VISCHER

Schweizer Banken

Umgang mit Risiken bei der Auslagerung in die Cloud

David Rosenthal
31. März 2021

Illegale Cloud?

ZOOM UND SKYPE

Berliner Datenschutzbeauftragte warnt abermals vor Microsoft-Produkten

AKTUALISIERT AM 25.05.2020 - 12:03

Der Warnhinweis mit Blick auf die Nutzung der Microsoft-Dienste kam bei dem Konzern nicht gut an. Nachdem er zunächst von der Webseite der Behörde gelöscht worden war, ist er nun wieder abrufbar.

Quelle: www.faz.net

Sensible Personendaten bei Behörden

Datenschützer warnen vor Microsoft-Produkt

Vertrauliche Angaben über die Schweizer Bevölkerung werden mit den Office-Programmen von Microsoft bearbeitet. Dabei besteht die Gefahr, dass sich US-Behörden Zugriff verschaffen, befürchten die kantonalen Datenschützer.

Quelle: Tagesanzeiger vom 25.5.2020

Schweizer Banken in der Cloud?

- Vor drei Jahren undenkbar
- Jetzt: **Alle wollen es**

Was hat sich geändert?

- Irritierende Signale von Datenschützern
- Keine Erfahrung mit der Cloud
- Alles ist ständig in Bewegung
- Schlecht formulierte Verträge
- Fehlende Methodik zur Risikobeurteilung

} **Ratlosigkeit, "Black Box"**

- Keine Frage des "ob", sondern des "wann" und "wie "

Vor zwei Jahren kippte die Stimmung

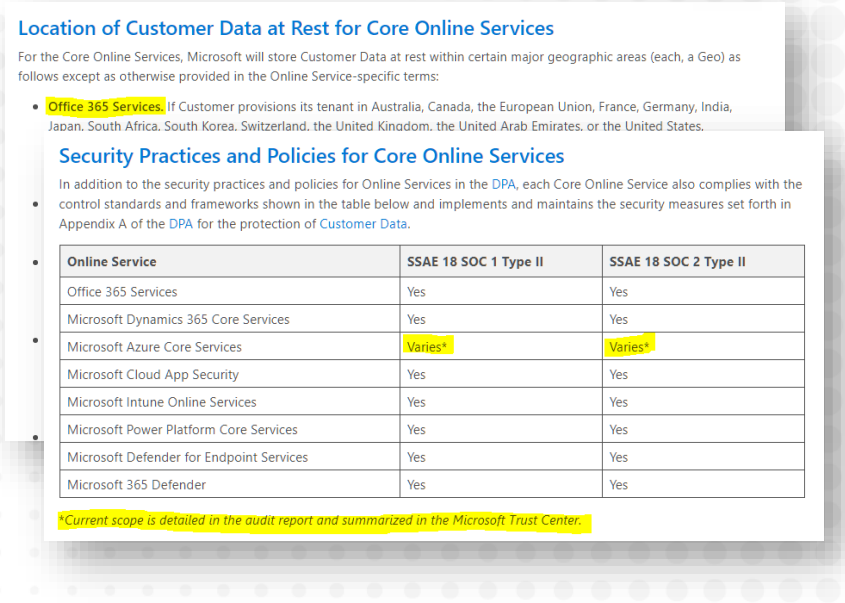
- Der **"Krieg" der Datenschützer** gegen Microsoft
  - Zwei völlig unterschiedliche Welten, die aufeinander treffen
  - Misstrauen, Ohnmacht: Aufbäumen gegen eine Marktmacht
  - In der Sache: Schrems II, Mitarbeiterdaten, Vertragsdrafting

- Entscheidend für die Banken: **Bankgeheimnis**
  - CID einem Dienstleister im Ausland anvertrauen?
  - Bankiervereinigung: Charmeoffensive mit "Cloud-Leitfaden"
  - Gutachten von WalderWyss & Laux: Kein Auslandsverbot
  - Microsoft: Zwei Rechenzentren in der Schweiz
  - Meine Publikation: Methode macht Lawful-Access-Risiko fassbar

Eine andere Welt

- **Datensicherheit** im Grundsatz kein Problem
  - Hyperscaler erhalten sehr gute Noten
- Der Teufel liegt **im Detail**
  - Unzählige verschiedene Services, die jeweils ihre eigenen Regeln haben
  - Wo liegen die Daten? Wo werden sie bearbeitet? Wozu Fernzugriffe?
  - Welche Prüfberichte sind wofür auch vertraglich garantiert?
  - Welche Verschlüsselungsvariante ist wo garantiert?

Ist das ein Problem?



Location of Customer Data at Rest for Core Online Services

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows except as otherwise provided in the Online Service-specific terms:

- Office 365 Services. If Customer provisions its tenant in Australia, Canada, the European Union, France, Germany, India, Japan, South Africa, South Korea, Switzerland, the United Kingdom, the United Arab Emirates, or the United States,

Security Practices and Policies for Core Online Services

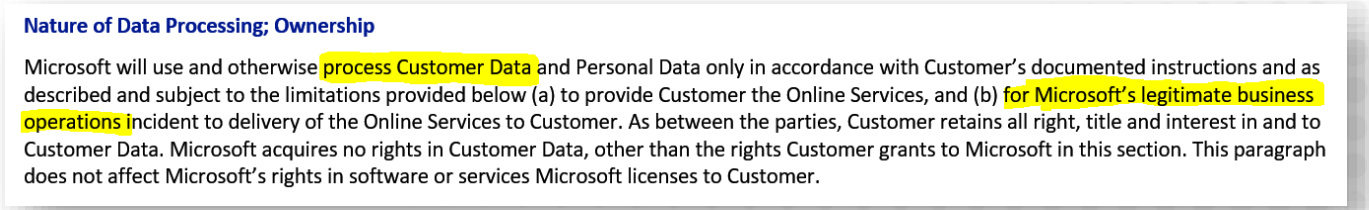
In addition to the security practices and policies for Online Services in the DPA, each Core Online Service also complies with the control standards and frameworks shown in the table below and implements and maintains the security measures set forth in Appendix A of the DPA for the protection of Customer Data.

Online Service	SSAE 18 SOC 1 Type II	SSAE 18 SOC 2 Type II
Office 365 Services	Yes	Yes
Microsoft Dynamics 365 Core Services	Yes	Yes
Microsoft Azure Core Services	Varies*	Varies*
Microsoft Cloud App Security	Yes	Yes
Microsoft Intune Online Services	Yes	Yes
Microsoft Power Platform Core Services	Yes	Yes
Microsoft Defender for Endpoint Services	Yes	Yes
Microsoft 365 Defender	Yes	Yes

*Current scope is detailed in the audit report and summarized in the Microsoft Trust Center.

Gewöhnungsbedürftige Verträge

- **Beispiel Microsoft**
  - Komplizierte Vertragsstruktur
  - Schlechtes Drafting
  - Zu breite oder unspezifische Formulierungen



Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data and Personal Data only in accordance with Customer's documented instructions and as described and subject to the limitations provided below (a) to provide Customer the Online Services, and (b) for Microsoft's legitimate business operations incident to delivery of the Online Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Bearbeitet Microsoft CID im Klartext auch für eigene Zwecke?

  - Woran liegt es?
  - **Wie lösen? Gibt es Alternativen?**

Risiken für das Unternehmen?

+ Reputationsrisiko

- **Datensicherheit** und **Geschäftsfortführung**
  - Zugriff unbefugter Dritter, Ausfall des Providers, Datenverlust
- **Regulatorische Vorgaben, Corporate Governance**
  - Daten in der Schweiz, Datenzugriff, Weisungsrecht, Prüfrechte, direkte Ansprüche gegen Provider, Ausfallrisiken, Rückführung, Subunternehmer, Überwachung des Providers, Konkursrisiko
- **Datenschutz**
  - Vor allem betr. Bearbeitung von Mitarbeiterdaten
  - Risiko für betroffene Personen vs. Risiko für das Unternehmen
- **Bankgeheimnis, vertragliche Geheimhaltung**
  - Ausländischer Lawful Access, Subordination

Risiken wegen …
… der Verträge
… der Technik
… des Handlings
… des Rechts

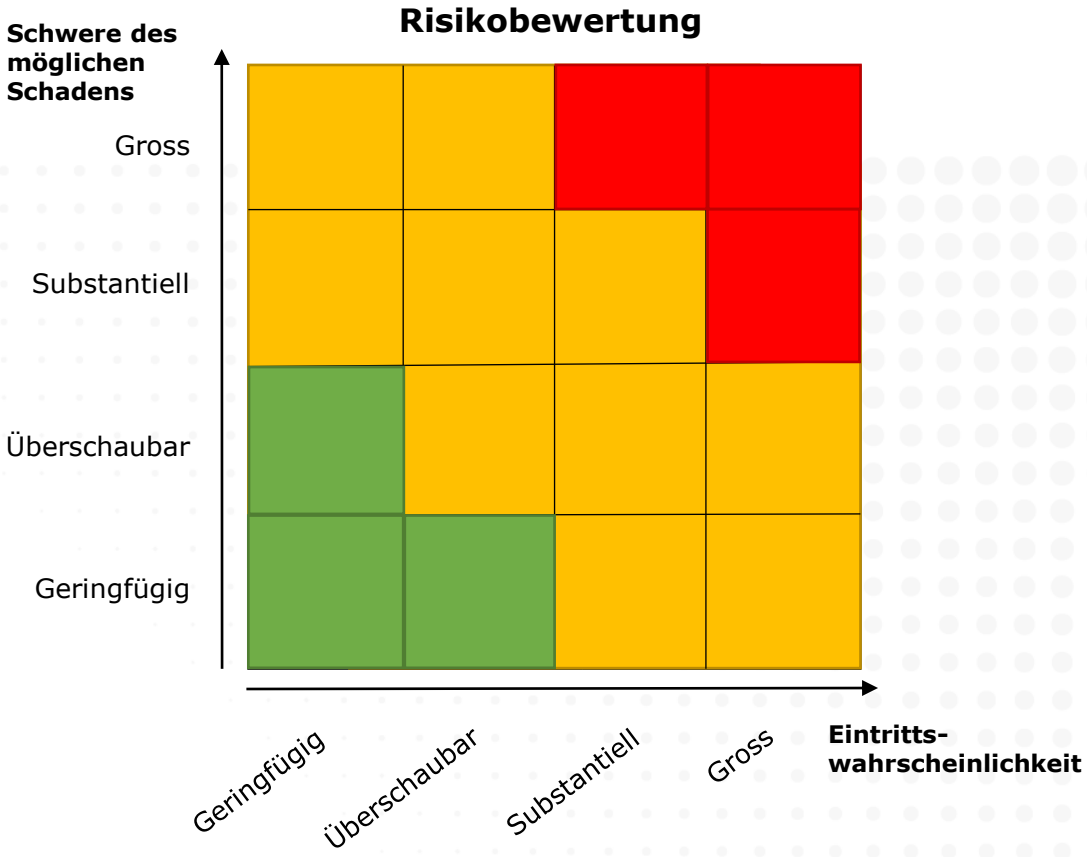
Vorgehensweise

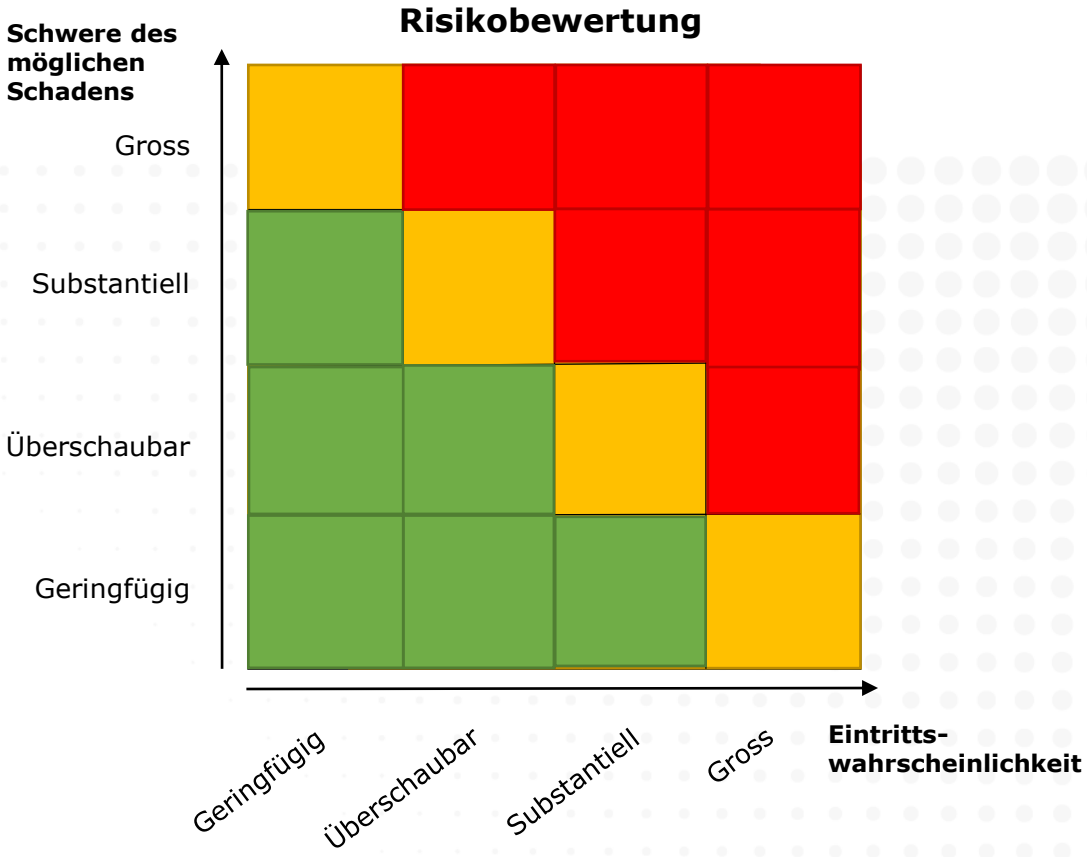
Wichtig: Alle Stakeholder an der Übung beteiligen!

- **Services** und **Fahrplan** festlegen
- **Datensicherheit** und **BCM** konzipieren und festlegen
- **Vertrag** bzw. Vertragsergänzungen mit Provider aushandeln
- **Dokumentation** des Vorhabens und der Risikobeurteilung
  - Beschreibung des Vorhabens (welche Daten wo, wann, wie etc.)
  - Beurteilung der klassischen Datensicherheits- und BCM-Risiken
  - Beurteilung des Lawful Access-Risikos (Excel)
  - Beurteilung der rechtlichen Vorgaben (FINMA, Datenschutz etc.)
- **Einbezug der externen Prüfgesellschaft** (und FINMA)
- **Management-Entscheid** bezüglich dargelegtem Restrisiko

[redacted] Projektspezifische Restrisiken im Bereich Datensicherheit, Datenschutz und Bankgeheimnis verbleiben insbesondere:

- **Risiken im Bereich der Datensicherheit:** Grundsätzlich verliert die Bank die alleinige systemtechnische Obhut über die in der Cloud gelagerten Datenbestände. Dieser Umstand bzw. die sich daraus ergebenen Risiken sind vor dem Hintergrund der von [redacted] beschriebenen technischen und organisatorischen Sicherheitsmassnahmen allerdings als "akzeptabel" zu bewerten.
- **Risiko eines Zugriffs ausländischer Behörden:** Ein solches Risiko und damit verbunden das Risiko einer unbefugten Preisgabe von Kundendaten (inklusive Verletzung des Bankgeheimnisses) besteht zwar (Stichwort "US CLOUD Act"), allerdings wird es unter Berücksichtigung des US-Rechts als theoretischer Natur eingestuft.
- **Übrige Risiken im Bereich des Datenschutzes:** Nebst den Risiken des Zugriffs durch unbefugte Dritte, führt die Verlagerung in die Cloud auch dazu, dass [redacted] in verstärktem Ausmass Mitarbeiterdaten (insbesondere die Benutzung der Cloud-Services) auswerten kann; da dies jedoch lediglich in pseudonymisierter


Risikobewertung
Schwere des möglichen Schadens
Gross
Substantiell
Überschaubar
Geringfügig
Geringfügig
Überschaubar
Substantiell
Gross
Eintritts-wahrscheinlichkeit


Risikobewertung
Schwere des möglichen Schadens
Gross
Substantiell
Überschaubar
Geringfügig
Geringfügig
Überschaubar
Substantiell
Gross
Eintritts-wahrscheinlichkeit

Beispiel Verschlüsselung

Pro memoria: In ihrer eigenen Cloud Microsoft kann *alles* umgehen

- Erfordert das Bankgeheimnis **"Bring your own key"**?
- **Wovon reden wir?**
  - Eigentlich: Der Kunde erzeugt den Schlüssel (und verwaltet ihn allenfalls auch in einer eigenen HSM* bei sich)
  - Wird synonym dafür benutzt, dass der Schlüssel in einer MS-HSM in der Microsoft-Cloud ist, aber vom Kunden verwaltet wird (AKV*)
    - Vorteil: Kunde kann Schlüssel löschen, Zugang verwalten
    - Nachteil: Kosten, Fehlerrisiko
  - Wird dies nicht getan, macht Microsoft das Schlüssel-Management
- **Wichtigere Frage ist:** Wer erhält Zugriff auf den Schlüssel?
  - Dies legt der Kunde über AD* selbst fest (und sieht er auch)

* AKV = Azure Key Vault
AD = Active Directory
HSM = Hardware Security Module

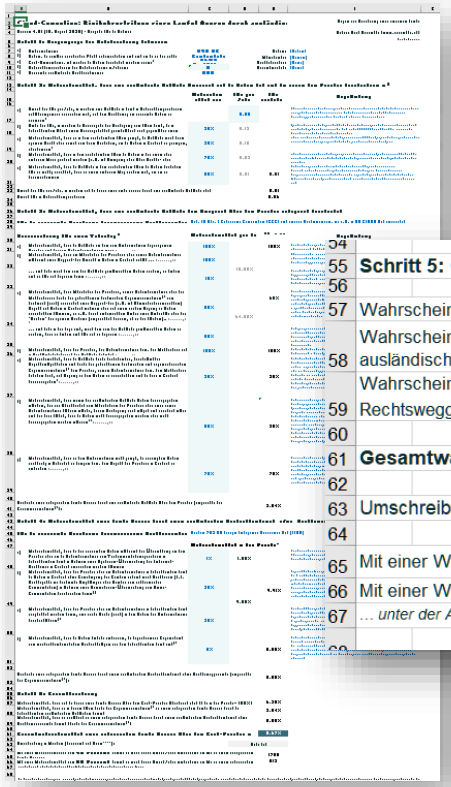
Beispiel Verschlüsselung

- **Braucht es BYOK für sensible Daten?**
  - Gewisse Datenschützer sagen ja
  - Diverse Berater sind vorsichtig und sagen ja
  - Die SBVg-Cloud-Leitfaden bleibt vage …
- Was bedeutet **"Zugriff unter Kontrolle des Instituts"?**
  - Wovor schützen wir uns? Dass Microsoft sich nicht an den Vertrag hält oder es Hintertüren gibt? Da nutzt auch ein AKV nichts …
- **Risikobeurteilung** erfordert Einbezug des **Gesamtpakets**
  - Technische Massnahmen (z.B. AD, AKV) + organisatorische Massnahmen (z.B. Vertrag, Audits) + rechtliche Schranken (z.B. was unter dem US CLOUD Act möglich und unter CH-Recht erlaubt ist)
  - Auslandszugriffe nicht ausgeschlossen, aber wie wahrscheinlich?

41 **Verschlüsselung**: Bei Verschlüsselung von CID, sollte darauf geachtet werden, dass der Verschlüsselungsschlüssel vor unberechtigten Zugriffen geschützt wird und der Zugriff unter der Kontrolle des Instituts steht, selbst wenn der Verschlüsselungsschlüssel auch dem Anbieter zur Verfügung steht oder bei diesem aufbewahrt und zur automatisierten Ver- und Entschlüsselung der CID im Rahmen der Cloud-Dienstleistung verwendet wird. Das Institut sollte auf der Grundlage einer Beurteilung der Risiken insbesondere im Hinblick der Klassifizierung der CID abwägen, welche Verfahren zur Ausprägung der Kontrolle des Verschlüsselungsschlüssels angemessen sind.

Quelle: Cloud-Leitfaden der Bankiervereinigung

Spezialfall Lawful Access



Benötigter Input: Bisherige Anfragen von Behörden, getroffene technische und organisatorische Massnahmen

54		
55	**Schritt 5: Gesamtbeurteilung**	
56		
57	Wahrscheinlichkeit, dass sich die Frage eines Lawful Access über den Cloud-Provider überhaupt stellt (1 Fall in der Periode = 100%)	6.25%
58	Wahrscheinlichkeit, dass es in diesen Fällen trotz der Gegenmassnahmen[14)] zu einem erfolgreichen Lawful Access durch die betreffenden ausländischen Behörden kommt	2.84%
59	Wahrscheinlichkeit, dass es zusätzlich zu einem erfolgreichen Lawful Access durch einen ausländischen Nachrichtendienst ohne Rechtsweggarantie kommt (trotz der Gegenmassnahmen[14)])	0.50%
60		
61	**Gesamtwahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider in der Betrachtungsperiode:*** **	0.67%
62		
63	Umschreibung in Worten (basierend auf Hillson****):	Sehr tief
64		
65	Mit einer Wahrscheinlichkeit von **90 Prozent** kommt es nach dieser Anzahl Jahre mindestens ein Mal zu einem erfolgreichen Lawful Access:	1'705
66	Mit einer Wahrscheinlichkeit von **50 Prozent** kommt es nach dieser Anzahl Jahre mindestens ein Mal zu einem erfolgreichen Lawful Access:	513
67	*… unter der Annahme, dass die Wahrscheinlichkeit sich über Zeit weder erhöht noch reduziert (wie bei einem Münzwurf)*	

Excel: https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx
Siehe auch den dazugehörigen Beitrag (https://bit.ly/2HaEet5) und Anhang (https://bit.ly/2H8MyZY)

Umgang mit Restrisiken

Welche Praxis werden die Aufsichtsbehörden entwickeln?

- **Versachlichung** der Diskussion
  - Wie ist es um die Risiken denn heute ohne Cloud bestellt?
- **Mit dem Strom** schwimmen?
  - Was sind die Alternativen? Wo wird die Welt in fünf Jahren sein?
- Schrittweises **Herantasten** an die Cloud
  - Kommunikation → Büroautomation → Plattform-as-a-Service
- Zusätzliche Massnahmen zur **Risikominderung**
  - z.B. AGB mit Bankgeheimnis-Waiver für Auslagerungen
- **Wichtig:** Hinter jedem Cloud Projekt steckt ein **Business Case**
  - Restrisiken werden vom Management in der Regel akzeptiert

VISCHER

Danke für Ihre Aufmerksamkeit!

Bei 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