VISCHER

Mit der öffentlichen Verwaltung in die Cloud.

Die häufigsten Fehlvorstellungen

David Rosenthal, Partner, VISCHER AG
27. Juni 2023

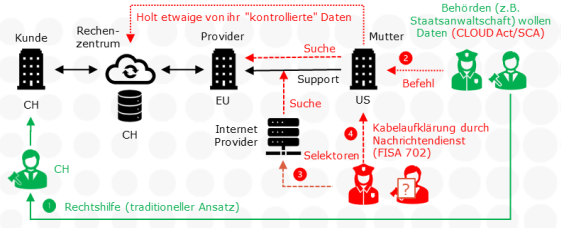
Drei Fehlvorstellungen

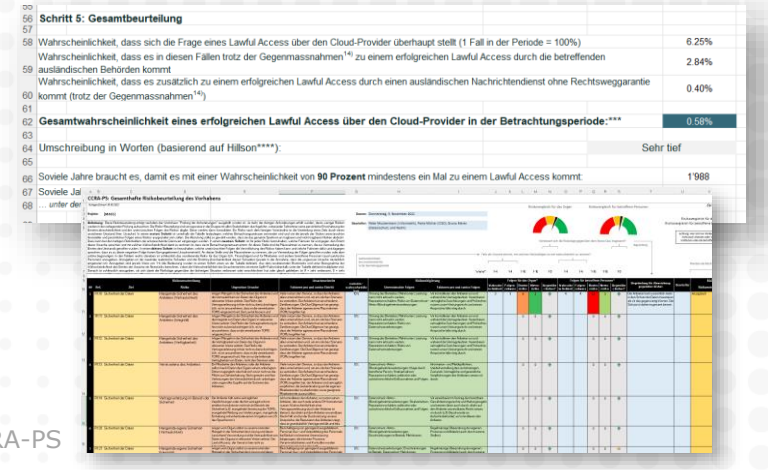
- "Ausländischer Behördenzugriff"
- "End-to-End-Verschlüsselung zwingend"
- "Alles steht und fällt mit dem Provider"

- Weitere

Nr. 1 – "Ausländischer Behördenzugriff"

- Der grösste **Zankapfel** aus rechtlicher Sicht
  - Fokus ist auf US CLOUD Act
  - Im öffentlichen Sektor bisher leider keine fundierte Diskussion
- **Andere Cloud-Risiken** sind gewichtiger
  - Abhängigkeit
  - Geschäftsfortführung
  - Kunde, der nicht in der Lage ist, die Cloud richtig zu steuern und zu überwachen
- Jedes öffentliche Organ muss selbst eine **Risikobeurteilung** vornehmen

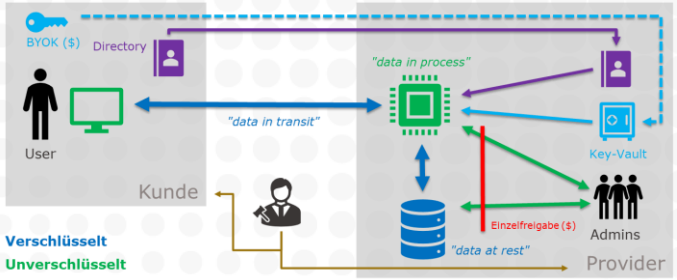




Tool: CCRA-PS

Nr. 2 – "End-to-End-Verschlüsselung zwingend"

- Wird von einzelnen **Datenschutzbehörden** noch verlangt
  - Für die meisten Anwendungen unrealistisch, weil der Computer in der Cloud mit den Daten arbeiten soll



Setup von M365

- Wesentlich ist, dass die **Kontrolle** über den Schlüssel grundsätzlich beim Kunden bleibt
  - Der Kunde definiert über sein Benutzerverzeichnis, wer für welche Daten den Schlüssel erhält
  - Der Schlüssel lagert jedoch im Rechenzentrum des Providers
  - Zugriffe durch Mitarbeiter des Providers auf Kundendaten werden vertraglich eingeschränkt (aber i.d.R. kein völliger Ausschluss)

Nr. 3 – "Alles steht und fällt mit dem Provider"

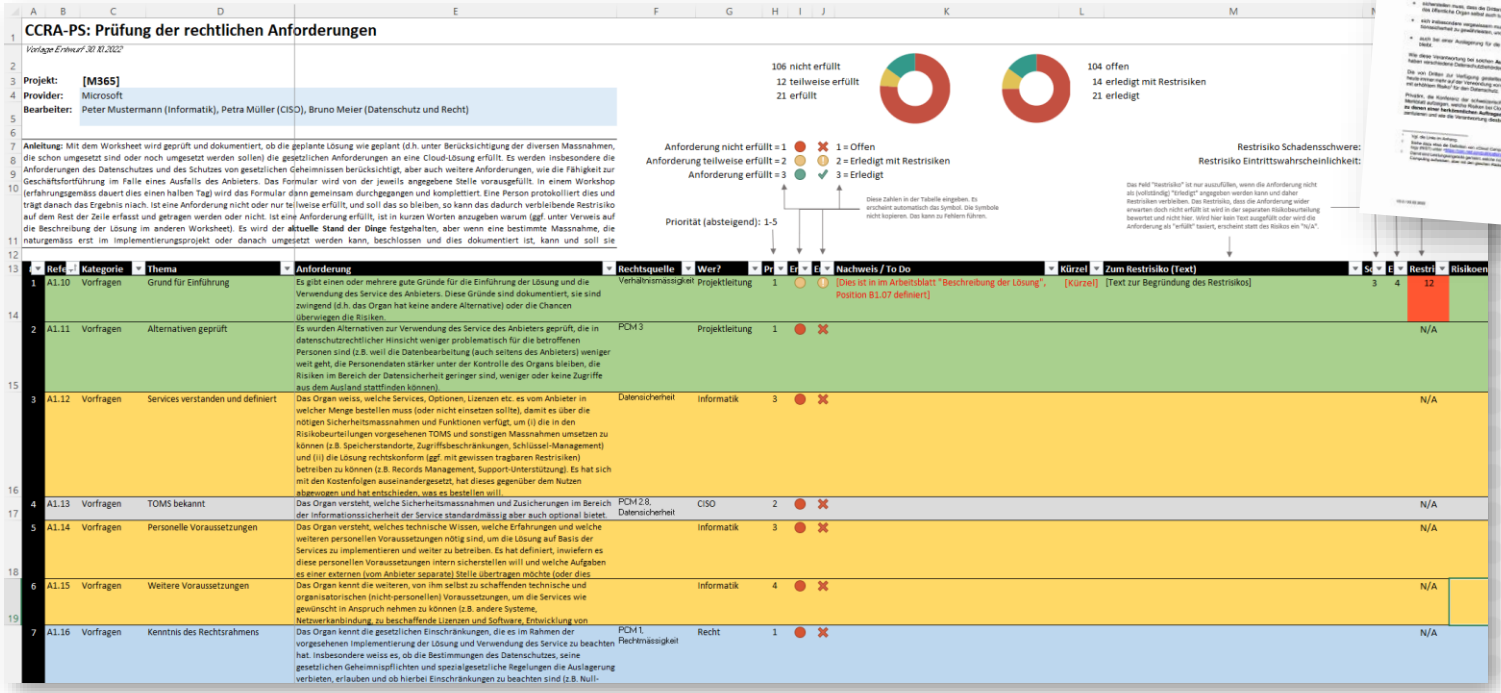
- **Provider** gilt als das grosse Problem
  - Recht und Marktmacht des Providers
  - Vertragsbedingungen des Providers
  - Sorgfalt des Providers
- Aber: Die mangelnde Cloud-Maturität des **Kunden** ist in der Praxis oft die grössere Herausforderung
  - Kann er die Services so steuern und kontrollieren, dass sie (nur) das tun, was sie sollen?
  - Ist er in der Lage, den Provider zu überwachen?
  - Hat er die ständigen Entwicklungen im Griff?
  - Welche Funktionen kann er seinen Mitarbeitenden zutrauen?

Bild von Pexels (Pixabay)

"Shared Responsibility Model"

VISCHER

140 Anforderungen für Cloud-Projekte



CCRA-PS: Prüfung der rechtlichen Anforderungen

Vorlage Entwurf 30.10.2022

Projekt: [M365]
Provider: Microsoft
Bearbeiter: Peter Mustermann (Informatik), Petra Müller (CISO), Bruno Meier (Datenschutz und Recht)

Anleitung: Mit dem Worksheet wird geprüft und dokumentiert, ob die geplante Lösung wie geplant (d.h. unter Berücksichtigung der diversen Massnahmen, die schon umgesetzt sind oder noch umgesetzt werden sollen) die gesetzlichen Anforderungen an eine Cloud-Lösung erfüllt. Es werden insbesondere die Anforderungen des Datenschutzes und des Schutzes von gesetzlichen Geheimnissen berücksichtigt, aber auch weitere Anforderungen, wie die Fähigkeit zur Geschäftsfortführung im Falle eines Ausfalls des Anbieters. Das Formular wird von der jeweils angegebene Stelle vorausgefüllt. In einem Workshop (erfahrungsgemäss dauert dies einen halben Tag) wird das Formular dann gemeinsam durchgegangen und komplettiert. Eine Person protokolliert dies und trägt danach das Ergebnis nach. Ist eine Anforderung nicht oder nur teilweise erfüllt, und soll das so bleiben, so kann das dadurch verbleibende Restrisiko auf dem Rest der Zeile erfasst und getragen werden oder nicht. Ist eine Anforderung erfüllt, ist in kurzen Worten anzugeben warum (ggf. unter Verweis auf die Beschreibung der Lösung im anderen Worksheet). Es wird der **aktuelle Stand der Dinge** festgehalten, aber wenn eine bestimmte Massnahme, die naturgemäss erst im Implementierungsprojekt oder danach umgesetzt werden kann, beschlossen und dies dokumentiert ist, kann und soll sie

106 nicht erfüllt
12 teilweise erfüllt
21 erfüllt

104 offen
14 erledigt mit Restrisiken
21 erledigt

Anforderung nicht erfüllt = 1
Anforderung teilweise erfüllt = 2
Anforderung erfüllt = 3

1 = Offen
2 = Erledigt mit Restrisiken
3 = Erledigt

Priorität (absteigend): 1-5

Restrisiko Schadensschwere:
Restrisiko Eintrittswahrscheinlichkeit:

	Refe	Kategorie	Thema	Anforderung	Rechtsquelle	Wer?	Pr	Er	E	Nachweis / To Do	Kürzel	Zum Restrisiko (Text)	S	E	Restri	Risikoen
1	A1.10	Vorfragen	Grund für Einführung	Es gibt einen oder mehrere gute Gründe für die Einführung der Lösung und die Verwendung des Service des Anbieters. Diese Gründe sind dokumentiert, sie sind zwingend (d.h. das Organ hat keine andere Alternative) oder die Chancen überwiegen die Risiken.	Verhältnismässigkeit	Projektleitung	1			[Dies ist in im Arbeitsblatt "Beschreibung der Lösung", Position B1.07 definiert]	[Kürzel]	[Text zur Begründung des Restrisikos]	3	4	12	
2	A1.11	Vorfragen	Alternativen geprüft	Es wurden Alternativen zur Verwendung des Service des Anbieters geprüft, die in datenschutzrechtlicher Hinsicht weniger problematisch für die betroffenen Personen sind (z.B. weil die Datenbearbeitung (auch seitens des Anbieters) weniger weit geht, die Personendaten stärker unter der Kontrolle des Organs bleiben, die Risiken im Bereich der Datensicherheit geringer sind, weniger oder keine Zugriffe aus dem Ausland stattfinden können).	PCM 3	Projektleitung	1								N/A	
3	A1.12	Vorfragen	Services verstanden und definiert	Das Organ weiss, welche Services, Optionen, Lizenzen etc. es vom Anbieter in welcher Menge bestellen muss (oder nicht einsetzen sollte), damit es über die nötigen Sicherheitsmassnahmen und Funktionen verfügt, um (i) die in den Risikobeurteilungen vorgesehenen TOMS und sonstigen Massnahmen umsetzen zu können (z.B. Speicherstandorte, Zugriffsbeschränkungen, Schlüssel-Management) und (ii) die Lösung rechtskonform (ggf. mit gewissen tragbaren Restrisiken) betreiben zu können (z.B. Records Management, Support-Unterstützung). Es hat sich mit den Kostenfolgen auseinandergesetzt, hat dieses gegenüber dem Nutzen abgewogen und hat entschieden, was es bestellen will.	Datensicherheit	Informatik	3								N/A	
4	A1.13	Vorfragen	TOMS bekannt	Das Organ versteht, welche Sicherheitsmassnahmen und Zusicherungen im Bereich der Informationssicherheit der Service standardmässig aber auch optional bietet.	PCM 2.8, Datensicherheit	CISO	2								N/A	
5	A1.14	Vorfragen	Personelle Voraussetzungen	Das Organ versteht, welches technische Wissen, welche Erfahrungen und welche weiteren personellen Voraussetzungen nötig sind, um die Lösung auf Basis der Services zu implementieren und weiter zu betreiben. Es hat definiert, inwiefern es diese personellen Voraussetzungen intern sicherstellen will und welche Aufgaben es einer externen (vom Anbieter separate) Stelle übertragen möchte (oder dies		Informatik	3								N/A	
6	A1.15	Vorfragen	Weitere Voraussetzungen	Das Organ kennt die weiteren, von ihm selbst zu schaffenden technische und organisatorischen (nicht-personellen) Voraussetzungen, um die Services wie gewünscht in Anspruch nehmen zu können (z.B. andere Systeme, Netzwerkanbindung, zu beschaffende Lizenzen und Software, Entwicklung von		Informatik	4								N/A	
7	A1.16	Vorfragen	Kenntnis des Rechtsrahmens	Das Organ kennt die gesetzlichen Einschränkungen, die es im Rahmen der vorgesehenen Implementierung der Lösung und Verwendung des Service zu beachten hat. Insbesondere weiss es, ob die Bestimmungen des Datenschutzes, seine gesetzlichen Geheimnispflichten und spezialgesetzliche Regelungen die Auslagerung verbieten, erlauben und ob hierbei Einschränkungen zu beachten sind (z.B. Null-	PCM 1, Rechtmässigkeit	Recht	1								N/A	

privatim

Merkblatt: Cloud-spezifische Risiken und Massnahmen

Tool:
CCRA-PS

Weitere Vorstellungen …

Die neue Cloud des Bundes, oder: Das Wolkenkuckucksheim

Der Bund will seine eigene Daten-Cloud ausbauen und so eine Alternative zu den grossen Big-Tech-Firmen schaffen. Doch ausgerechnet das zuständige Bundesamt für Informatik ist damit überfordert.

Eine Recherche von Adrienne Fichter (Text) und Clara San Millán (Illustration), 08.06.2023

Republik.ch

- "Die Cloud ist sicher."
- "Schweizer Provider sind sicher vor ausländischen Zugriffen."
- "Es gibt keine Alternative zur Cloud."
- "Eine Swiss Cloud ist ebenso gut wie jene der Hyperscaler."
- "Die Cloud ist günstiger."
- "In der Cloud sind die Daten überall auf der Welt."
- "Mit Cloud-Providern kann nicht verhandelt werden."
- "Am Schluss müssen die Gerichte entscheiden, ob das alles geht."

Die fünf Fragen, die gestellt werden sollten …

	Strategie und Vorgehensweise	Beurteilung eines konkreten Vorhabens
Motive & Alternativen	Welche Dinge erhoffen wir uns vom Gang in die Cloud und wie gut wollen wir die Alternativen kennen?	Was sind die geschäftlichen, operationellen und anderen Anforderungen an das Vorhaben und wieso überwiegt die gewählte Lösung gegenüber anderen Techniken (d.h. Alternativen zur Cloud), anderen Cloud-Providern und dem Status quo?
Compliance	Wie gehen wir vor, um die Einhaltung des Berufs- und Amtsgeheimnisses und der diversen gesetzlichen, regulatorischen wie auch eigenen Vorgaben systematisch zu prüfen, zu dokumentieren und während der ganzen Laufzeit der Cloud-Vorhaben sicherzustellen?	Halten wir mit dem Vorhaben das Berufs- und Amtsgeheimnis und die gesetzlichen, regulatorischen wie auch die eigenen Vorgaben ein und wie haben wir dies systematisch geprüft, dokumentiert und für die ganze Laufzeit des Cloud-Vorhabens sichergestellt?
Organisation & Internes Kontrollsystem (IKS)	Was sind wir bereit zu tun und zu verlangen, damit unsere Organisation Cloud-Provider und deren Lösungen verstehen, kontrollieren und steuern können, so dass wir sie nicht nur richtig handhaben können, sondern auch Abweichungen vom Soll rechtzeitig erkennen und beseitigen können?	Welche Vorkehrungen haben wir getroffen oder treffen wir, damit wir den Provider und seinen Cloud-Lösung mit unseren internen Mitteln so gut verstehen, kontrollieren und steuern können, dass wir die Cloud-Lösung gemäss den Anforderungen richtig handhaben, Abweichungen vom Soll rechtzeitig erkennen und sie beseitigen können werden, inklusive seiner bzw. ihrer "end-to-end" Einbindung in unser IKS?
Geschäftsfortführung	Welche Anforderungen stellen wir an die Sicherstellung der Geschäftsfortführung bei einem Ausfall oder Datenverlust und unsere Fähigkeit für einen kurzfristigen (Monate) und mittelfristigen (12-18 Monate) Ausstieg aus einem Cloud-Service und welchen Aufwand sind wir bereit dafür zu betreiben?	Was ist unser Plan für den Fall, dass der Cloud-Provider seinen Service plötzlich abstellt, die Lösung oder unsere Daten nicht mehr verfügbar sind oder wir kurzfristig (Monate) und mittelfristig (12-18 Monate) von ihm oder seiner Lösung weg müssen oder wollen?
Restrisiken	Wie stellen wir sicher, dass wir konkrete Bedrohungen, die mit einem Cloud-Vorhaben einhergehen und gewichtige Folgen für das Organ haben können, richtig einschätzen, steuern und in Bezug zu den Restrisiken stellen, die wir sonst bzw. sowieso haben?	Welche weiteren Bedrohungen, welche für das Organ gewichtige Folgen haben können, bringt das Cloud-Vorhaben mit sich, wie gut haben wir diese im Griff und wie stehen die Restrisiken zu jenen Risiken, die wir ohne das Vorhaben bzw. sowieso hätten?

VISCHER

Danke für Ihre Aufmerksamkeit!

Weitere Infos und Tools:
www.rosenthal.ch

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