Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

European Cloud Service
Data Protection Certification

Workshop 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 0.7 veröffentlicht, welcher Kriterien, Erläuterungen, Umsetzungshinweise und Nachweise enthält (docs.auditor-cert.de).

Um die Anwendbarkeit des AUDITOR-Katalogs sicherzustellen, war es das Ziel des Workshops, beispielhafte Umsetzungen der Kriterien des Katalogs zu diskutieren („Use-Cases“). Dabei wurden im wesentlich zwei verschiedene Bereiche unterschieden: Technische und organisatorische 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.

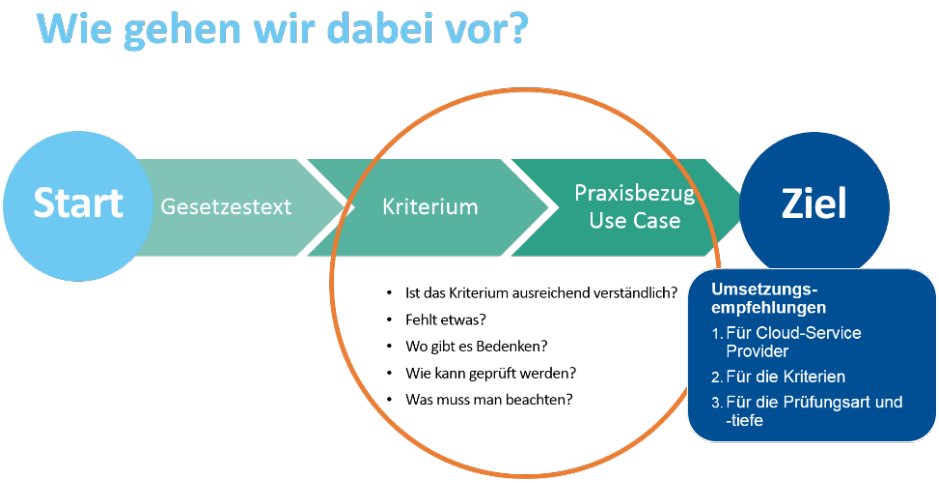
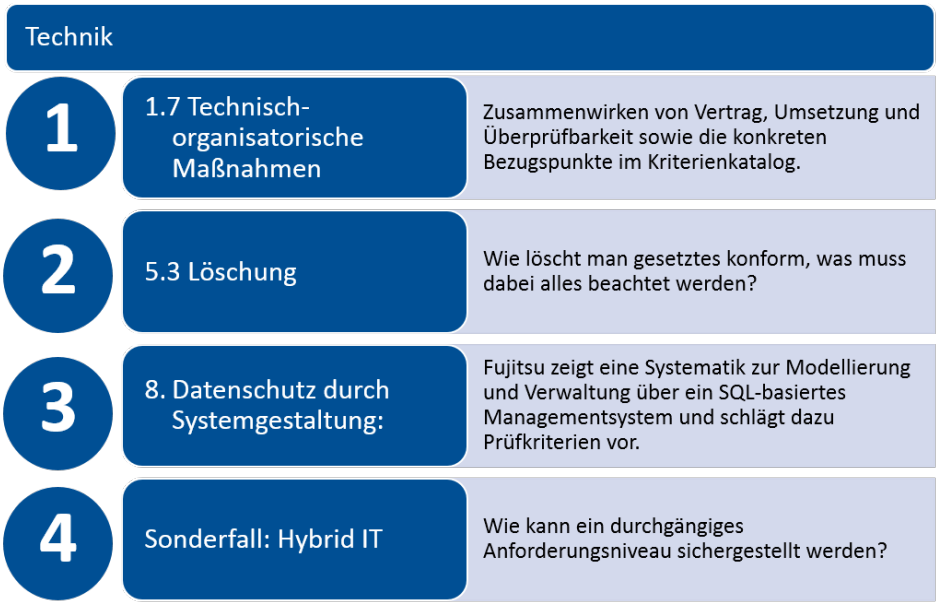


Abbildung 1. Ziele des Workshops.

Überblick über die Use Cases „Technik“



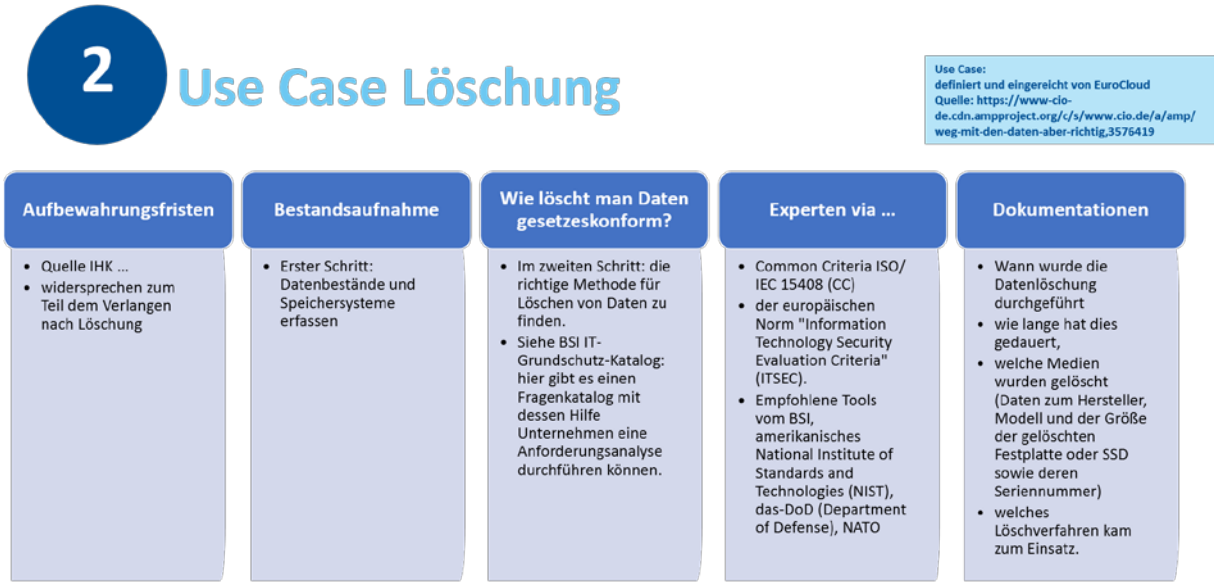
Anmerkungen und Ergebnisse zu den Use Cases

Use Case 1 „Technisch-organisatorische Maßnahmen“

- Korrelation Schutzklasse und Pseudonymisierung sollte beachtet werden
- Schutzklassen müssten genauer definiert, überarbeitet und abgrenzt werden
- Je nach Schutzklasse wird eine Anforderungsliste impliziert
- Schutzklassenbetrachtungen über alle Maßnahmen sind zu grob
- Zum Teil ist es eine Kundenentscheidung oder sogar Kundenverantwortung, auf welchen Strecken Daten pseudonymisiert werden
- Bestimmte Geschäftsmodelle sind mit Pseudonymisierung nicht möglich

Die ideale Lösung ist ein hoher Automatisierungsgrad

Use Case 2 „Löschung“



- Es bleibt die offene Fragestellung: Wie weist man eine Löschung nach?
- Das Kriterium ist konkreter und besser gefasst als im TCDP
- Die Din Referenzen sind falsch angegeben
- Die gängige Definition des BSI IT Grundschutz ist bei Cloud Anwendungen nicht 1:1 anwendbar

Use Case 3 „Datenschutz durch Systemgestaltung“

- Die gezeigte Referenzarchitektur (siehe Abbildung 2) ist eine gute Vorlage zur weiteren Ausarbeitung
- Kriterium hängt nicht von den Schutzklassen ab, sollte es aber
- Unterschiedliche Voreinstellungen je nach Schutzklasse sollten möglich sein, aber nicht beliebig je nach Anforderung des Kunden

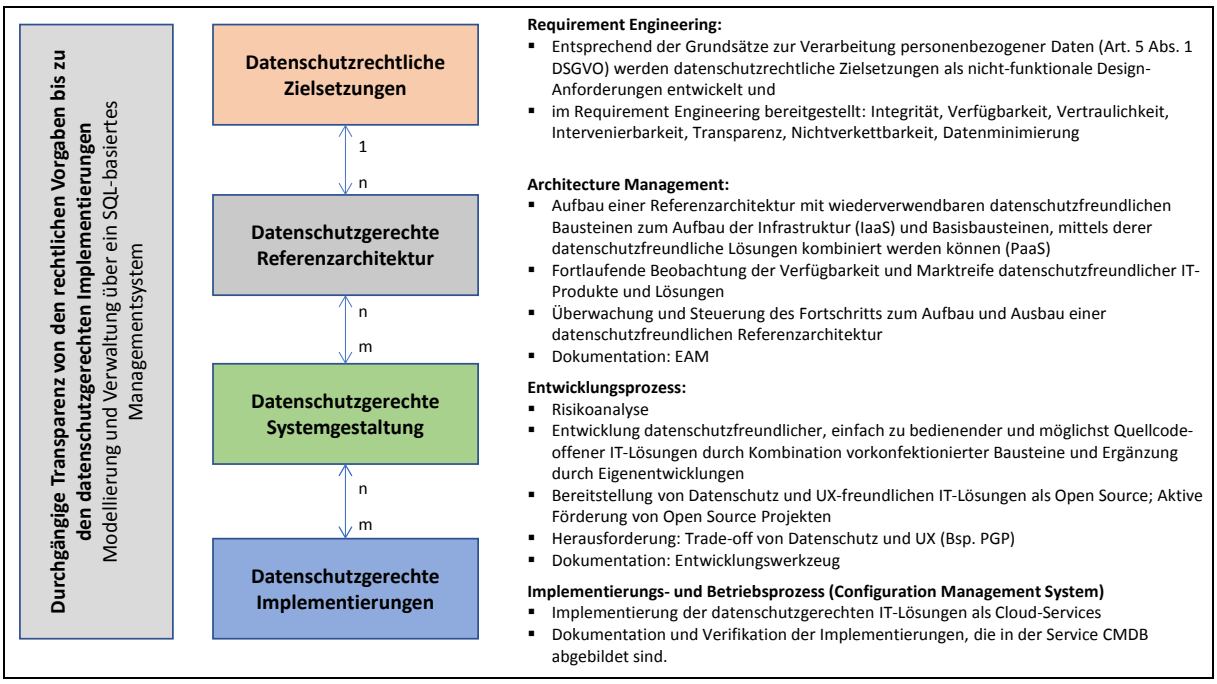


Abbildung 2 Referenzarchitektur für Datenschutz durch Systemgestaltung gemäß Fujitsu

Use Case 4 „Sonderfall Hybrid IT“

- Diskussion über ein modulares Konzept, das in der Verfahrensordnung beschrieben werden muss
- Verfahrensgesamtheit muss betrachtet werden; das kann in Modulen erfolgen, deren Grenzen genau definiert sind.
- Kriterium 1.5 Abs. 3 muss konkretisiert werden: wesentliche Abweichung?
- Generelle Terminologie müsste überprüft und vereinheitlicht werden: Zugang, Zutritt, Zugriff, Admin oder Nutzerzugriffe
- Kriterium 10.1. hier müsste der Schutzraum im Rahmen der Verarbeitungstätigkeit erweitert werden, bzw. darüber müsste man diskutieren

Überblick über die Use Cases „Organisation“

Anmerkungen und Ergebnisse zu den Use Cases

Use Case 1 „Cloud-Vertrag“

- Die Formulierung „Cloud-Vertrag“ ist missverständlich und sollte in „Auftragsverarbeitungsvertrag“ umgeändert werden, da in der Praxis in der Regel zwei Verträge geschlossen werden: Ein Auftragsverarbeitungsvertrag und ein diesem zugrunde liegender Vertrag über die Leistungserbringung.
- Der Vertrag wird in der Praxis weiterhin in der Formulierung sehr abstrakt gehalten
- Ggf. ist ein Beispielsvertrag oder eine Vertragsstruktur anzufertigen
- Bei der Übersicht über mögliche Weisungen nimmt die Leistungsbeschreibung eine maßgebliche Rolle ein
- Die namentliche Befugnis Erteilung für Weisungen ist nicht möglich. Es sollte eine Weisungsbefugnis Erteilung auf Abteilungs- Funktionsebene im Vertrag verankert werden.
- Ein Zusatz zum Weisungsrecht sollte im Vertrag verankert werden
- Bei der Angabe des Ortes der Datenverarbeitung sind der Rechtsraum und das entsprechende Datenschutzniveau entscheidend. Es muss angegeben werden, ob die Daten in der EU/im EWR oder in Drittländern verarbeitet werden. Eine spezifische Adressangabe wird von der DSGVO nicht gefordert, sollte aber möglichst präzisiert werden, um Vertrauen am Markt zu erzeugen.

Use Case 2 „Beauftragter für Informationssicherheit und Kooperation“

- Klärung, ob die gleiche Person die Rolle des Informationssicherheits- und Datenschutzbeauftragten innehaben kann. Meinung der Teilnehmer: prinzipiell können beide Rollen in einer Person verankert werden, insofern es zu keinen Interessenkonflikten kommt. Dies ist insb. bei der Beauftragung von externen Datenschutzbeauftragten relevant.
- AUDITOR sollte die Kooperation zwischen den Beauftragten nicht fordern, sondern lediglich als Umsetzungshinweis bzw. Empfehlung angeben.

- Bei der Europäisierung von AUDITOR sollte beachtet werden, dass vorwiegend deutsche Konzepte, wie die des Informationssicherheitsbeauftragten nicht mit anderen EU-Vorstellungen kollidieren.

Use Case 3 - 4 „Auskunftserteilung & Widerspruch“

- Die Wahrung der Betroffenenrechte ist stark abhängig vom jeweiligen Service-Model des Cloud-Dienstes. So sind diese insbesondere im Falle eines IaaS-Anbieters nur begrenzt oder nicht umsetzbar.
- Die Spezifikation der Service-Modelle sollte sich an der etablierten Klassifizierung von SaaS, PaaS und IaaS orientieren, jedoch nur inhaltlich. Eine abstraktere Formulierung erlaubt mehr Spielraums und eine bessere Verortung der Cloud-Dienste.

Ihre Empfehlungen – Unsere Aufgaben

Das AUDITOR-Konsortium wird gemeinsam die Anmerkungen der Teilnehmer kritisch reflektieren und überlegen, welche Änderungen am Katalog wie vorgenommen werden können. Insbesondere sind folgende wesentliche Schritte geplant:

- Überprüfung der generellen Terminologie:
    - Vereinheitlichung und Detaillierung der genutzten Begriffe
    - Ggf. Orientierung an den Begrifflichkeiten in den Gesetztestexten, bspw. „Cloud-Nutzer“ → „Verantwortlicher“
- Überarbeitung des Schutzklassenkonzeptes:
    - Schutzklassen müssten genauer definiert, überarbeitet und abgrenzt werden
    - Ziel einer Normalverteilung der Schutzklasse, wobei die meisten Anbieter in Schutzklasse 2 fallen würden
- Spezifikation der Zertifikatsreichweite
    - Erläuterung welche Reichweite (insb. in Hinblick auf Subprovider) AUDITOR einnimmt
    - Ergänzung von Beispielen zum besseren Verständnis
    - Das AUDITOR-Zertifikat muss eine klare Aussage über den Zertifizierungsgegenstand und -scope an den Verantwortlichen und Betroffenen vermitteln können
- Überprüfung, ob der Kriterienkatalog Anforderungen enthält, welche nicht explizit in der EU-DSGVO gefordert werden
- Planung von weiteren Maßnahmen zur Schaffung einer Awareness von AUDITOR und dadurch Erhöhung der Marktakzeptanz
- Rückmeldung zur Einarbeitung des Feedbacks geben

Impressionen


1
WAS

Nächste Schritte

Das AUDITOR-Konsortium weitere Workshops zur Validierung des Katalogs:

- Follow-Up Workshop im Oktober/November mit allen Teilnehmern
- Mögliches BMWi-Symposium April 2019
- Workshop in Brüssel im Januar / Februar 2019 zur Europäisierung von AUDITOR
- Prüfung des British Standards BS 10012:2017 ob er in Vergleichbarkeit zu AUDITOR eine GDPR Zertifizierung ermöglicht
  Siehe auch: https://www.bsigroup.com/de-DE/BS-10012/?gclid=CjwKCAjw7cDaBRBtEiwAsx-prXXRoFoTQYUIp8GUsBzYDl4z39Wh4oczfIYqoHfemdKbazUaKJQSunhoCeVQQAvD_BwE

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