Neuer Cloud-Dienst? – Gibt es da was zu beachten?

HiSolutions Know-how to go

HiSolutions AG

Daniel Jedecke

jedecke@hisolutions.com

+49 30 533 289-221

Daniel Jedecke

Senior Expert

- Dipl.-Wirtschaftsinformatiker & Master of Science in Applied IT Security

Seit 2001 in der Informationssicherheit tätig:

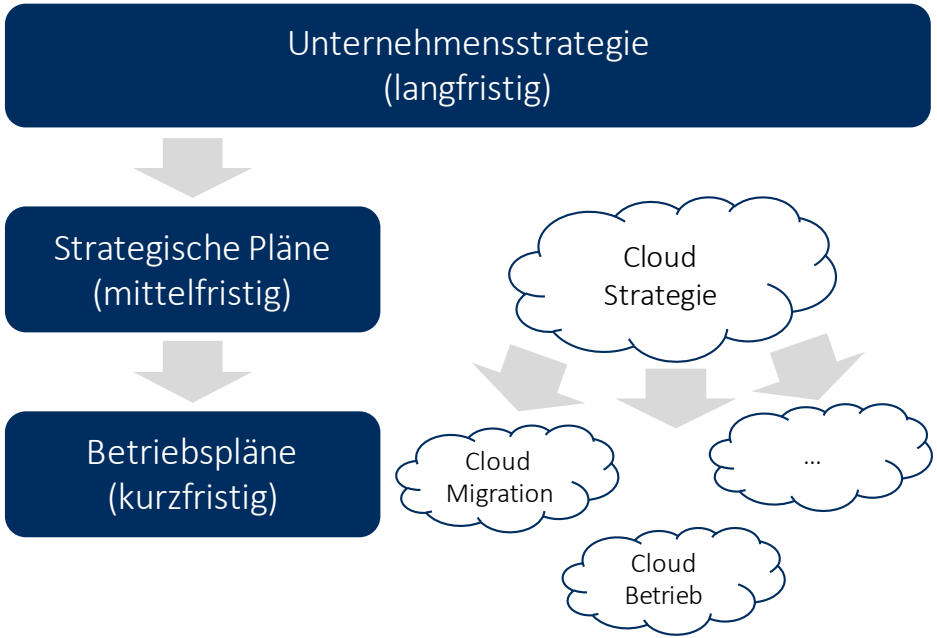
- langjährige Erfahrung im Bereich technische IT-Sicherheit und Audits
- Dozent an der EUFH Brühl / CBS International Business School
- Spezialthemen: KRITIS, Netzwerksicherheit und Cloud
- Expertenwissen in den Bereichen Rechenzentrum, Banken, Aviation und Fraud/Malware

Zertifizierungen (Auswahl):

- Certified Lead Auditor ISO 27001
- Zusätzliche Prüfverfahrens-Kompetenz für § 8a BSIG
- Certified Information Systems Auditor (CISA) & zertifizierter DSB
- GIAC Defensible Security Architecture (GDSA) & GIAC Global Industrial Cyber Security Professional (GICSP)

Cloud Strategie, die gibt es doch bestimmt, oder?

Cloud Strategie im Unternehmenskontext



Was ist eine Cloud Strategie?

Eine Cloudstrategie…

…definiert den Einsatz cloudbasierter Lösungen und Services im Unternehmen.

…leitet sich idealerweise aus den übergeordneten IT-Strategien ab und wird von IT und Fachbereichen gemeinsam entwickelt.

…beinhaltet u. a. Nutzungs- und Migrations-Szenarien, strategische Cloud-Ziele und das Vorgehen zur Etablierung der Cloud.

Cloud-Nutzungsstrategie nach OPS.2.2 Cloud Nutzung

Die Erstellung einer Nutzungsstrategie nach OPS.2.2 basiert auf 3 Säulen

Machbarkeitsstudie

- Definition von Zielen, Chancen und Risiken
- Analyse der rechtlichen und organisatorischen Rahmenbedingungen
- Untersuchung der technischen Anforderungen

Nutzungsanalyse

- Analyse der eigenen Dienste: Welche Dienste können in welchem Bereitstellungs-modell von einem Service-Anbieter bezogen werden?
- Berücksichtigung aller grundlegenden technischen und organisatorischen Sicherheitsaspekte

Sicherheitsanalyse

- Sicherheitsanalyse für den geplanten Cloud-Dienst
- Wiederholung bei Änderung von technischen oder organisatorischen Rahmenbedingungen
- Release-Roadmap bei größeren Projekten

Beispiele für Cloud Strategien

Branchenspezifische Regularien am Beispiel BaFin

- Die BAIT stellen klar, dass AT 9 der Mindestanforderungen an das Risikomanagement der Banken (MaRisk) auch für die Nutzung von Cloud-Computing Dienste gilt, die eine Auslagerung von IT-Dienstleistungen darstellen.
- Es muss vor der Auslagerung geprüft werden, ob es sich um eine wesentliche Auslagerung handelt.
  - Es sind die Vorgaben für wesentliche Auslagerungen einzuhalten, insbesondere auch die Regelungen zu angemessenen beziehungsweise uneingeschränkten Informations- und Prüfungsrechten.
- Mögliche Vorgehensweise werden in der Orientierungshilfe beschrieben. Insbesondere die Möglichkeit „Pooled Audits“ durchzuführen wird beschrieben.

Quelle: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2018/meldung_181108_orientierungshilfe_cloud_anbieter.html

Branchenspezifische Regularien am Beispiel BSI

- Der Mindeststandard des BSI sollte von Bundesbehörden eingehalten werden. Verpflichtend wird dieser nur wenn dieser als allgemeine Verwaltungsvorschrift durch das BMI im Benehmen mit dem IT-Rat erlassen wird.
- Regelt den Lebenszyklus einer Auslagerung an einen externen Cloud-Anbieter: Planung, Beschaffung, Einsatz und Beendigung
- Beispiele:
  - Cloud-Nutzungs-Strategie erstellen
  - Notfall- und Kontinuitätsmanagement
  - Umsetzung Sicherheitsanforderungen
  - Gerichtsbarkeit und Lokation vertraglich zusichern

Quelle: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

Datenschutzrisiken in der Public / Community Cloud

- unberechtigter Zugriff auf Daten durch den Cloud Provider (u.a. Mitarbeiter), durch Dritter oder Geheimdienste
- Datenverlust
- Datenmanipulation
- Diebstahl der Zugriffskennungen und Missbrauch des Accounts
- Zweckentfremdung personenbezogener Daten

Die technischen Anforderungen sollten durch den Cloud-Anbieter umgesetzt sein.

Gibt es Zertifikate, denen man vertrauen kann?

ISO 27001/27002

- ISO 27001 ist ein internationaler, unabhängiger und nichtstaatlicher Standard, der Firmen beim Schutz von Informationsressourcen unterstützt
- Beschreibt Anforderungen für das Einrichten, Realisieren, Betreiben und Optimieren eines dokumentierten Informationssicherheitsmanagementsystems
- ISO 27002 empfiehlt Kontrollmechanismen für die Umsetzung der Anforderungen in 27001
- Im deutschsprachigen Raum ist der BSI IT-Grundschutz auf Basis der ISO 27001 der etablierte und bekannte Standard für Informationssicherheit

Dies ist keine spezielle Zertifizierung für Cloud Provider,

sondern für das gesamte ISMS.

ISO 27017/27018

ISO 27017

- Fachspezifische Subnorm der ISO 27002 mit Anforderung für Cloud-Sicherheit
- Soll die Lücken in ISO 27002 schließen, in dem das Wort „Cloud“ kein einziges Mal vorkommt
- Die Anforderungen richten sich an Cloud-Anbieter und Cloud-Kunden
- Beispiele für Regelungen:
  - Gemeinsame Rollen und Pflichten innerhalb einer Cloud Computing-Umgebung
  - Entfernen und Rückgabe von Kundenressourcen in Cloud Services nach Vertragsende
  - Schutz und Trennung der virtuellen Umgebung eines Kunden von der Umgebung anderer Kunden

ISO 27018

- Fachspezifische Subnorm der ISO 27002 mit Anforderung für Datenschutz in der Cloud
- In 2014 erste datenschutzspezifische Regelungen für Cloud Computing
- Soll datenschutzspezifische Anforderungen zur ISO 27002 und ISO 27017 ergänzen
- Die Anforderungen richten sich allein an Cloud-Anbieter
- Beispiele für Regelungen:
  - Kunden müssen über Speicherorte informiert werden
  - Kundendaten dürfen nicht ohne ausdrückliche Zustimmung für Marketing- oder Werbezwecke verwendet werden

ISO 22301

- International anerkannte High Level Norm für Business Continuity Management
- Definiert Anforderungen an die Planung, den strukturierten Aufbau, die Implementierung, Überwachung und Verbesserung eines Business Continuity Management Systems
- Ganzheitliche Risikobetrachtung und auf allen Geschäftsebenen bzgl. eines Notfallbetriebs
- Entwicklung effektiver Sicherungssysteme und -prozesse
- Hier sind u. a. Notfallübungen gefordert

Auch dies ist keine spezielle Zertifizierung für Cloud Provider, sondern für ein BCM,

welches u. a. Cloud-Aspekte berücksichtigt.

ISO 27012

- Fachspezifische Subnorm der ISO 27002 mit Anforderung für Cyber Versicherungen
- Gehört zur 27000-Familie und muss zusammen mit diesen Normen verwendet werden

Ist eher ein Nischenstandard und hat bisher kaum Bedeutung auf dem Markt

Cloud Controls Matrix (CCM)

- Erstellt von der Cloud Security Alliance (CSA), einer weltweit führenden Organisation zur Definition und Sensibilisierung von Best Practices hin zu einer sicheren Cloud Computing Umgebung
- Community erstellt Richtlinien, Anforderungskataloge und mehr in Workgroups
- Enthält einen Basis-Satz an Sicherheitsmaßnahmen
- Dient zur Hilfe und als Richtschnur für Cloud-Anbieter
- Orientiert sich an internationalen Standards wie NIST CSF, CoBIT, ISO 27001
- Aufgeteilt in 3 Bereiche mit 16 Steuerungselementen:
  - Cloud Architektur
  - Steuerung in der Cloud
  - Betrieb in der Cloud
- Möglichkeit der Selbstauskunft, einer Zertifizierung oder eines Testats
- Ein kontinuierliches Auditverfahren ist in Erstellung
- Webseite: https://cloudsecurityalliance.org

STAR (Security, Trust, Assurance and Risk Registry)

Öffentliche Auflistung von Cloud-Anbietern, die die CSA-Selbstauskunft ausgefüllt haben

- STAR Level 1: Selbstauskunft über den CAIQ v4 Fragebogen
- STAR Level 2: Bescheinigung durch Auditor, welcher die Compliance mit der CSA Cloud Controls Matrix (CCM) bewertet
- STAR Level 3: Der Anbieter überwacht und meldet kontinuierlich die Effektivität der Sicherheitsmaßnahmen über die CSA Continuous Monitoring Guidelines for Cloud Service Providers

Durch diese Selbsteinschätzung und die Auflistung im STAR-Registry können Cloud-Anbieter ihren Sicherheitsanspruch und Transparenz demonstrieren.

CAIQ v4 (Consensus Assessments Initiative Questionnaire v4)

- Sicherheitsfragebogen zur Bewertung von Cloud-Service-Providern
- 16 Steuerungsbereiche (Datenverwaltung, Compliance, Risikomanagement, Vorfallreaktion etc.)
- Basierend auf CCM
- Keine Test- oder Zertifikatsgrundlage, lediglich ein Werkzeug zur Einschätzung
- Muss ausgefüllt werden für einen Eintrag im STAR-Registry (als STAR Level 1)

Der CAIQ v4 bietet eine erste Orientierung für die Selbsteinschätzung bzw.

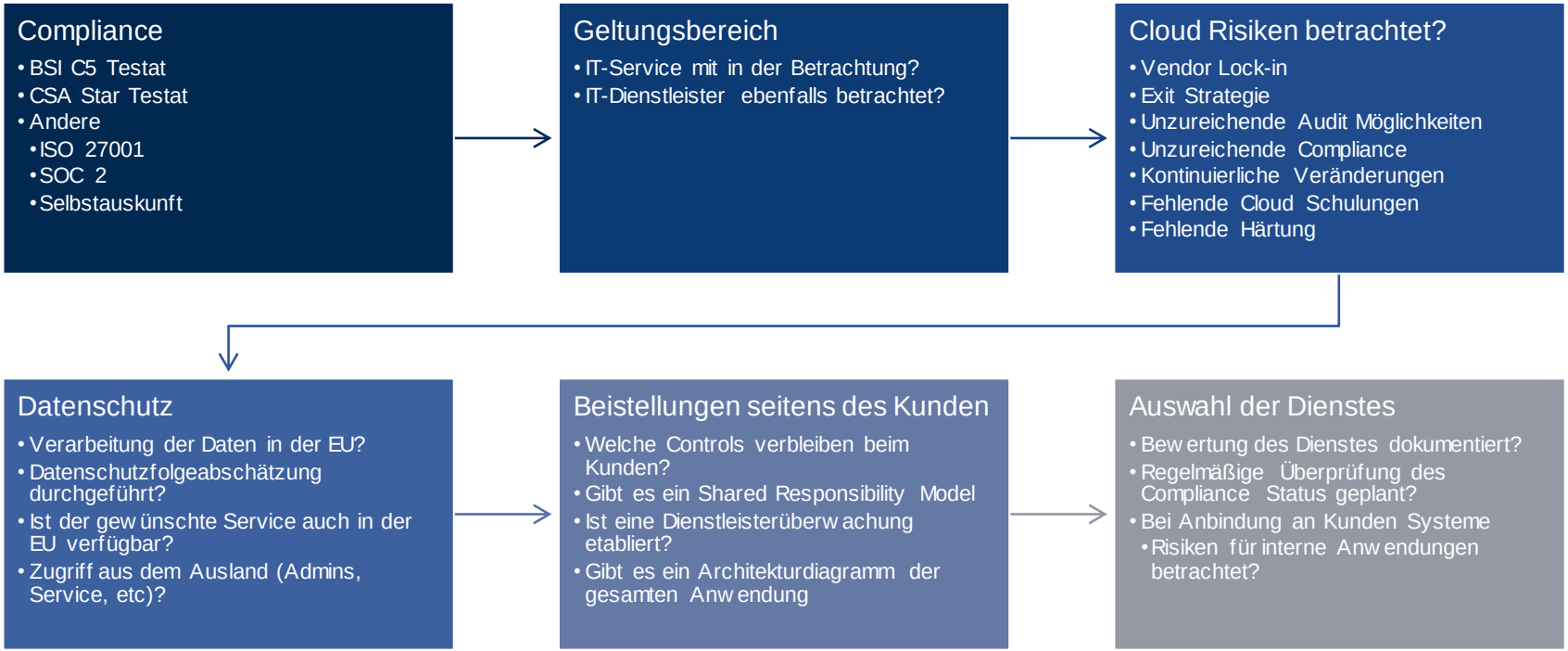
Einschätzung eines Anbieters.

Zertifizierungen / Testate die helfen können, die Sicherheit einzuschätzen

Name des Nachweis	Nachweisart	Prüfungsthemen	Zeitpunkt / Zeitraum
BSI Anforderungskatalog Cloud Computing C5	Testat	Cloudspezifische Prüfung der organisatorischen und technischen Sicherheitsmaßnahmen	Zeitraum
CSA STAR-Selbsteinschätzung	Selbstauskunft	Cloudspezifische Informationen aufgrund einer Selbstauskunft	Zeitpunkt
CSA STAR-Zertifizierung	Zertifizierung	Cloudspezifische Prüfung der organisatorischen und technischen Sicherheitsmaßnahmen	Zeitpunkt
CSA STAR-Testat	Testat	Cloudspezifische Prüfung der organisatorischen und technischen Sicherheitsmaßnahmen	Zeitraum
ISO 22301	Zertifizierung	Allgemeines Notfallmanagement	Zeitpunkt
ISO 27001 mit ISO 27017 und ISO 27018	Zertifizierung	Allgemeine Informationssicherheit mit speziellen Cloud-Anteilen	Zeitpunkt
Trusted Cloud	Selbstauskunft	Cloudspezifische Informationen aufgrund einer Selbstauskunft	Zeitpunkt

Gibt es eine typische Vorgehenweise?

Mögliche Vorgehensweise für die Auswahl eines Cloud Dienstes



Fazit und Ausblick

- Die Auswahl eines Cloud Dienstes ist sehr komplex, da viele Anforderungen zu beachten sind.
- Viele Anforderungen sind den Entscheidern nicht bekannt oder man geht davon aus, das dies schon geklärt ist.

Oft wird ein Cloud Dienst angeschafft, ohne aber zu wissen wie er genutzt werden soll.

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com