Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Sicherheitstechnische Herausforderungen in Cloud-Computing-Architekturen

Chancen und Herausforderungen für die gemeinsame Datennutzung in Justiz und Verwaltung

32. Deutscher EDV-Gerichtstag

14.09.2023, Saarbrücken

Agenda

Konzepte gemeinsame Datennutzung

Datenhoheit vs. Überwachungsschutz

Paradigma Cloudcomputing

Sicherheit Cloud-Architekturen

BSI Angebote für Cloudsicherheit

Technische Perspektive Akteneinsicht

Digitale Transformation in Justiz und Verwaltung

- Große Datenmengen sind zu speichern
- Daten müssen vielfach transportiert werden
- Sicherheit der Daten gewährleisten
- Nutzererlebnis und Leistungsfähigkeit gestalten

Kritischer Erfolgsfaktor → Speicherstrategie

Sicherheitstechnische Perspektive Akteneinsicht

Dezentrale Datenhaltung

Jede Behörde speichert eine Aktenkopie

+ Hohe IT+Daten Souveränität
+ Geringeres Überwachungsrisiko
- Hoher IT Ressourcen Aufwand
- Lange eGov Transformationszeit
- Unterschiedliches Sicherheitsniveau
- Varianz in der Datenaktualität
- Geringe Aktenhoheit

Zentrale Datenhaltung

Gemeinsame Speicherung in einem RZ

+ Optimierte IT Ressourcen
+ Ermöglicht eGov Flexibilität
+ Steuerbarer Datenzugriff [Aktenhoheit]
+ Einheitliches Sicherheitsniveau
- Abgabe von Kontrolle
- Attraktives Angriffsziel
- Potenzielles Überwachungsrisiko

Sicherheitstechnische Perspektive
Akteneinsicht

Datenhoheit - Kontrolle und Steuerung von Zugriffsrechten

- Komplexe Zugriffssteuerung ist technisch möglich
- Fokus auf das Bereitstellen von Informationen statt Dateien
- Behördenübergreifendes Identitätsmanagement
- Berechtigungsmanagement
- Wirksamkeitskontrolle und Dokumentation
- Protokollierung und Nachvollziehbarkeit

Sicherheitstechnische Perspektive
Akteneinsicht

Datenschutz - Vermeidung von Überwachungen der Einsichtnahmen

- Anonyme Zugriffe sind technisch möglich
- Anonymisierte / Pseudonymisierte Authentisierungsinformationen
- Schwache Zugriffsprotokollierung
- Beschränkte Speicherdauer der Protokollierung
- Transparente und eingeschränkte Berechtigung auf Logdaten und Protokolle

Sicherheitstechnische Perspektive
Zentrale Datenhaltung

Datenhoheit

Anforderungen

- Transparente Berechtigung
- Wirksamkeit Zugriffssteuerung
- Nachweis berechtigte Zugriffe
- Vorsorge für IT Forensik

Datenschutz

Anforderungen

- Transparente Berechtigung
- Keine personalisierte Zugriffshistorie
- Vertraulichkeit der Einsichtnahme
- Vermeidung Ausforschungsmöglichkeit

Paradigma Cloud Computing

Cloud Computing ist eine Form der Bereitstellung von IT-Dienstleistungen über Netze.

Gemeinsam nutzbare und flexibel skalierbare IT-Leistungen durch nicht fest zugeordnete IT-Ressourcen.

Hoch automatisierte Servicebereitstellung ermöglicht die bedarfsorientierte, dynamische Anpassung von Angebot, Nutzung und Abrechnung.

Cloud Bereitstellungsmodelle

Public Cloud [Externe Cloud]

- Nutzbar durch die Allgemeinheit oder große Gruppen
- Keine Lokalisierung der IT-Ressourcen
- Die Nutzer sind organisatorisch nicht verbunden

Private Cloud

- Betrieb innerhalb einer Organisation oder eines geschlossen Verbunds
- Nach Cloud-Kriterien virtualisierte Betriebsumgebung unter Kontrolle des Kunden

Community Cloud [Justizcloud]

- Infrastruktur wird von mehreren Institutionen und Akteuren geteilt

Cloud Computing
Chancen und Risiken

Chancen / Potenzial

- Flexible IT-Services (Agilität)
- Dynamische Anpassung an Bedarf
- Verteilte IT-Leistungserbringung
- Selbstservice
- Schnelle Realisierbarkeit
- Auch bei fehlendem Know-How
- Kostensenkung

Risiken / Bedrohungen

- Zugriff auf Daten durch Cloud-Betreiber
- Datenverlust bzw. Informationsabfluss
- Ausfall der Netzverbindung
- Denial-of-Service Angriffe auf DL
- Digitale Souveränität (Abhängigkeiten)
- Kompromittierung der Authentisierung
- Know-How Verlust

Informationssicherheit in Cloud-Architekturen

Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität

Sicherheit der Cloud-Infrastruktur

- Rechenzentrumssicherheit,
- Server, Virtualisierung, Netzwerk

Sichere Verwaltung von Cloud-Services

- Identitäts- und Rechteverwaltung,
- Protokollierung, Beweissicherung,
- Interoperabilität und Portabilität

Sicherheit von Daten und Plattformen

- Logische / physische Trennung,
- Daten-Backup und Wiederherstellung

Sicherheit von Web-Applikationenn

- Authentifizierung und -verschlüsselung,
- Sitzungsverwaltung,
- Eingabevalidierung,
- Auditing and Logging sowie
- Ausnahme-Management.

BSI Angebote Cloud-Nutzung

Vorgaben, Expertise und Arbeitshilfen

- BSI Informationen zu Risiken und Sicherheitstipps
- Grundschutz Cloudbausteine
- Mindeststandard Nutzung externer Cloud-Dienste
- eVB-IT Cloud
- BSI Kriterienkatalog - C5

Nutzung von Public Clouds in der [Bundes]verwaltung

Mindeststandard des BSI

- Voraussetzung: ISMS auf Basis IT-Grundschutz
- Umsetzungspflicht in Bundesbehörden (§ 8 Absatz 1 Satz 1 BSIG)
- Schritt für Schritt Vorgehensweise
- Konkrete Sicherheitsanforderungen

eVB-IT Cloud

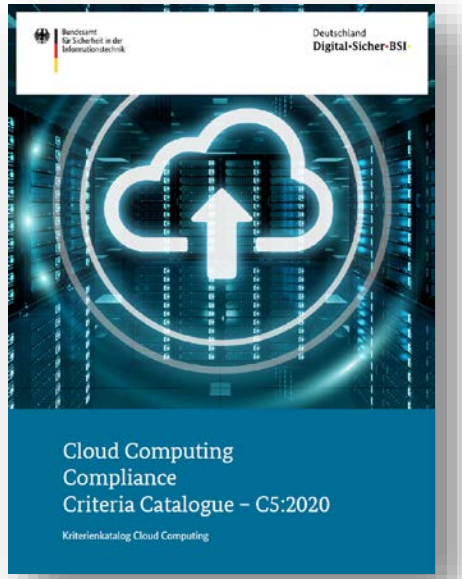
- Ergänzende Vertragsbedingungen zur Beschaffung von IT-Leistungen Cloud
- Verhandelt zwischen BMI und BITKOM (unter Beteiligung BSI)
- Einhaltung BSI C5 durch Anbieter ist Vertragsbestandteil

BSI Kriterienkatalog Cloud Computing [C5:2020]
Standard für Cloud-Sicherheit

Cloud Computing Compliance Criteria Catalogue …

- spezifiziert Kriterien zur Beurteilung der Sicherheit von Cloud-Diensten,
- richtet sich an professionelle Cloud-Anbieter, deren Prüfer und Kunden.

- Grundlage ist ISO/IEC 27001
- C5-Kriterien gliedern sich in 17 Bereiche
- Basiskriterien und Zusatzkriterien
- Ergänzende Informationen und Hinweise zu Rahmenbedingungen
- Prüfung nach ISAE 3000/3402 (WP Audit)



BSI Kriterienkatalog Cloud Computing [C5:2020]

Bereich 7: Identitäts- und Berechtigungsmanagement (IDM)

Zielsetzung: Absichern der Autorisierung und Authentifizierung von Benutzern des Cloud-Anbieters zur Verhinderung von unberechtigten Zugriffen.

- IDM-02: Vergabe und Änderung von Zugangs- und Zugriffsberechtigungen,
- IDM-06: Privilegierte Zugriffsberechtigungen
- IDM-07: Zugriff auf Daten der Cloud-Kunden
- IDM-08: Vertraulichkeit von Authentisierungsinformationen

BSI Kriterienkatalog Cloud Computing [C5:2020]

Bereich 7: Regelbetrieb (OPS)

Zielsetzung: … Protokollierung und Überwachung von Ereignissen.

- OPS-10 Konzept Protokollierung und Überwachung,
- OPS-11 Protokollierung – Umgang mit Metadaten
- OPS-12 Protokollierung – Zugriff, Speicherung und Löschung
- OPS-13 Protokollierung – Erkennung von Ereignissen
- OPS-14 Protokollierung – Aufbewahrung der Protokollierungsdaten

BSI Kriterienkatalog Cloud Computing [C5:2020]

BC-05 Angaben zum Umgang mit Ermittlungsanfragen staatlicher Stellen

- Verfahren zur Verifizierung der Rechtsgrundlage solcher Anfragen,
- Verfahren zur Information und Einbindung der Cloud-Kunden,
- Widerspruchsmöglichkeiten,
- Möglichkeit zur Entschlüsselung von Kundendaten

Beschreibungen zu Rahmenbedingungen (Deutschland, USA, China)

Schlussbemerkung

- Cloud Computing → Akteneinsicht 2.0
- Cloud Risiken können beherrscht werden

- Paradigmenwechsel Information
- Datenhoheit vs. Überwachung

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Kontakt

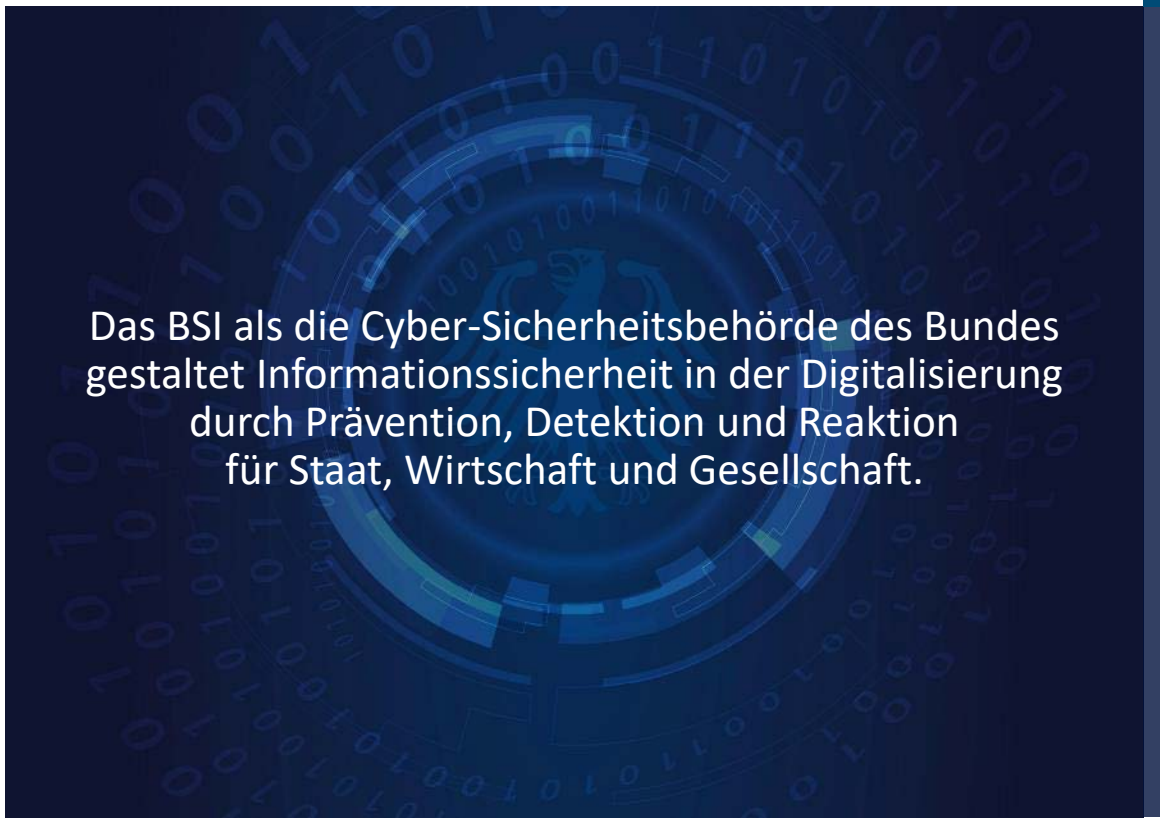
Steven Müller – TRR M.Sc. Dipl.-Ing.
Informationssicherheitsberatung für die Justiz
Referat BL13 Informationssicherheitsberatung Standort Sachsen

steven.mueller@bsi.bund.de

sicherheitsberatung-justiz@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Twitter: **@BSI_Bund @certbund**



Bundesamt
für Sicherheit in der
Informationstechnik