Bundesministerium
für Wirtschaft
und Energie

Trusted Cloud

Cloud-Standards und Zertifizierungen im Überblick

Was „Cloud-spezifisch“ beachtet werden sollte

Version 1.0
18. Februar 2016

TrustedCloud

Entwicklung neuer Standards in der EU

Obwohl Cloud Computing im Allgemeinen als etwas Neues Wahrgenommen wird, stellt es aus technischer Sicht nichts grundsätzlich Neues dar.

Neu ist, dass beispielsweise Software, Datenspeicher oder auch Rechenkapazität statt wie bisher im Eigenbetrieb und statisch, nunmehr über ein Netzwerk und dynamisch an den Bedarf der Nutzer angepasst als Dienste zur Verfügung gestellt werden.

Neu ist auch das Ausmaß, in dem die Bereitstellung dieser Dienste erfolgt. Sie zielen nicht mehr auf die Bereitstellung möglichst individualisierter Lösungen ab, sondern auf die massentaugliche Standardisierung der Angebote.

Auf europäischer Ebene befasst sich derzeit die Organisation ETSI (im Auftrag der Europäischen Kommission) mit der Schaffung von Standards für Cloud Computing. Ziel ist es, zunächst bestehende Standards und deren Anwendbarkeit im Cloud-Umfeld sowie fehlende Regelungen zu analysieren und auf dieser Grundlage den weiteren Fahrplan festzulegen.

Der Koordinierungs- und Standardisierungsprozess bei der ETSI wurde in einer 2. Phase überarbeitet. Aufgrund des, vor allem auch politischen, Interesses an Standards für Cloud Computing ist aber davon auszugehen, dass er bald zu weiteren verwertbaren Ergebnissen führen wird.[1]

Im Kontext Cloud Computing sind es die Bereiche Technologie, Management und Recht zu denen allgemeine Vorgaben zu erfüllen sind. Diese sind zumeist nicht Cloud-spezifisch, sondern generell in den Bereichen IT-Outsourcing und Interoperabilität zu berücksichtigen.

[1] http://csc.etsi.org/

Cloud-relevante Standards in Hinsicht auf Compliance-Betrachtungen

	Standards	Beispiele
Technologie	Datei und Austauschformate	OVF, EC2, USDL, CIM SVM, EDI, …
	Programmierungsmodelle	MapReduce, JAQL, PIG, HIVE
	Protokolle & Schnittstellen	OCCI, CDMI, Cloud Audit, Google DLF, …
	Standardkomponenten & Referenzarchitekturen	OpenStack, OSGI, NIST RM, IBM RM, DMTF, CTP, …
	Benchmark & Test	Benchmarking Suits, Security Assessment, …
Management	Geschäftsmodelle	IaaS, PaaS, SaaS operating models, Hybrid, Community
	Service Level-Vereinbarungen	WS-Vereinbarungen (W3C), Business SLAs, …
	Vertragsbedingungen	EVB-IT, EU SVK, Komponenten von T&C, EULA
	Management-Modelle & Prozesse	ISO 27001 / 27002, ITIL, COBIT, …
	Controlling-Modelle & Prozesse	SSAE, SAS 70
	Richtlinien	BSI-Anforderungen, NIST UC, EuroCloud LDP & C
Recht	Gesetzliche Anforderungen	EU Datenschutz Vorschriften, nationale Vorschriften, Privacy Shield (vormals Safe Harbor)
	Freiwillige Verpflichtung	Open Cloud Manifesto, …

Source Analyse by Booz & Company und FZI[2]

[2] http://www.bmwi.de/DE/Mediathek/publikationen,did=476730.html

Cloud-Zertifizierungen

Im Rahmen der European Cloud Partnership hat die EU Kommission weitere Arbeitsgruppen mit ausgewählten Industrievertretern gebildet, die praxisorientierte Empfehlungen für die Themen erarbeiten: Certification, Service Level Agreements, Code of Conduct

Die Ergebnisse werden Basis für die Umsetzung der Anforderungen in der Europäischen Union sein.

Bis dahin kann man folgendes sagen:
Es wird zwischen den drei Arten der Zertifizierungen im Cloud-Umfeld unterschieden und zwar:

1. Zertifizierung von Cloud-Services, wie z.B. EuroCloud Star Audit, CSA oder ISO 27001;
2. Zertifizierung von Cloud-Experten, wie z.B. CCSK (Certification in Cloud Security Knowledge) von CSA, Certified Cloud-Professional (CCP) der Cloud-Schule, CompTIA Cloud Essentials oder EMC Cloud Architect Certification;
3. Zertifizierung von Partnern und Anbietern, wie z.B. Microsoft Private Cloud-Zertifizierung oder SAP-zertifizierter Anbieter von Cloud-Services.

Eine Selbst-Zertifizierung nach Safe Harbor im Bereich Datenschutz mit Anbietern aus den USA reicht nach Meinung von vielen Experten nicht aus und ist seit 1.2.2016 nicht mehr gültig.[3]

Derzeit befindet sich eine Reihe von Cloud-IT-Zertifizierungen im Aufbau. So arbeitet BSI gegenwärtig an den neuen Grundschutzbausteinen „Cloud Management“ und „Cloud Nutzung“, um welche der bestehende IT-Grundschutz erweitert wird. Im Rahmen der ISO wird ebenfalls an spezifischen Vorgaben für Cloud-Computing-Umgebungen gearbeitet und zwar werden die neuen Standards ISO 27017 „Information technology -- Security techniques -- Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002“ und ISO 27018 „Information technology — Security techniques — Code of practice for data protection controls for public cloud computing services” gerade entwickelt.

Cloud-IT-spezifische Auditierungen

Derzeit befindet sich eine Reihe von Cloud-IT-Zertifizierungen im Aufbau. Eine Anlehnung an bestehende internationale Zertifizierungen aus dem Bereich ISO, IDW und nationaler Prüfsysteme macht durchaus Sinn. Allerdings ist es gerade bei einem Klassiker wie der ISO 27001 nicht ganz klar, was denn überhaupt geprüft wurde. Es wird gerne mit dieser Zertifizierung geworben, und es ist unstrittig, dass damit ein relevanter Nachweis der Professionalität des Anbieters erfolgt. Bei dieser Zer-

[3] http://www.eurocloud.de/2016/dokumente/safe-harbor-schonfrist-vorbei-erste-bussgeldverfahren-eingeleitet.html

tifizierung muss aber vorher der Anwendungsbereich (Scope) festgelegt werden, auf den geprüft wird, und dieser muss nicht zwingend den Anforderungen der Compliance-Betrachtung entsprechen. In gleicher Weise ist auch die beliebte Zertifizierung SSAE16/ISAE 3420 (vormals SAS 70 II) zu sehen, die in erster Linie die korrekte Durchführung von Transaktionen in Bezug auf buchhaltungsrelevante Vorgänge testiert.

Relevante Zertifikate von Cloud-Services

Zertifizierung	Cloud-Kontext	Abdeckung/ Reichweite	Anbieter/	Ablauf	Laufzeit	Abdeckung/ Reichweite
EuroCloud Star Audit	explizit	Europäisch	EuroCloud	Dokumenten-review und Vor-Ort Audit	24 Monate	Anbieterprofil, Vertrag und Compliance, Sicherheit, Betrieb und Infrastruktur, Betriebs-prozesse, Anwendung, Implementierung
Trust in Cloud	explizit	National (DE)	SaaS-EcoSystem	Self-Assessment, Dokumenten-review	12 Monate	Referenzen, Daten-sicherheit, Qualität der Bereitstellung, Entschei-dungssicherheit, Vertragsbedingungen, Service-Orientierung, Cloud-Architektur
"Trusted Cloud - TÜV"	explizit	Europäisch (mind. DACH)	TÜV Trust IT GmbH (Austria)	Vor-Ort Audit (TÜV)	24 Monate	Sicherheit
TÜV Cloud Security	explizit	National (Deutschland)	TÜV Rheinland	Dokumentenreview, Vor-Ort Audit (TÜV)	k.A.	Sicherheit
TRUSTed Cloud Privacy Zertifizierung	explizit	International (wichtig für CSPs welche in der EU operieren)	TRUSTe	TRUSTe Review und Evaluation	12 Monate	Datenschutz, Bescheini-gung der Compliance
CSA STAR	explizit	International	CSA	Self-Assessment	12 Monate	Sicherheit
FedRaMP	explizit	USA	FedRaMP General Services Administrati-on; Akkreditierte Zertifizierungs-organisation	Self-Assessment	12 Monate	Sicherheit
EuroPrise (Euro-pean Privacy Seal)	implizit	EU	Unabhängiges Landes-zentrum für Daten-schutz Schleswig-Holstein (ULD), Zwei akkreditierte Experten (Recht und IT)	Vor-Ort Audit, Do-kumentenreview	24 Monate	Datenschutz
ISAE 3402/SSAE 16 Typ II (früher SAS70)	implizit	International	Diverse zertifizierte Organisationen, z.B. PWC	Vor-Ort Audit	6-12 Mo-nate	Interne betriebliche Kontrollen (IKS)
ISO 27001	implizit	International	Diverse, s.o.	Vor-Ort Audit	36 (12) Monate	Sicherheit
BSI IT-Grundschutz	implizit	National (DE)	BSI, Zertifizierte Audi-toren	Dokumenten-Review, Vor-Ort Audit	36 (12) Monate	Sicherheit

Bundesministerium
für Wirtschaft
und Energie

Trusted Cloud

Impressum

Redaktion

Kompetenznetzwerk Trusted Cloud e. V.

c/o INNOVA Beratungsgesellschaft mbH

Lückhoffstraße 33

14129 Berlin