

Interview zur Sicherheit bei Cloud Computing

Ein kurzes Gespräch zwischen Roger Gisi und Christian Katz

RG: Sie sind Experte für Informationssicherheit. In diesem Zusammenhang machen Sie sich andere Gedanken als die zukünftigen Cloud-Nutzer.

CK: Ja, Informationen sind so wichtig für das Unternehmen wie mein Gehirn für mein Leben.

Wenn Sie sich auf Cloud Computing einlassen, wird Ihr Unternehmen vom Cloud Service Provider (CSP) abhängig.

Trotzdem ist Ihre Geschäftsleitung für die Daten und die IT verantwortlich. Diese Abhängigkeit führt zu Unsicherheit, denn Sie wissen nicht:

Ist der CSP zuverlässig?

Hält der CSP die Gesetze, Vorschriften und Verträge ein, welche Sie einhalten müssen?



RG: Was sind die besonderen Risiken?

CK: Der Cloud-Nutzer muss sich mindestens folgende Fragen stellen und darauf die für ihn passenden Antworten finden:

- Wird es meinen CSP auch in einigen Jahren noch geben?
- Erfüllt er meine Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit?
- Wie kann er mir dies garantieren?
- Erfüllt er meine Compliance-Anforderungen?
- Wie kann er mir dies garantieren?

RG: Was ist zu tun?

CK: Machen Sie sich klar, welche Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit Sie an die auszulagernden Dienste und Informationen stellen und formulieren Sie daraus die Kernsätze für einen Servicevertrag (Service Level Agreement).

Damit Ihr Unternehmen sicher gedeiht!

Prüfen Sie, welchen Gesetzen Ihr Unternehmen unterliegt, auch in Bezug auf Ihre Kundenbeziehungen.

Machen Sie eine Risikoanalyse: Was sind die Auswirkungen auf mein Business, wenn der CSP die SLAs nicht erfüllt?

Machen Sie einen ausführbaren Plan, wie Sie am Anfang der Geschäftsbeziehung mit dem CSP Ihre Services und Daten in die Cloud migrieren. Berücksichtigen Sie dabei alle technischen und organisatorischen Abhängigkeiten.

Machen Sie einen ausführbaren Exit-Plan, wie Sie am Ende der Geschäftsbeziehung mit dem CSP Ihre Services und Daten wieder zurückholen können.

Machen Sie einen Notfallplan für den Fall, dass der CSP plötzlich untergeht. Klären Sie bereits heute, wie Sie in dieser Notsituation die ausgelagerten Services und Daten wieder zurückholen können.

Wählen Sie einen CSP, der mindestens nach ISO 27001 zertifiziert ist. Dieser hat er seine Risiken im Griff, er wird regelmässig auditiert und er ist gezwungen, seine Informationssicherheit kontinuierlich zu verbessern.

Wählen Sie als CSP ein Schweizer Unternehmen, welches Ihre Daten physisch in der Schweiz lagert. Bedenken Sie: auch eine Schweizer Niederlassung eines amerikanischen Unternehmens unterliegt US-amerikanischen Gesetzen und muss unter Umständen die Daten seiner Kunden offenlegen.

Gerne unterstütze ich Sie auf dem Weg zum sicheren Cloud-Computing.

Damit Ihr Unternehmen sicher gedeiht!

