Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

European Cloud Service
Data Protection Certification

Workshop Nr. 2 für Cloud Service Provider
Use Cases zur Datenschutzzertifizierung AUDITOR

Protokoll

Inhaltsverzeichnis

Einleitung

Ziel des Forschungsprojekts „AUDITOR“ als Nachfolger des Trusted Cloud Datenschutz-Profil (TCDP) ist die Konzeptionierung, exemplarische Umsetzung und Erprobung einer nachhaltig anwendbaren EU-weiten Datenschutzzertifizierung von Cloud-Diensten. Die Zertifizierung nach Maßgabe der EU-Datenschutz-Grundverordnung (DSGVO) ist im Interesse aller Beteiligten: Der Cloud-Kunden, die nur mit solchen Cloud-Anbietern zusammenarbeiten dürfen, die hinreichend Garantien zur Einhaltung des Datenschutzes vorweisen können; der Cloud-Anbieter, die mit einer Zertifizierung eben diese Sicherheit bieten können; und der Zertifizierer, für deren Geschäftsfeld die DSGVO zwingende Regeln vorsieht.

Um eine nachhaltige Datenschutzzertifizierung zu konzipieren, wird zunächst ein Kriterienkatalog für die Zertifizierung von Cloud-Diensten nach der DSGVO entwickelt und eine entsprechende Standardisierung angestrebt. Außerdem werden geeignete Organisationsstrukturen und Verfahren zur Durchführung einer europaweit anerkannten Datenschutzzertifizierung konzipiert. Hierzu zählt insbesondere auch die Spezifikation von modularen Zertifizierungs- und Auditierungsprozessen.

Um eine nachhaltige Verwendung und weitreichende Verbreitung von AUDITOR sicherzustellen, werden schließlich Geschäftsmodelle für ein nachhaltig erfolgreiches AUDITOR-Verfahren untersucht. Das erarbeitete Zertifizierungsverfahren und die im AUDITOR-Projekt erarbeiteten und für eine Standardisierung vorbereiteten Kriterien sollen schließlich in der Praxis erprobt und validiert werden.

Das Projekt AUDITOR hat eine Laufzeit von zwei Jahren und ist am 01.11.2017 offiziell gestartet. Das Projekt wird vom Bundesministerium für Wirtschaft und Energie mit einem Gesamtvolumen von 1,7 Mio. Euro gefördert. Verbundkoordinator ist Prof. Dr. Ali Sunyaev vom Karlsruher Institut für Technologie. Die weiteren Konsortialpartner CLOUD&HEAT, datenschutz cert, DIN e.V., ecsec, EuroCloud Deutschland_eco e.V. und Universität Kassel bringen komplementäre Expertise in das Projekt ein.

Ziele des Workshops

Das Forschungsprojekt AUDITOR hat seinen Kriterienkatalog in der Entwurfsfassung 0.8 nur den Teilnehmern zur Verfügung gestellt. Ebenso wurden auch weitere Dokumente verteilt (http://www.auditor-cert.de/publikationen/).

- Kriterienkatalog deutsch: https://www.auditor-cert.de/wp-content/uploads/2018/10/Kriterienkatalog_prev0_8.pdf
- Kriterienkatalog englisch: https://www.auditor-cert.de/wp-content/uploads/2018/10/Criteria_Catalogue_v0_8.pdf
- Umsetzungshinweise/Nachweis: https://www.auditor-cert.de/wp-content/uploads/2018/10/UmsetzungshinweiseNachweise_prev0_8.pdf
- Schutzklassenkonzept: https://www.auditor-cert.de/wp-content/uploads/2018/10/Schutzklassenkonzept_prev0_8.pdf

Um die Anwendbarkeit des AUDITOR-Katalogs sicherzustellen, war es das Ziel des Workshops, beispielhafte Umsetzungen der Kriterien des Katalogs zu diskutieren („Use-Cases“). Durch die Diskussionen im Workshop sollten auch Probleme und offene Fragestellungen, bspw. in Bezug auf die Verständlichkeit der Kriterien, identifiziert werden (siehe Abbildung 1). Basierend auf dem Feedback wird das AUDITOR-Konsortium die Kriterien und Umsetzungshinweise überarbeiten und weiter verfeinern.

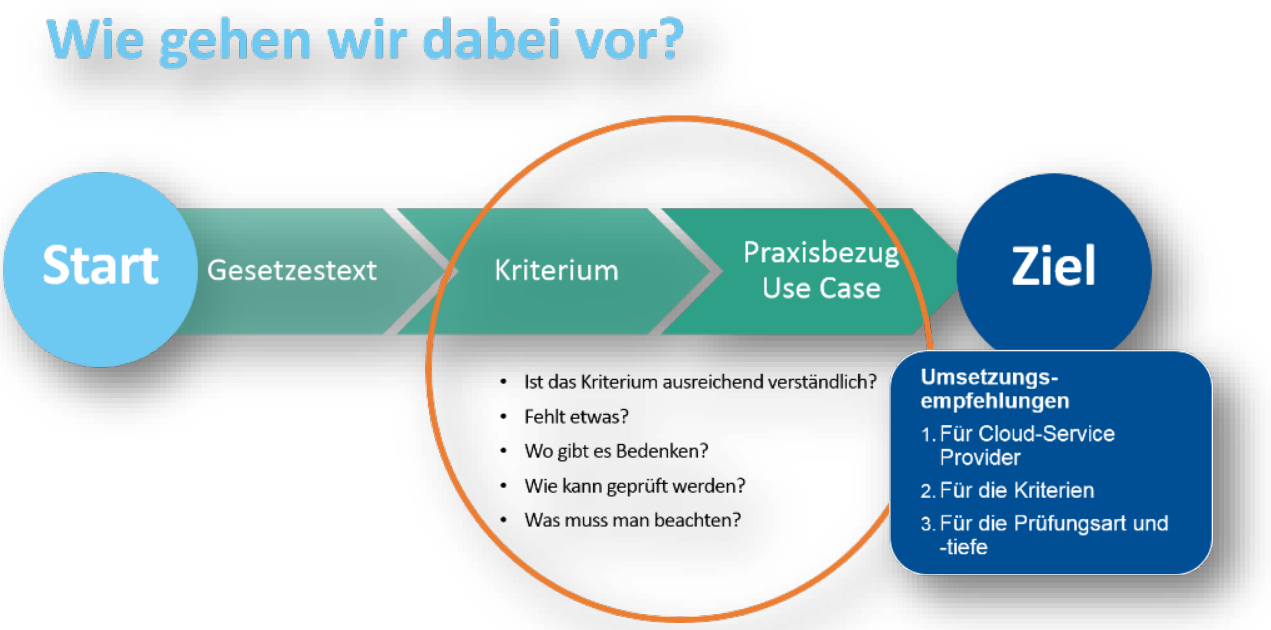


Abbildung 1. Ziele des Workshops.

Überblick über die Use Cases.

1	8.2 Meldung von Datenschutzverletzungen	Datenschutzvorfall – Was muss man tun?
2	10.1 bis 10.5 Subauftragsverarbeitung	Subunternehmer einordnen und abgrenzen
3	Das Standard Datenschutzmodell der Aufsichtsbehörde	Gewährleistungsziele sind den „Erläuterungen“ zu den Kriterien beigefügt. Ist das ausreichend?
4	11.1 und 11.2 Auftragsverarbeitung in Drittländern	Welche Vereinbarungen gibt es? Wie auf die Dynamik der Entwicklung reagieren?

Anmerkungen und Ergebnisse zu den Use Cases

Use Case 1 „Meldung von Datenschutzverletzungen“

- Prozessverlauf und Einzelbetrachtung sind hier wichtig -> die Notwendigkeit eines vordefinierten Prozesses wird unterstrichen

Offene Fragen Anmerkungen:

- Ab wann ist was Meldepflichtig (Verdachtsfälle vs. Nachweisliche Datenschutzverletzung) -> das müsste irgendwo festgelegt werden
- Das Ausmaß des Vorfalles ist entscheidend
- Daten müssen verwertbar für den Anwender sein, hinreichend konkretisiert via Template -> es müsste allgemeine Templates dazu geben

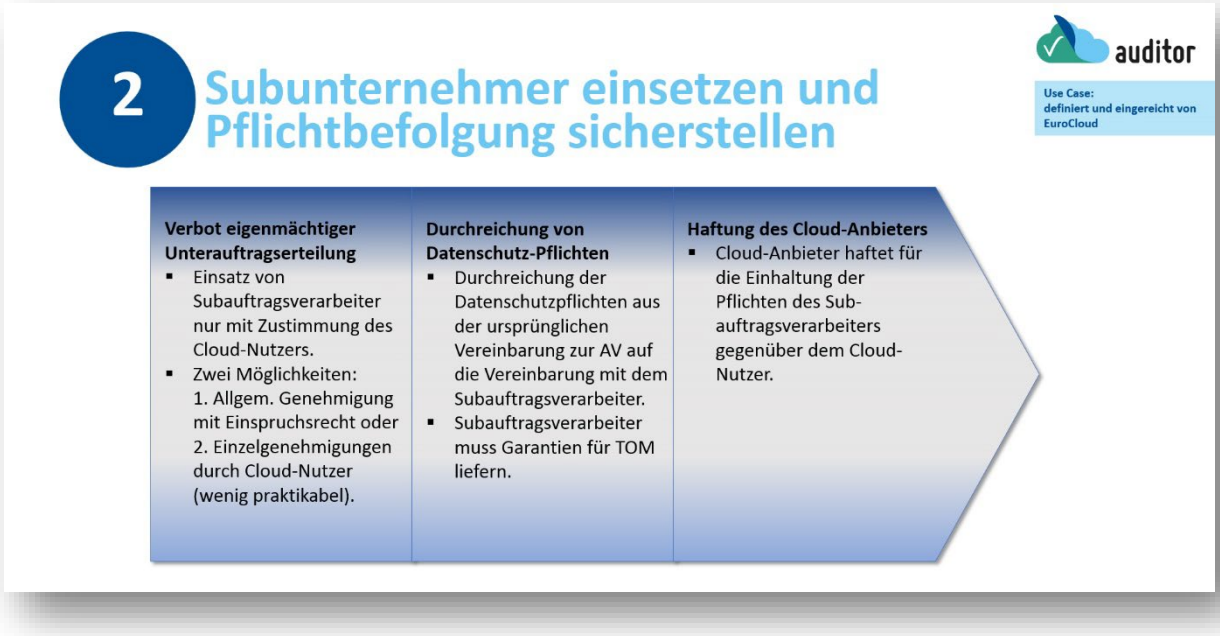
Hinweise:

- Datenschutzvorfall ist ein Security Incident, dieses setzt auf bewährte Prozesse auf
- Behörden haben Formulare, welches bei den Umsetzungshinweisen berücksichtigt werden könnte
- auf beide „Standards kann man aufsetzen

Relevanz für die Prüfung:

- Wie wird der Erfüllungsgrad bemessen?
- Gibt es einen Bewertungsspielraum?

Use Case 2 „Subauftragsverarbeitung“



- Wie geht man damit um: eine Rechtsverbindliche Vereinbarung kann auch mündlich erfolgen?
- Die Auswahl des Subunternehmens unterliegt dem Provider, der Kunde hat nach Information über einen Wechsel ein Sonderkündigungsrecht, **die Vorrausetzung dazu ist Portabilität**
- Datenschutzrechtliche Unterscheidung zwischen Abrechnungsdaten des Providers und den Kundendaten ist noch nicht zur Verantwortungsabgrenzung geklärt.
- Im Kriterium 10.2 ist nicht klar definiert, wie der Vertrag aussieht. Ist hier auch die Definition bzgl. schriftlich/elektronisch anwendbar?
- Sind im Kriterium 10.5 auch Lieferanten-Assessments wirksam? Sollte in den Umsetzungshinweisen klar definiert werden.

Zur Prüfung

- Im Pilotverfahren sollte folgendes konkretisiert werden:
    - Wird es ein Punktesystem für Erfüllungsgrad geben?
    - Wird es Mappings von anderen Zertifizierungen geben?

Orientierungswissen:

- Im Einkauf und der Beschaffung:
  Können die Kriterien auch für das Lieferanten Assessment dienen (Orientierungswissen oder Umsetzungshinweise?)

Use Case 3 „Das Standard-Datenschutzmodell der Aufsichtsbehörden“

- Das SDM wird als Hilfestellung verstanden
- Die Gegenseitige Rückkopplung dient zum Verständnis und zu Ableitungen
- Die Erwartung ist, dass es evtl. Auswirkungen auf die Ausgestaltung der Prüfung hat
- Es wird die Bitte an uns herangetragen, die Zuordnungstabelle mit der Kriterien Übersicht zu EU-DSGVO und SDM zur Verfügung zu stellen.

Use Case 4 „Auftragsverarbeitung in Drittländern “

- Vertreter sollte nicht nur eine Briefkastenfirma sein, sondern zulieferfähig d.h.:
  - telefonisch erreichbar
  - auskunftsfähig
  - handlungsfähig

Ihre Empfehlungen – Unsere Aufgaben

Das AUDITOR-Konsortium wird gemeinsam das Feedback der Teilnehmer aufnehmen und prüfen. Die Ergebnisse, die aus dem Feedback des Workshops hervorgehen, werden in der Veröffentlichung der nächsten Versionen der AUDITOR Dokumente berücksichtigt.

Impressionen

Nächste Schritte

Das AUDITOR-Konsortium plant weitere Workshops zur Validierung des Katalogs:

- Mögliches BMWi-Symposium April
- Workshop in Brüssel im März 2019 zur Europäisierung von AUDITOR

Wir bedanken uns bei allen Teilnehmern und freuen uns auf eine weitere Zusammenarbeit!