Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Ist ein Cloud Service sicher?

OMNISECURE 2024
22.01. bis 24.01.2024 in Berlin

Ist ein Cloud Service sicher? Beurteilung aus Verwaltungssicht

Christoph Pfeifer, BSI Referat TK 22 – Virtualisierung und Cloud-Sicherheit
OMNISECURE – Berlin 2024

Grundlagen

Was ist ein Cloud Service?
Sind (gleiche) Cloud Services wirklich vergleichbar?
Gibt es Gemeinsamkeiten?

Resultierende Folgen für die Beurteilung

Ein Cloud Service ist

- ein Angebot
- abhängig vom jeweiligen Anbieter

und deshalb

- immer individuell zu betrachten.

Dies macht ein Vergleich oder eine Beurteilung von Cloud Services schwierig – nicht nur in Bezug auf Sicherheit.

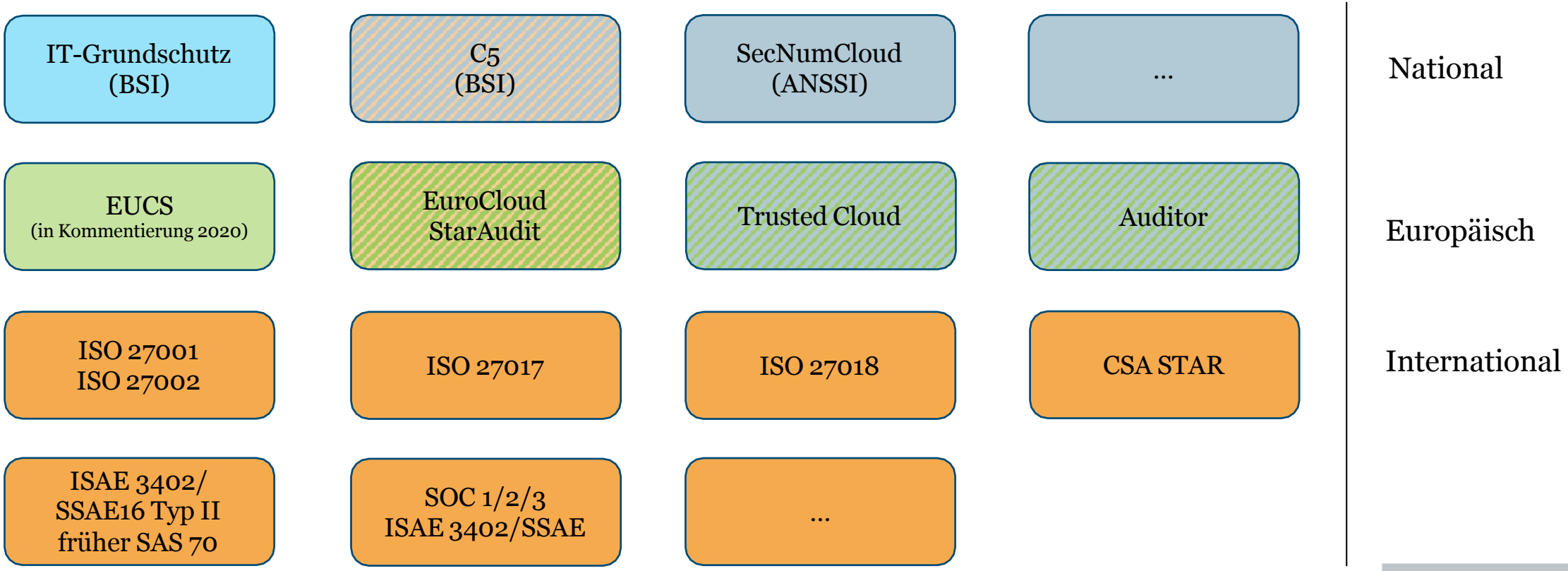
Mögliche Beurteilungsmethoden

Eine Beurteilung kann nur durch den Nutzer erfolgen.

Wie kann diese Beurteilung durchgeführt werden?

- eigener Fragenkatalog/Interview
- standardisierte Fragenkataloge/Schemata
- Auswertung von Berichten

Was für Standards gibt es am Markt für Cloud Services



Mehrere Farben: Ursprung des Standards, Erteilung des Zertifkats/Testats und Wirkungskreis auf unterschiedlichen Ebenen

Was ist bei diesen Standards generell zu beachten?

Auswahlkriterien	Beschreibung
Wirkungskreis, Reichweite	National, Europäisch, International
Kontext	Übergreifend, Fachspezifisch (Finanzwesen) oder Cloud spezifisch
Prüfer/Zertifizierer	Anbieter/neutrale/anerkannte Stelle
Durchführung, Methode	Dokumentenreview, Vor-Ort-Audit, Interview, Selbsterklärung
Inhalt, Abdeckung	Datenschutz, IT-Sicherheit, Betrieb, Infrastruktur, Implementierung, Interoperabilität, Anbieterprofil,…
Laufzeit, Gültigkeit	Aussage über Zukunft, Vergangenheit
Messgrößen	Latenz, SLA
Prüfobjekt	Cloud Service, Cloud-Anbieter, Cloud-Kunde
Konsequenzen	Haftung (grob fahrlässig, fahrlässig)

Auswahlkriterien: Quelle Buch „Cloud-Service-Zertifizierung“ von Sebastian Lins, Stephan Schneider und Ali Sunyaev ergänzt durch eigene Kriterien

Exkurs

- Was ist ein Zertifikat?
- Was ist ein Testat?

- Welche Auswirkungen haben diese beiden Nachweise für den Cloud Service Provider?

Welchen Weg hat die Bundesverwaltung gewählt?

Mindeststandard nach § 8 Absatz 1 Satz 1 BSIG

Mindeststandard zur Nutzung von externen Cloud-Diensten (aktuell Version 2.1 vom 15.12.2022)

Informationssicherheit entlang des gesamten Lebenszyklus (Planung, Beschaffung, Einsatz und Beendigung) und setzt auf IT-Grundschutz-Baustein OPS.2.2 Cloud-Nutzung auf

Verpflichtend: Erstellung einer Sicherheitsrichtlinie, die mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Cloud Computing Compliance Criteria Catalogue – C5 als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegt.

C5 im Überblick

- Cloud Computing Compliance Criteria Catalogue
- Erstveröffentlichung 2016, Aktualisierung 2020
- Sicherheitskriterien für Cloud-Dienste
- Transparenz durch Rahmenbedingungen
- Hilfestellung und Werkzeug
- Testat nach standardisierter Prüfung

Bilder: © BSI, sdecoret/Fotolia, cherries/Fotolia

Hintergrund zum C5

- Sicherheitskriterien anstatt konkrete Umsetzungsvorgaben
- Sicherheit des Service im Fokus anstatt ISMS
- Nutzung eines vorhandenen Prüfstandards (ISAE 3000)
- auswertbarer und auch vergleichbarer Bericht anstatt Zertifikat
  - Typ 1 – Umsetzung der Kontrollen zum Zeitpunkt
  - Typ 2 – Wirksamkeit der Kontrolle während des zu prüfenden Zeitraums

Struktur des C5

17 Domänen

121 Kriterien

- Basiskriterium
- Zusatzkriterium (optional)
- Ergänzende Informationen
  - *Zum Kriterium*
  - *Korrespondierende Kriterien für Kunden (optional)*
  - *Hinweise zur kontinuierlichen Prüfung*

Domänen des C5 (1/2)

1. Organisation der Informationssicherheit (OIS)
2. Sicherheitsrichtlinien und Arbeitsanweisungen (SP)
3. Personal (HR)
4. Asset Management (AM)
5. Physische Sicherheit (PS)
6. Regelbetrieb (OPS)
7. Identitäts- und Berechtigungsmanagement (IDM)
8. Kryptographie und Schlüsselmanagement (CRY)
9. Kommunikationssicherheit (COS)

Domänen des C5 (2/2)

10. Portabilität und Interoperabilität (PI)
11. Beschaffung, Entwicklung und Änderung von Informationssystemen (DEV)
12. Steuerung und Überwachung von Dienstleistern und Lieferanten (SSO)
13. Umgang mit Sicherheitsvorfällen (SIM)
14. Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)
15. Compliance (COM)
16. Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)
17. Produktsicherheit (PSS)

Exemplarisch ein Kriterium des C5

Domäne Physische Sicherheit (PS)

PS-02 Redundanzmodell

- Basiskriterium (2 Standorte, hinreichender Abstand, Betriebsredundanz)
- Zusatzkriterium (mehr als 2 Standorte, Georedundanz, zeitgleicher Ausfall von 2 Standorten möglich ohne Totalverlust)
- Korrespondierenden Kriterien für Kunden (Spiegelung von Redundanzmodell und Nachweise des Cloud-Anbieters mit den eigenen Anforderungen zur Verfügbarkeit und Verlässlichkeit des Cloud-Dienstes)

Fazit

- Bundesverwaltung hat mit dem C5 ein Werkzeug zur umfassenden Beurteilung von Cloud Services
- Cloud Services werden beurteilbar – passt dieser Cloud Service für mich als Nutzer mit meinen spezifischen Anforderungen
  (Hilfestellung: Auswerteleitfaden des BSI)
- Umsetzung und Wirksamkeit der Kontrollen wird geprüft
- shared responsibility wird berücksichtigt
- kein gesonderter Zertifizierungsprozess
- C5 ist auch außerhalb der Verwaltung bekannt und wird als Maßstab zur Beurteilung auch von Nutzern außerhalb der Verwaltung herangezogen

Vielen Dank
für Ihre Aufmerksamkeit!

Danke für Ihr Interesse

Deutschland
Digital•Sicher•BSI•

Kontakt

Christoph Pfeifer
Referat TK 22, Cloudsicherheit und Virtualisierung
Christoph.Pfeifer@bsi.bund.de
cloudsecurity@bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Quellen

- IT-Grundschutz-Baustein OPS.2.2 Cloud-Nutzung
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2021.pdf?__blob=publicationFile&v=2
- Mindeststandard zur Nutzung von externen Cloud-Diensten
  https://www.bsi.bund.de/dok/MST-Cloud
- C5
  https://www.bsi.bund.de/dok/7685384 und https://www.bsi.bund.de/dok/13368652
- Auswerteleitfaden zum C5
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/Auswertung/Auswertung_node.html