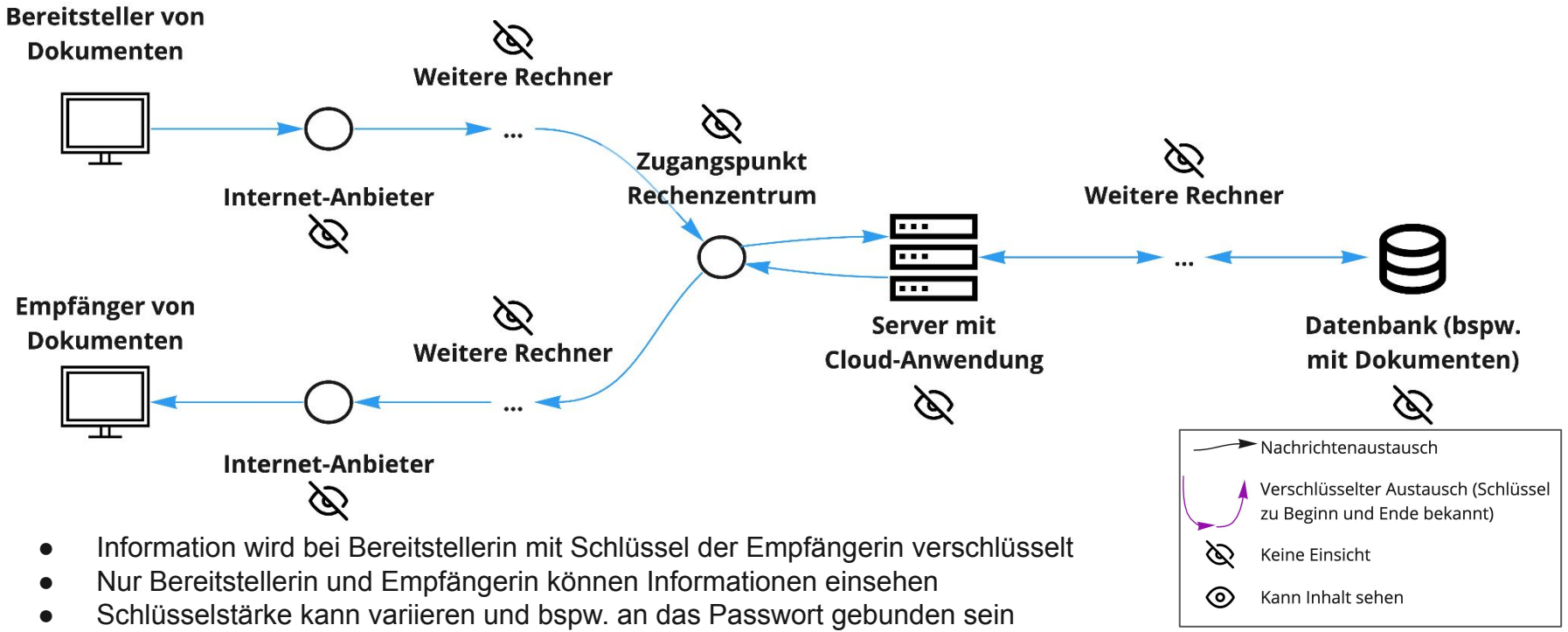


- Bietet keinen Zugriffsschutz vor Dienstanbieter

ⓘ Beispiel: Bring Your Own Key (BYOK) bei Microsoft Teams

Microsoft: "Die Dienstverschlüsselung soll nicht verhindern, dass Microsoft-Mitarbeiter auf Ihre Daten zugreifen"

Ende-zu-Ende-Verschlüsselung



- Information wird bei Bereitstellerin mit Schlüssel der Empfängerin verschlüsselt
- Nur Bereitstellerin und Empfängerin können Informationen einsehen
- Schlüsselstärke kann variieren und bspw. an das Passwort gebunden sein

Checkliste Ende-zu-Ende-Verschlüsselung

Kriterium	Ende-zu-Ende verschlüsselt	Daten vom Anbieter einsehbar
Keywords auf Webseite	Verschlüsselung im Browser, User-zu-User-Verschlüsselung, Ende-zu-Ende-Verschlüsselung	Sicher, Sichere Ablage, Sichere Kommunikation, Verschlüsselte Kommunikation (Kein Keyword von links, stattdessen allgemeine Aussagen)
Schlüssel	Auf Sicherung eines (Backup-) Schlüssels wird hingewiesen	Keine Hinweise auf Schlüssel oder nur Schlüssel für Ablage (siehe Verschlüsselte Datenablage)
Dokumentenfreigabe	Keine Freigabe ohne Passwort oder vorherige Anmeldung der Empfängerin	Freigabe von Dokumenten per Link ohne zusätzlichen Schutz
Automatische Datenverarbeitung	Eingeschränkt im Browser oder gesondertem Desktop-Client möglich	Dokumente werden automatisiert verarbeitet, z.B. integrierte Virenprüfung oder Volltextsuche
Passwortzurücksetzen/ Passwort ändern	Kein Passwortzurücksetzen ohne altes Passwort möglich, falls kein gesonderter Schlüssel vorhanden	Einfach möglich

Checkliste Sicherheitsniveau

Kriterium	Erhöhtes Sicherheitsbewusstsein	Geringeres Sicherheitsniveau
Fremdzugriff von Dritten	Datenschutzerklärung schliesst dies aus	Datenschutzerklärung mit US-bezug oder Verweis auf Weiterverarbeitung (durch Dritte)
Anmeldung an neuen Geräten	Erfordert Eingabe des Schlüssels (bei Ende-zu-Ende-Verschlüsselung)	Erfordert nur die Passworteingabe
ISO-27001-Zertifizierung	Zertifiziert: gewisses Sicherheitsverständnis	Keine Zertifizierung
E-Mails des Anbieters	Möglichkeit E-Mails selbst zu versenden d.h. Eigenes E-Mail-Programm öffnet sich beim Versenden von (Kunden-) E-Mails (Anbieter will Kenntnisnahme der E-Mail-Adresse vermeiden)	Enthalten schützenswerte Informationen (Anbieter hat Zugriff auf diese Daten und Schutz ist ihm nicht wichtig) - Passwörter im Klartext - Namen oder andere Daten ihrer Kunden - Dateinamen
Passwörter	Keyword: “Zero-Knowledge”-Beweis beim Passwort (Keine Übertragung des Passworts zum Anbieter)	Passwörter im Klartext im Profil oder E-Mails

Abschätzung Sicherheit vs. Benutzbarkeit

- Höheres Sicherheitsniveau schränkt (oft) die Benutzbarkeit der Anwendung ein
  Beispiele:

1) Dokumente per E-Mail verschicken vs.
   Freigabe von Dokumenten per Download-Link vs.
      Zusätzliches Passwort oder Account bei Dateifreigabe

2) Keinerlei Anmeldedaten zur Dateifreigabe vs.
   Benutzername und Passwort zur Anmeldung vs.
      Zusätzlicher Schlüssel bei Anmeldung

3) Personalisierte Suchvorschläge und Werbung vs.
   Volltextsuche der Dokumente und Daten im Web vs.
      Volltextsuche im lokalen Dateisystem, weil Online-Suche ausgeschlossen

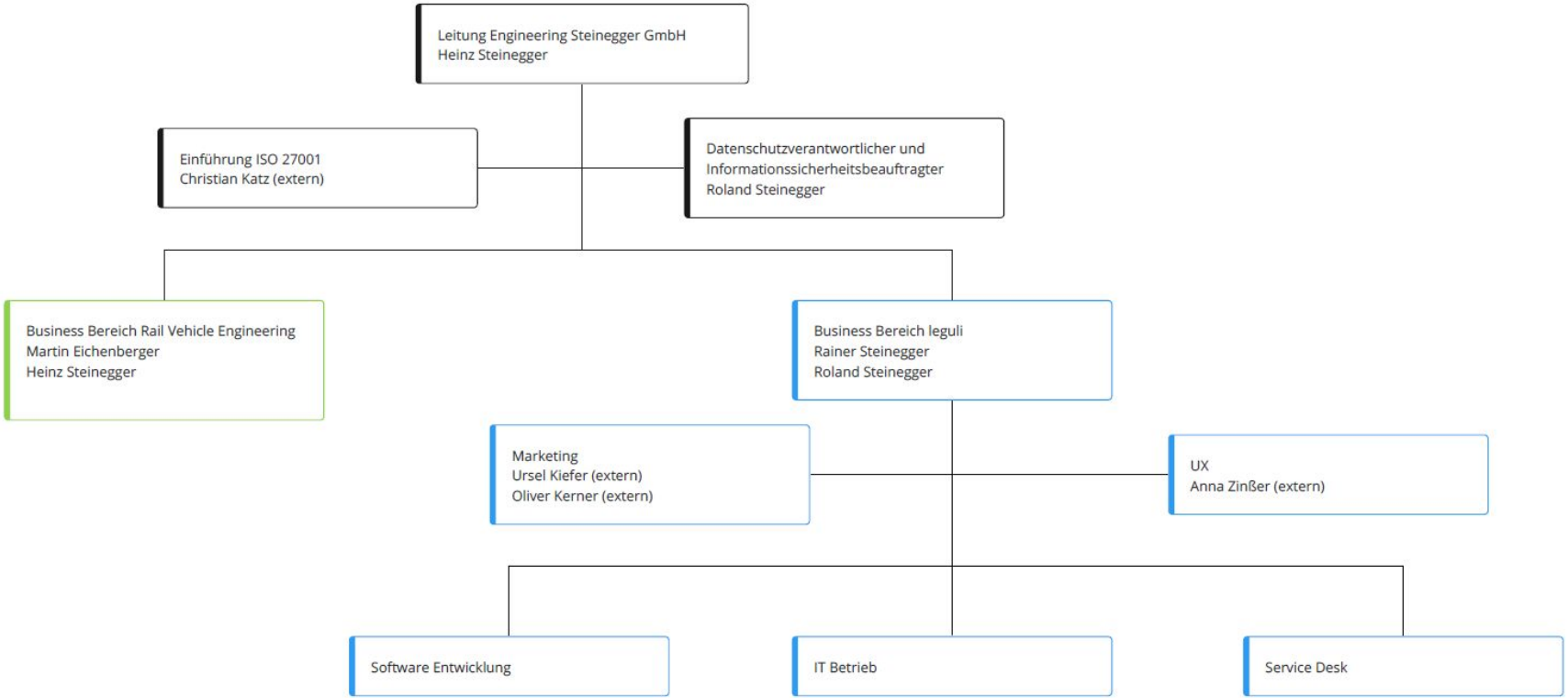
Risikoabschätzung für Cloud-Anbieter

- Zu schützende Daten identifizieren
  - Was habe ich für Daten?
    z.B. Dokumente, E-Mails, CRM (Adressen, Kontakte etc.) “Projektmanagement” (Aufgaben, Vorgänge etc.)
- Schutzbedarf ermitteln
  - Wie sicher müssen die Daten gehalten werden?
    z.B. Datenschutzrelevant, eigene und fremde Firmengeheimnisse, Verhandlungsrelevante Geheimnisse haben eher hohen Schutzbedarf
- Risiko abschätzen
  - Schutzbedarf x Bedrohungslage/Angriffswahrscheinlichkeit
    z.B. Hoher Schutzbedarf x Hohe Angriffswahrscheinlichkeit
    = Starke Schutz-Massnahmen notwendig
  - Bei Informationen zu Finanztransaktionen erhöhtes Interesse der USA

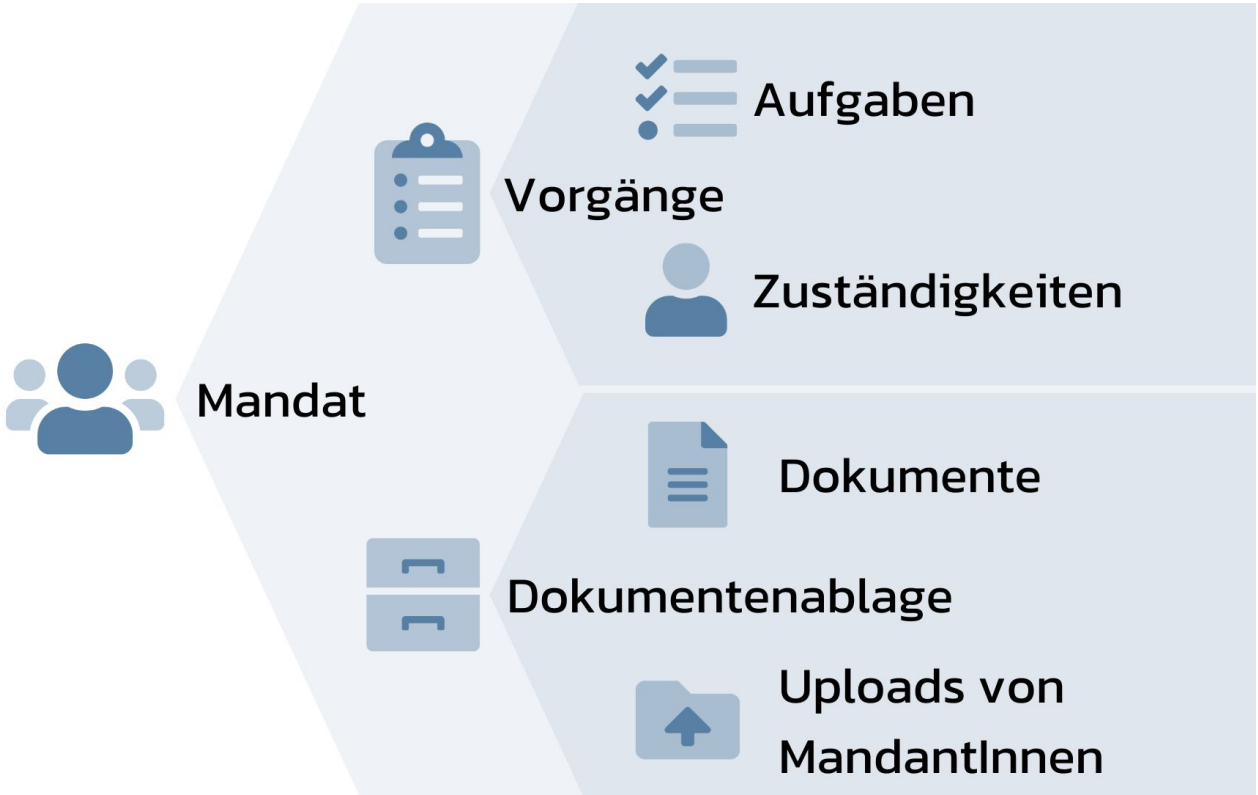
Zusammenfassung

- Risikobewertung bei Wahl von Cloud-Anbieter notwendig
  - Welche schützenswerten Daten habe ich?
  - Welche Gefahren gibt es?
  - Wie gross sind die Risiken?
- Weitere Massnahmen bei Wahl eines Anbieters ohne Ende-zu-Ende-Verschlüsselung notwendig
  - Anbieter muss Zusicherungen über verantwortungsvolle Verarbeitung geben
    Verantwortung liegt bei Ihnen (Stichwort: Auftragsdatenbearbeitung)
  - Offenlegung der Daten birgt Risiken, da Sicherheitsverständnis bei Anbietern oft gering
- Hohe Sicherheit schliesst Benutzbarkeit nicht aus
- Checkliste erleichtert Einordnung von Anbietern

Vorstellung leguli – Engineering Steinegger GmbH



Struktur leguli



Vorführung leguli

Informationen auf der Homepage von leguli: leguli.ch

Im Linkedin: leguli

leguli 14 Tage kostenlos testen, alle Daten bleiben bei einem Kauf erhalten!

Für weitere Informationen stehen wir jederzeit gerne zur Verfügung:

Mail: kontakt@leguli.ch

Telefon: +41 61 813 36 06

Vielen Dank!

Quellen

Empfehlungen des SAV FSA bei der Nutzung von Cloud Diensten:

https://digital.sav-fsa.ch/digitale-kanzlei-nutzung-von-clouddiensten

Informationen zu Log4j:

https://www.govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/

Umgang mit Kundendaten bei Amazon:

https://www.golem.de/news/amazon-schwere-vorwuerfe-zum-umgang-mit-daten-2111-161276.html

Umgang mit Berufsgeheimnissen in der Cloud:

https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf

Dokumentation des wissenschaftlichen Dienstes des deutschen Bundestags zum Zugriff US-amerikanischer Behörden auf Daten:

https://www.bundestag.de/resource/blob/796102/ea53ffe8e08a9ab11e270719263d8c53/WD-3-181-20-pdf-data.pdf