VISCHER

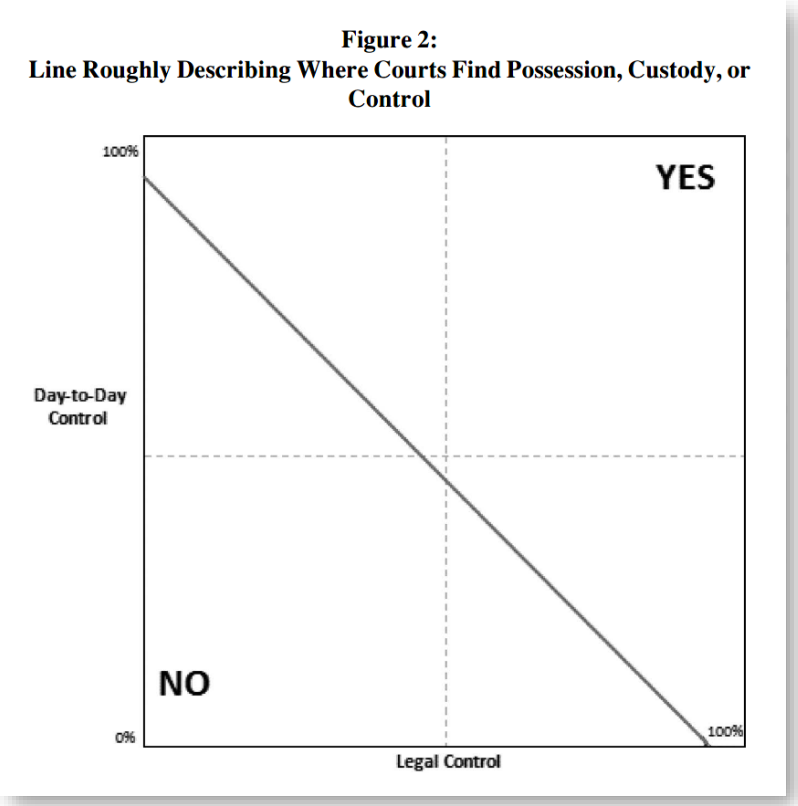
US CLOUD Act.

Beurteilung des Restrisikos eines Foreign Lawful Access beim Gang in die Cloud

David Rosenthal, Partner, VISCHER AG
1. Mai 2022

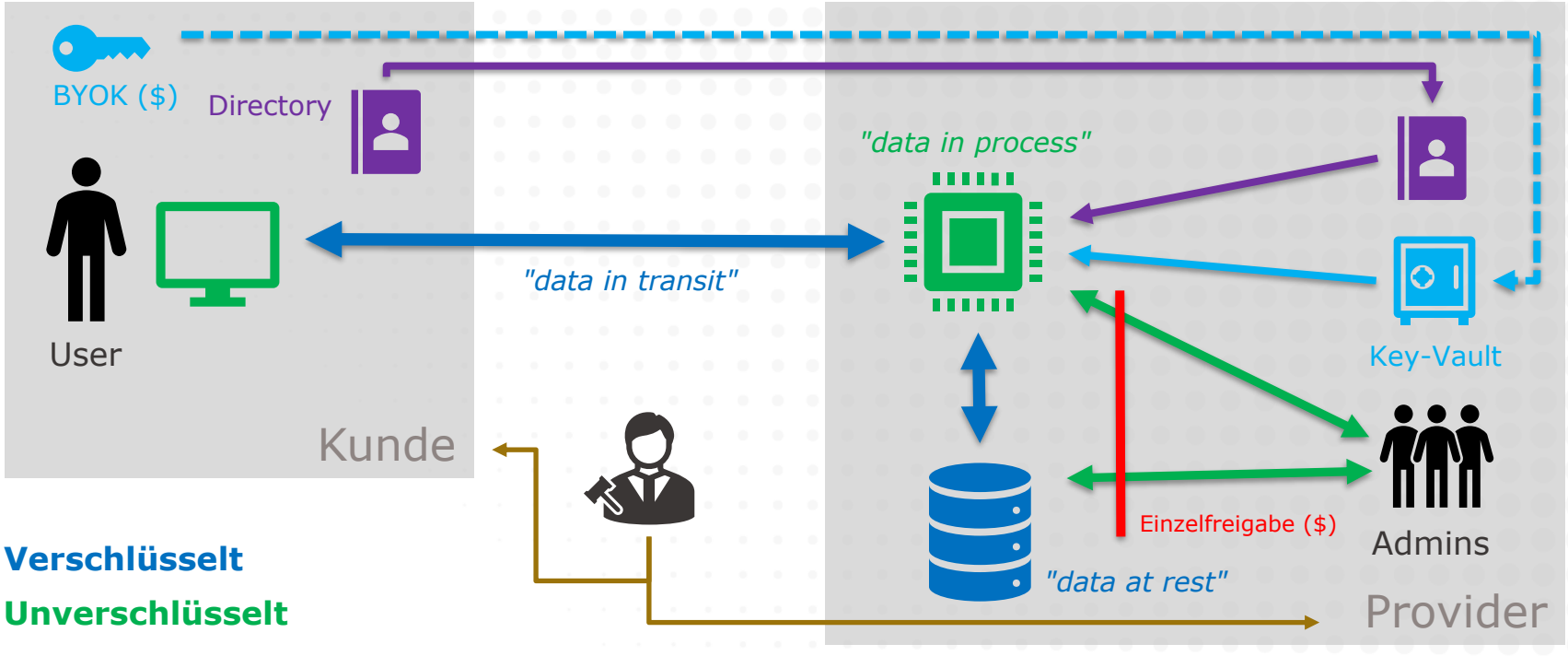
Umgang mit dem US CLOUD Act

- US CLOUD Act: US-Strafbehörden können von US-Providern im Falle schwerwiegender Straftaten Herausgabe von Daten verlangen, die sie «besitzen» oder «kontrollieren», auch wenn sie im Ausland sind
  - Analog Art. 18 Abs. 1 Cybercrime Convention (SR 0.311.43)
- Daten sind vor solchem "Foreign Lawful Access" via ausländischen Provider ggf. zu schützen (Berufs-/Amtsgeheimnis, Datenschutz)
  - Daten in der Schweiz, aber Fernzugriff aus den USA möglich
  - US-Nachrichtendienste sind auch zu berücksichtigen («Schrems II»)
- Dazu werden diverse Massnahmen getroffen (Vertrag, Technik etc.)
  - Sollen in Kombination dafür sorgen, dass Provider Daten nicht edieren kann oder muss (z.B. keine Pflicht, eigene Systeme zu hacken)
  - Wie wirksam sind die Massnahmen? Sorgfaltspflichten erfüllt?

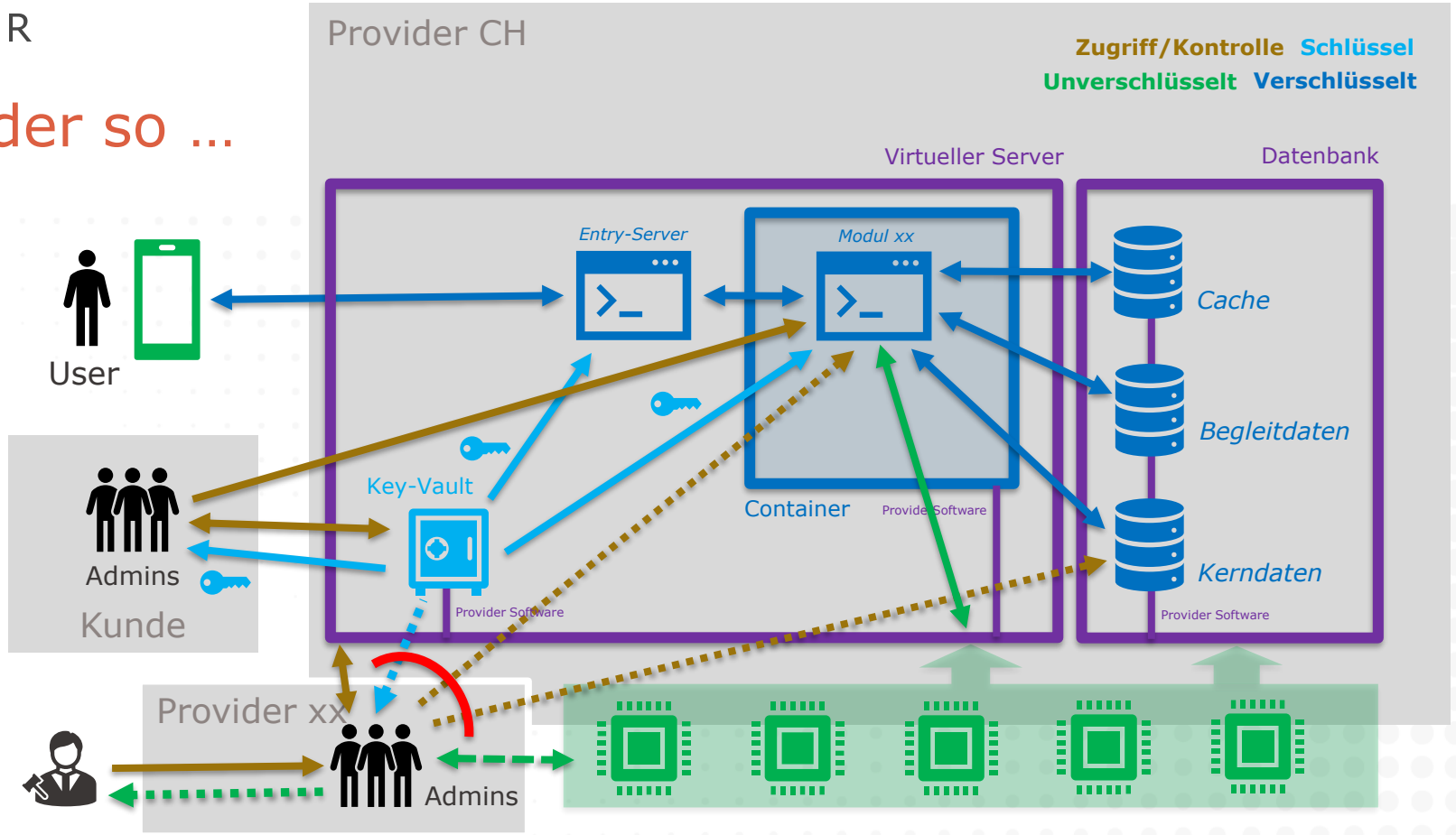


Quelle: Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 vom 23. Januar 2020 (https://bit.ly/3i2xfC9)

Wie Daten in der Cloud geschützt werden



Oder so …


Provider CH
Zugriff/Kontrolle Schlüssel
Unverschlüsselt Verschlüsselt
Virtueller Server
Datenbank
Entry-Server
Modul xx
Cache
Begleitdaten
Kerndaten
User
Key-Vault
Container
Provider Software
Admins
Kunde
Provider Software
Provider Software
Provider xx
Admins

Erläuterungen des Modells

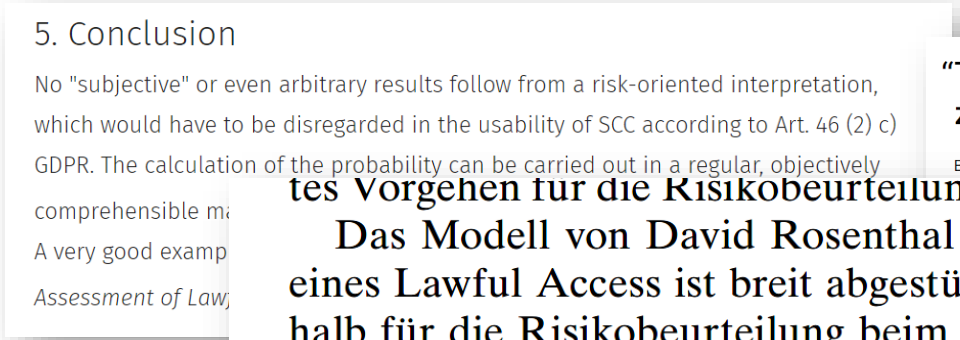
- 2019 für eine Schweizer Grossbank (Bankgeheimnis) entwickelt, 2020 als "open source" publiziert (mit Aufsatz), 2021 von der IAPP unter eigenem Namen angeboten
  - Frei verfügbar, in etlichen Fällen (Amts-/Berufsgeheimnis) eingesetzt
- Strukturierte, objektivierte Risikobeurteilung statt "Bauchentscheid"
- Grundidee sind drei Fragen
  - Wie oft sind ausländische Behörden an den hier relevanten Daten ernsthaft interessiert und kommen nicht anders an sie heran?
  - Welche Voraussetzungen (auch rechtlich) müssen zusammentreffen, damit es zu einem Lawful Access auf Daten im Klartext kommt?
  - Wie wahrscheinlich ist jede einzelne Voraussetzung erfüllt?
- Aus der Einschätzung der Einzelelemente wird für eine Periode die statistische Eintrittswahrscheinlichkeit einer Offenbarung berechnet
  - Das Restrisiko im Leben ist nie Null, doch ist dies auch nicht verlangt

Input: Bisherige Erfahrungen mit Anfragen ausländischer Behörden, technische und organisatorische Massnahmen

35	d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%	100%	The Provider reserves the right to provide the service also from the USA. This m subcontractors is under the jurisdiction of the US authorities.
36	e)	Probability [illegible] counterme parent com text7) (prere			
37	f)	Probability liability of e and realisti (prerequisite			

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
Vgl. auch den Beitrag unter https://bit.ly/2HaEet5 und Anhang unter https://bit.ly/2H8MyZY.

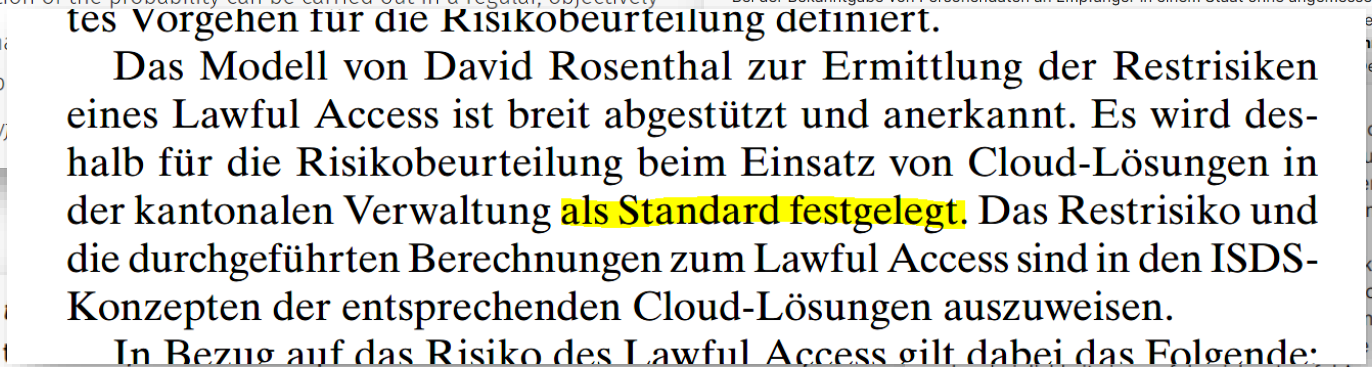


5. Conclusion

No "subjective" or even arbitrary results follow from a risk-oriented interpretation, which would have to be disregarded in the usability of SCC according to Art. 46 (2) c) GDPR. The calculation of the probability can be carried out in a regular, objectively comprehensible ma

A very good examp

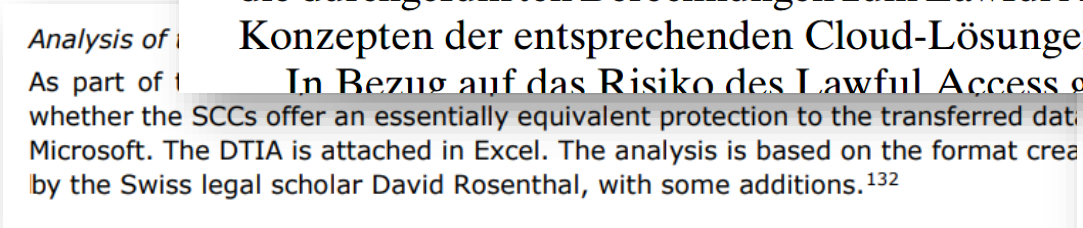
Assessment of Law



tes Vorgehen für die Risikobeurteilung definiert.

Das Modell von David Rosenthal zur Ermittlung der Restrisiken eines Lawful Access ist breit abgestützt und anerkannt. Es wird deshalb für die Risikobeurteilung beim Einsatz von Cloud-Lösungen in der kantonalen Verwaltung als Standard festgelegt. Das Restrisiko und die durchgeführten Berechnungen zum Lawful Access sind in den ISDS-Konzepten der entsprechenden Cloud-Lösungen auszuweisen.

In Bezug auf das Risiko des Lawful Access gilt dabei das Folgende:



Analysis of

As part of t

whether the SCCs offer an essentially equivalent protection to the transferred data

Microsoft. The DTIA is attached in Excel. The analysis is based on the format crea

by the Swiss legal scholar David Rosenthal, with some additions.[132]

"Transfer Impact Assessments": IAPP veröffentlicht zwei Formulare von David Rosenthal

Bei der Bekanntgabe von Personendaten an Empfänger in einem Staat ohne angemessenes Daten-

eln (SCC) zu

ren, ob das loka-

er Europäische

s

odell zur

ul Access

n (!) Vor-

mit es zu

Behörde

keit eines

chkeit für

n von Ro-

Gesamt-

wahrscheinlichkeit eines erfolgreichen Lawful Access über den Cloud-Provider von 0,67 Prozent in der (auf fünf Jahre festgelegten) Betrachtungsperiode. Das bedeutet, dass es in diesem Beispiel erst nach 513 Jahren mit einer Wahrscheinlichkeit von 50 Prozent zu einem erfolgreichen Lawful Access kommen würde. Für die genaue Berechnung und die Begründung der getroffenen Annahmen wird auf das Excel-Dokument von Rosenthal verwiesen.[34]

Quellen: datenrecht.ch, www.rijksoverheid.nl, steigerlegal.ch, www.wolterskluwer.com, www.dr-datenschutz.de, RRB ZH Nr. 542 2022

VISCHER

Danke für Ihre Aufmerksamkeit!

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