VISCHER

Cloud 101 für Juristinnen und Juristen.

Damit Sie mitreden können

David Rosenthal
9. Dezember 2021

Bundesverwaltung setzt Cloud-Strategie um – für eine geordnete und effiziente Nutzung von Clouds

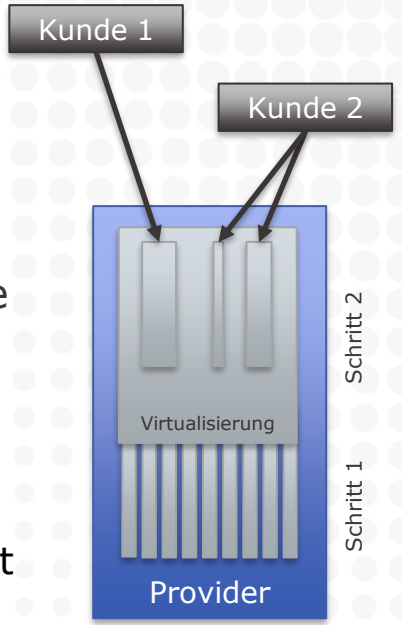
(Letzte Änderung 10.11.2021)

Bern, 10.11.2021 - Der Einsatz von Cloud-Diensten unterstützt die digitale Transformation der Bundesverwaltung. Mit der WTO-Beschaffung «Public Clouds Bund» kann der Bund künftig hochskalierbare Cloud-Dienste flexibel beziehen. Mit dem Rückzug der Beschwerde im Verfahren können nun alle Arbeiten weitergeführt werden.

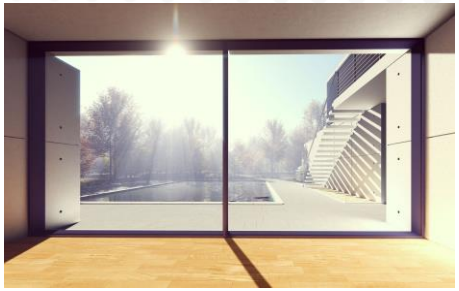
www.admin.ch

Was ist eine (Public) Cloud?

- **Gemietete Rechner- und Speicherkapazität** eines von vielen genutzten Rechenzentrums bzw. RZ-Verbunds
  - Inklusive mehr oder weniger Software (inklusive Unterhalt)
  - Zugriff via Internet
  - Leistung wird hochstandardisiert und automatisiert erbracht
- **Marktführer:** Amazon Web Services (AWS), Microsoft, Google
- Sie sind **"Hyperscaler"**
  - Schritt 1: Bündelung der Kapazität beliebig vieler einzelner physischer Computer- und Speichersysteme
  - Schritt 2: Beliebige, kundenspezifische Stückelung der Kapazität in Form "virtueller" Computer- und Speichersysteme



Von der Kaltmiete zum möblierten Zimmer …



- Infrastructure-as-a-Service ("IaaS") oder Platform-as-a-Service ("PaaS")
- Leeres Zimmer, mit Eingang, Strom und Wasser und bei "PaaS" mit Küchenzeile, Einbauschränken, Lampen, Internet
- Virtueller Server, ggf. mit Systemsoftware

- Software-as-a-Service ("SaaS")
- Ein wohnbereites Zimmer, mit Reinigungs- und weiteren Services
- Online-Softwarelösung (z.B. Mail-Server, CRM-Lösung)
- Variante: Nutzung als Untermieter

Bilder: Pixabay

Cloud-Angebote (Beispiele)

Swisscom

Snowflake

Microsoft Azure

salesforce

Microsoft 365

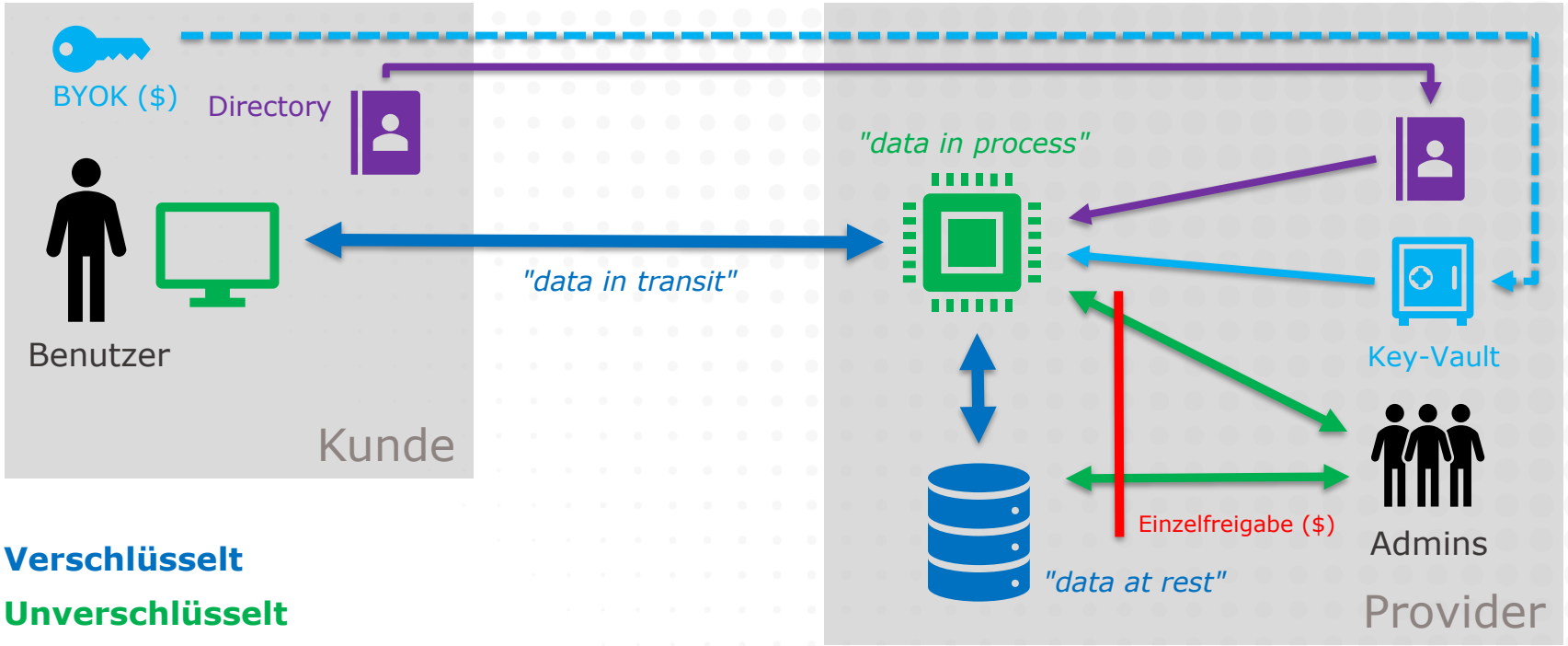
AWS EC2

AWS S3

Google Workspace

Google Cloud

Ein typisches Cloud-Schutzkonzept

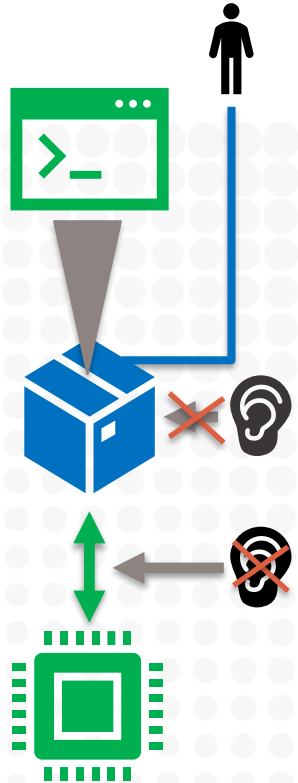


Verschlüsselt

Unverschlüsselt

Nochmals zur Verschlüsselung …

- "Hold-your-own-key" (HYOK) taugt nur in wenigen Fällen, da auch die Systeme die Daten nicht im Klartext lesen können
- "Bring-your-own-key" (BYOK) ist dort relevant, wo der Kunde der Schlüsselgenerierung des Providers nicht vertrauen will
- "Customer-managed Key" ist dort relevant, wo der Kunde alle Daten auf einen Schlag unbrauchbar machen können will
- In fast allen Szenarien könnte ein Provider die dem Prozessor übergebenen Daten durch "Aushorchen" im Klartext lesen
  - Ausnahmen sind HYOK und "Confidential Computing" (wo die Entschlüsselung erst innerhalb des Prozessors erfolgt)
- Andere Schutzmassnahmen denkbar (z.B. Speicherstruktur)



Typische Schutzmassnahmen

Auch grosse Provider wie z.B. AWS erfüllen diese Vorgaben ohne Vertragsanpassungen oft noch nicht

- Verschlüsselung
- Weitere Massnahmen zur Datensicherheit des Providers
- Regelmässige Audit-Berichte betr. deren Umsetzung
- Geolokalisation der Datenspeicherung (und ggf. der Zugriffe)
- Zugriff durch Mitarbeiter des Providers nur mit Einzelfreigabe
- Auftragsbearbeitungsvertrag, der auch das DSG berücksichtigt
- Schutz von Personendaten auch für Berufsgeheimnisdaten
- Vertraulichkeitsverpflichtung mit "Defend-your-data"-Klausel
- FINMA-regulierte Institute: Zusatzvereinbarung zur Einhaltung der Vorgaben des Outsourcing-Rundschreibens der FINMA

Weiterführende Literatur

- Mit Berufsgeheimnissen in die Cloud (Jusletter)
  - https://bit.ly/3pvvgJ5, https://bit.ly/3EqF4dA
- Modell zur Beurteilung des Lawful-Access-Risikos
  - https://bit.ly/3lzUmW7
- Beiträge über Schweizer Banken in der Cloud
  - Praxisbericht/Blog: https://bit.ly/3rDrKPs
  - Vortrag: https://bit.ly/3Esi0ei
  - Checkliste: https://bit.ly/3orfqA0
- Beitrag über M365 für Anwälte (Anwaltsrevue)
  - https://bit.ly/3prkOSX

ANWALTSPRAXIS / PRATIQUE DU BARREAU

MICROSOFT CLOUD FÜR SCHWEIZER ANWÄLTE

DAVID ROSENTHAL
Partner bei VISCHER AG

Stichworte: Cloud, Microsoft, Berufsgeheimnis, M365, Outsourcing

Immer mehr Unternehmen wechseln mit ihren Office-Anwendungen in die Microsoft Cloud. Eine wachsende Zahl von Schweizer Anwaltskanzleien will dies ebenfalls tun oder hat es schon getan. Dieser Beitrag erläutert, welche vertraglichen Voraussetzungen dafür geschaffen werden müssen. Die bisherigen Standardverträge des Marktführers in diesem Bereich genügen jedenfalls nicht. Wann bietet Microsoft eine Lösung, die für alle Anwälte zugänglich sind?

Um es vorwegzunehmen: Technisch gesehen, punkto Handhabung und in Sachen Sicherheit erhält Microsofts M365-Service in der Privatwirtschaft praktisch durchwegs gute Noten.[1] Die meisten Unternehmen starten mit Teams (Videokonferenz, Telefonie und andere Gruppenkommunikation), dann folgen die klassischen Office-Anwendungen (die es auch in Online-Varianten gibt), mit Exchange auch der Mail-Server, Sharepoint Online (als Dateiablage) sowie OneDrive for Business (u. a. zum Teilen von Dateien mit Dritten). Diese und weitere Dienste fasst Microsoft unter der Bezeichnung «M365» zusammen. Seltener kommt Azure zur Anwendung, quasi ein Cloud-basierter, virtueller Server, auf dem Kunden eigene Anwendungen installieren und betreiben können – wie ihn aber auch Konkurrenten wie Amazon oder Google anbieten.

I. Ungenügende Standardverträge

Doch nicht in jeder Hinsicht schneidet Microsoft gut ab. Ungenügend ist der Softwarekonzern noch immer hinsichtlich seiner Verträge. Diese genügen für Schweizer Anwälte und andere Berufsgeheimnisträger nicht den gesetzlichen Anforderungen – entgegen dem, was aus einem kürzlichen Bericht in der «Anwaltsrevue» hätte geschlossen werden können.[2] Daher dieser Beitrag zur Klarstellung.

Microsoft bietet zu ihren Standardverträgen für Anwälte zwar ein «Professional Secrecy Addendum» an, aber darin bestätigt Microsoft im Grunde nur, dass sie wisse, dass die Daten des Kunden unter das Berufsgeheimnis fallen können. Es wird mitunter vertreten, das mache sie zu einer Hilfspersonen, was wohl wiederum das Problem des Anwaltsgeheimnisses lösen soll.[3] Das ist jedoch nicht richtig. Das Wissen um die Existenz von Berufsgeheimnisdaten macht noch niemanden zur Hilfsperson, und selbst, wo Microsoft als Hilfsperson zu betrachten ist, sind die Vorgaben aus dem Anwaltsgeheimnis damit (leider) noch nicht eingehalten; gewisse vertragliche Voraussetzungen müssen zusätzlich geschaffen werden. Dies wurde in BGE 145 II 229 verdeutlicht.[4]

Die Voraussetzungen, die eine Auslagerung in die Cloud erfüllen muss, damit sie den gesetzlichen Anforderungen genügt, sind vom Autor an anderer Stelle eingehend diskutiert worden.[5] Hier soll konkret über den Nachbesserungsbedarf der Verträge speziell von Microsoft orientiert werden, damit Anwälte und andere Berufsgeheimnisträger von Microsoft entsprechende Anpassungen verlangen können. Microsoft wird deshalb als einzelne Anbieterin herausgenommen, weil sie in diesem Bereich mit M365 besonders erfolgreich ist und sich deshalb auch in der Anwaltschaft oft die Frage stellt, ob in die Cloud gewechselt werden soll und was zu tun ist.

Faktisch wird diese Entwicklung nicht aufzuhalten sein. Jede Anwaltskanzlei wird zwar für sich selbst eine Risikobeurteilung vornehmen und sich auch entsprechende Alternativen und Ausgestaltungen (wie Backups ausserhalb der Microsoft Cloud) überlegen müssen. Doch auch wenn das Angebot von Microsoft gut erscheint und die Erfahrungen derjenigen, die schon gewechselt haben, diesen Eindruck bestärken mögen, werden auch Schweizer Anwälte über kurz oder lang nicht darum herumkommen, den korrekten Umgang mit ihren Daten und jenen ihrer Klienten und den Betrieb wesentlicher Aspekte ihres Ge-

1 Der Verfasser ist in Cloud-Projekten jeweils auf der *Gegenseite* von Microsoft tätig.
2 DANIEL HÜRLIMANN/MARTIN STEIGER, Auf dem Weg zur digitalen Anwaltskanzlei trotz Berufsgeheimnis und Datenschutz, in: Anwaltsrevue 5/2021, S. 199–205 (https://www.sav-fsa.ch/de/documents/dynamiccontent/199arv0521.pdf [besucht am 4.10.2021]).
3 Ebd., S. 204.
4 Ebd., S. 202 f.; DAVID ROSENTHAL, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter 10. 8. 2020 (https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess.pdf, https://www.rosenthal.ch/downloads/Rosenthal-CloudLawfulAccess-Anhang.pdf [besucht am 4.10.2021]).
5 ROSENTHAL, ibid.

ANWALTS REVUE DE L'AVOCAT 10/2021 443

Anwaltsrevue

VISCHER

Noch Fragen?

drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com