

Sechs Prüffragen vor jeder Cloud-Entscheidung

Ein Arbeitsleitfaden für Verwaltungsräte und Geschäftsleitungen: was Sie fragen, welche Belege Sie verlangen und welche Antworten eine Unterschrift verschieben sollten.

- 01 Welchem Recht unterliegen Betreiber, Control Plane und Support-Pfade im Konfliktfall?
- 02 Wer kann Admin-Zugriffe erzwingen, und wer kann sie verweigern?
- 03 Liegt die Schlüsselverwaltung nachweisbar ausserhalb der Anbietersphäre?
- 04 Wurde der Exit real getestet, nicht nur dokumentiert?
- 05 Erhöht dieser Vertrag die Kontrolltiefe oder nur den Funktionsumfang?
- 06 Wer entscheidet im Ernstfall, und wie schnell?

Warum dieser Leitfaden

Jedes grosse Cloud-Angebot kommt heute mit einem Souveränitätskapitel. Es listet Rechenzentrumsstandorte, Zertifizierungen und einen beruhigenden Absatz über europäische Gesellschaften. Verwaltungsräte lesen es, fühlen sich beruhigt und unterschreiben.

Souveränität ist keine Eigenschaft eines Rechenzentrums. Sie ist eine Eigenschaft von Verträgen, Architekturen und geprobten Abläufen, und sie zeigt sich nur unter Druck: an dem Tag, an dem ein Anbieter, ein Regulator oder ein ausländisches Gericht ihn ausübt.

Keine der sechs Fragen verlangt technische Tiefe. Sie verlangen die Disziplin, auf dokumentierte, prüfbare Antworten zu bestehen, und die Bereitschaft, eine Unterschrift zu verschieben, bis sie vorliegen.

So setzen Sie ihn ein

1. Senden Sie die sechs Fragen vor der Sitzung an das Management oder den Anbieter.
2. Verlangen Sie schriftliche Antworten mit Belegen, keine Präsentation.
3. Halten Sie im Arbeitsblatt auf Seite 5 fest, was vorliegt und was noch offen ist.

Die sechs Fragen sind mit Zustimmung des Autors dem Buch *Sovereign Cloud. Der Leitfaden für Systemarchitekten und CTOs* (Rheinwerk Computing, 436 Seiten) entnommen, das aus unserem Team heraus entstanden ist.

O1 Welchem Recht unterliegen Betreiber, Control Plane und Support-Pfade im Konfliktfall?

Nicht der Normalbetrieb zählt, sondern der Ernstfall: der Tag, an dem zwei Rechtsordnungen uneins sind, wer Ihre Systeme einsehen oder stoppen darf.

BELEGE, DIE SIE VERLANGEN SOLLTEN

- ✓ Die Betreibergesellschaft und ihre letzte Eigentümerin
- ✓ Von wo aus die Control Plane betrieben und administriert wird
- ✓ Wo Betriebs- und Supportpersonal mit Zugriff sitzt und welches Recht es bindet

ANTWORTEN, DIE SIE BREMSEN SOLLTEN

- ! «Die Daten bleiben in der EU» ohne Aussage zu Control Plane und Supportpersonal
- ! Betreibergesellschaft und Vertragspartnerin sind unterschiedliche Unternehmen

O2 Wer kann Admin-Zugriffe erzwingen, und wer kann sie verweigern?

Die Antwort steht selten in der Pressemitteilung. Sie steht in den Nutzungsbedingungen, der Liste der Unterauftragnehmer und der Eigentümerstruktur dahinter.

BELEGE, DIE SIE VERLANGEN SOLLTEN

- ✓ Nutzungsbedingungen und Auftragsverarbeitungsvertrag, inklusive Klauseln zu behördlichen Anfragen
- ✓ Die vollständige Liste der Unterauftragnehmer und das Verfahren für Änderungen
- ✓ Veröffentlichte Transparenzberichte des Anbieters, sofern vorhanden

ANTWORTEN, DIE SIE BREMSEN SOLLTEN

- ! Der Anbieter kann Unterauftragnehmer ohne Vorankündigung wechseln
- ! Keine vertragliche Zusage, Zugriffsanfragen anzufechten oder mitzuteilen

O3 Liegt die Schlüsselverwaltung nachweisbar ausserhalb der Anbietersphäre?

Nachweisbar heisst auditierbar. Eine Zusicherung auf einer Folie ist kein Beleg.

BELEGE, DIE SIE VERLANGEN SOLLTEN

- ✓ Wo Schlüssel erzeugt, gespeichert und verwendet werden (zum Beispiel ein externes HSM unter Ihrer Kontrolle)
- ✓ Eine dokumentierte Key Ceremony und wer daran teilnimmt
- ✓ Zugriffsprotokolle, die ein unabhängiger Dritter prüfen kann

ANTWORTEN, DIE SIE BREMSEN SOLLTEN

- ! «Kundenverwaltete Schlüssel», während der Anbieter den Schlüsseldienst weiterhin betreibt
- ! Kein unabhängiges Audit des Schlüsselmanagements

04 Wurde der Exit real getestet, nicht nur dokumentiert?

Ein Exit-Plan, der nie auch nur teilweise ausgeführt wurde, ist eine Vermutung mit Budgetposten.

BELEGE, DIE SIE VERLANGEN SOLLTEN

- ✓ Der Exit-Plan mit Datenformaten, Werkzeugen und Verantwortlichkeiten
- ✓ Ergebnisse einer Probe für mindestens einen Workload, mit der benötigten Zeit
- ✓ Vertragliche Regeln für Datenrückgabe, Löschung und Übergangsunterstützung

ANTWORTEN, DIE SIE BREMSEN SOLLTEN

- ! Der Exit ist beschrieben, wurde aber nie getestet
- ! Proprietäre Dienste ohne dokumentierten Migrationspfad

05 Erhöht dieser Vertrag die Kontrolltiefe oder nur den Funktionsumfang?

Funktionskataloge wachsen jedes Quartal. Kontrolltiefe (wer was stoppen kann, und wie schnell) wächst selten. Mehr Funktionen bedeuten nicht mehr Souveränität. Oft das Gegenteil.

BELEGE, DIE SIE VERLANGEN SOLLTEN

- ✓ Eine Liste der gewonnenen Kontrollen: wer welchen Workload stoppen, isolieren oder verschieben kann
- ✓ Welche Funktionen neue Abhängigkeiten schaffen und wie sie ersetzt werden können
- ✓ Service Levels für Kontrollfunktionen, nicht nur für die Verfügbarkeit

ANTWORTEN, DIE SIE BREMSEN SOLLTEN

- ! Der Business Case beruht auf Funktionen statt auf Kontrollen
- ! Zentrale Kontrollen gibt es nur in einer höheren Stufe, die später verhandelt wird

06 Wer entscheidet im Ernstfall, und wie schnell?

Lautet die Antwort «drei Gremien und ein Eskalationspfad beim Anbieter», ist die Abhängigkeit bereits Ihre. Unklare Verantwortung ist die teuerste Abhängigkeit von allen.

BELEGE, DIE SIE VERLANGEN SOLLTEN

- ✓ Eine benannte entscheidungsbefugte Person auf Ihrer Seite, mit Stellvertretung
- ✓ Der Eskalationspfad beim Anbieter und die zugesagten Reaktionszeiten
- ✓ Das Datum der letzten Übung und was sie gezeigt hat

ANTWORTEN, DIE SIE BREMSEN SOLLTEN

- ! Entscheidungsrechte sind auf mehrere Gremien verteilt, ohne letzte Verantwortung
- ! Das Notfallverfahren wurde nie geübt

Arbeitsblatt für die Verwaltungsratsvorlage

Halten Sie vor dem Entscheid den Stand jeder Frage fest. Ein Angebot ist unterschriftsreif, wenn jede Zeile einen schriftlichen Beleg hat oder ein dokumentiertes und akzeptiertes Risiko.

	FRAGE	SCHRIFTLICH BEANTWORTET	BELEG IM ANHANG	OFFENER PUNKT / VERANTWORTLICH
01	Recht im Konfliktfall	☐	☐	
02	Erzwungener Zugriff	☐	☐	
03	Schlüsselverwaltung	☐	☐	
04	Getesteter Exit	☐	☐	
05	Kontrolltiefe	☐	☐	
06	Entscheide im Ernstfall	☐	☐	
Datum		Verantwortlich Management		Vorsitz

Drei praktische Schritte

- 01 Machen Sie die sechs Fragen zum festen Bestandteil** jeder Cloud-Vorlage an den Verwaltungsrat, schriftlich vom Management beantwortet, mit Belegen im Anhang.
- 02 Trennen Sie die Souveränitätsentscheidung von der Anbieterentscheidung.** Legen Sie zuerst fest, welche Kontrollen Sie benötigen. Vergleichen Sie erst dann, wer sie liefern kann.
- 03 Finanzieren Sie die Probe.** Ein getesteter Exit für einen kritischen Workload kostet einen Bruchteil eines Programmbudgets und macht aus der Exit-Klausel eine echte Option statt einer Hoffnung.

Über Cloud Tower Group

Cloud Tower Group arbeitet mit Verwaltungsräten und Geschäftsleitungen als unabhängiges Gegenüber bei Cloud- und KI-Entscheidungen: Prüfung von Souveränitätszusagen gegen Vertrag und Architektur, Vorbereitung der Verwaltungsratsvorlage und, wo eine Entscheidung Menschen erfordert, die die Organisation noch nicht hat, die Besetzung der Architekten und Interim-Führungskräfte, die sie tragen können. Wir halten keine Anbietermandate und verkaufen keine Software.

Die sechs Fragen sind mit Zustimmung des Autors dem Buch *Sovereign Cloud. Der Leitfaden für Systemarchitekten und CTOs* (Rheinwerk Computing, 436 Seiten) entnommen, das aus unserem Team heraus entstanden ist.



Cloud-Entscheidung mit einem Partner besprechen

gens.ctowertech.com/de · info@ctowertech.com

Dieser Leitfaden enthält allgemeine Informationen und stellt keine Rechts-, Regulierungs- oder Beschaffungsberatung für einen konkreten Fall dar.