Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Veranstaltung der GI - Fachgruppe SECMGT
Cloud Sicherheit
Sichere Nutzung von Cloud-Diensten

Marion Demand, Referat TK 22, BSI
28.05.2021

Inhalt

1. Cloud Sicherheit
2. Cloud (Security) Standards
3. Cloud Computing Compliance Criteria Catalogue (C5) des BSI
4. Fazit

Cloud Sicherheit

Cloud Sicherheit

Muss ich mich nicht mehr ums IT-Sicherheit und Datenschutz kümmern,
wenn ich meine Daten in die Cloud lege?

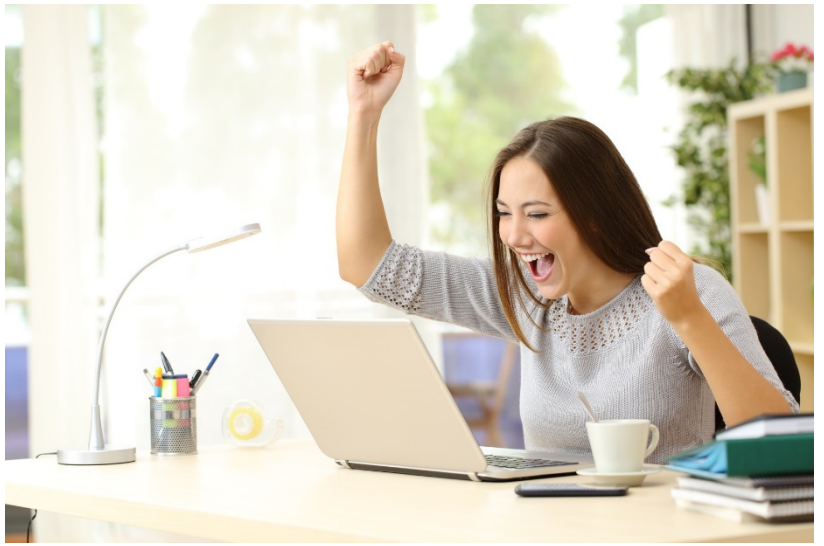


Bild: © AntonioGuillem/ Fotolia

Cloud Sicherheit

Doch, das muss ich weiterhin.
Aber ich teile mir die Verantwortung mit dem Cloud-Anbieter

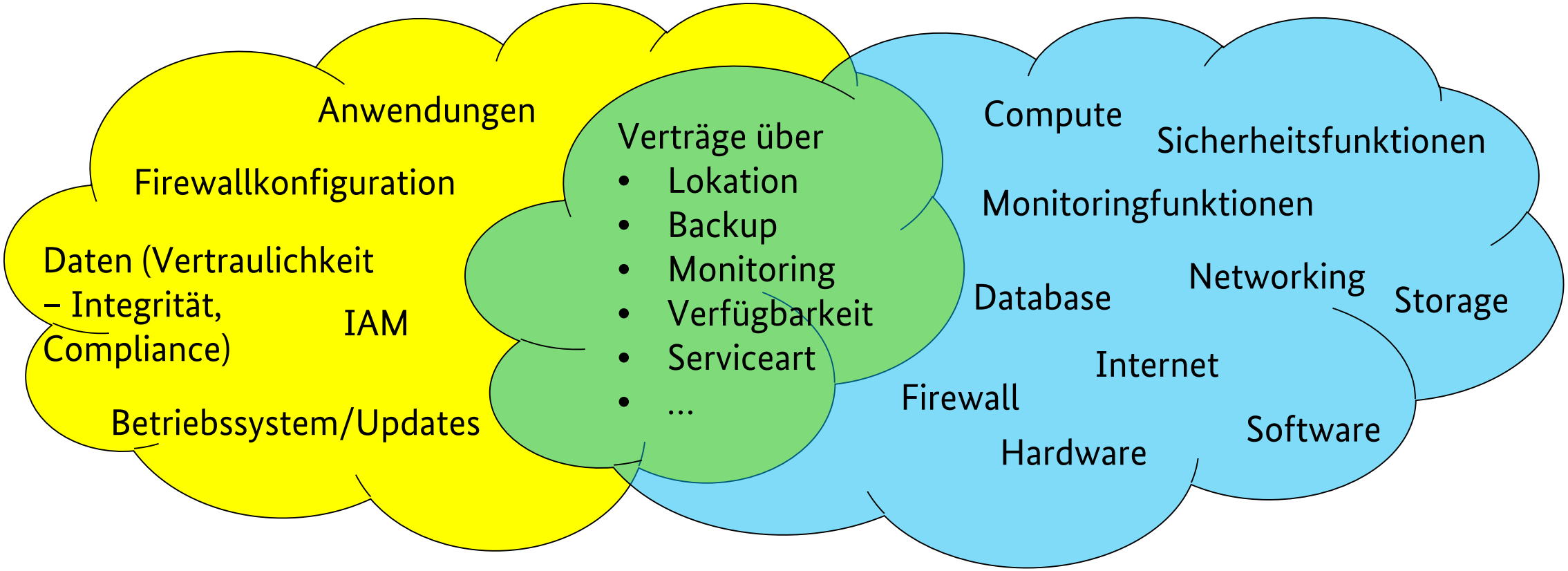
Stichwort: Shared Responsibility

Bild: © Rawpixel.com / Fotolia

Shared Responsibility

Kunde
Sicherheit in der Cloud

Cloud-Dienstanbieter
Sicherheit von der Cloud



<- Abhängig vom gebuchten Dienst verschieben sich Verantwortlichkeiten ->

Cloud Sicherheit

Aber wie kann ich als Kunde sicher sein, dass meine Daten in der Cloud wirklich sicher sind?

Bild: © GoodLuz/ Fotolia

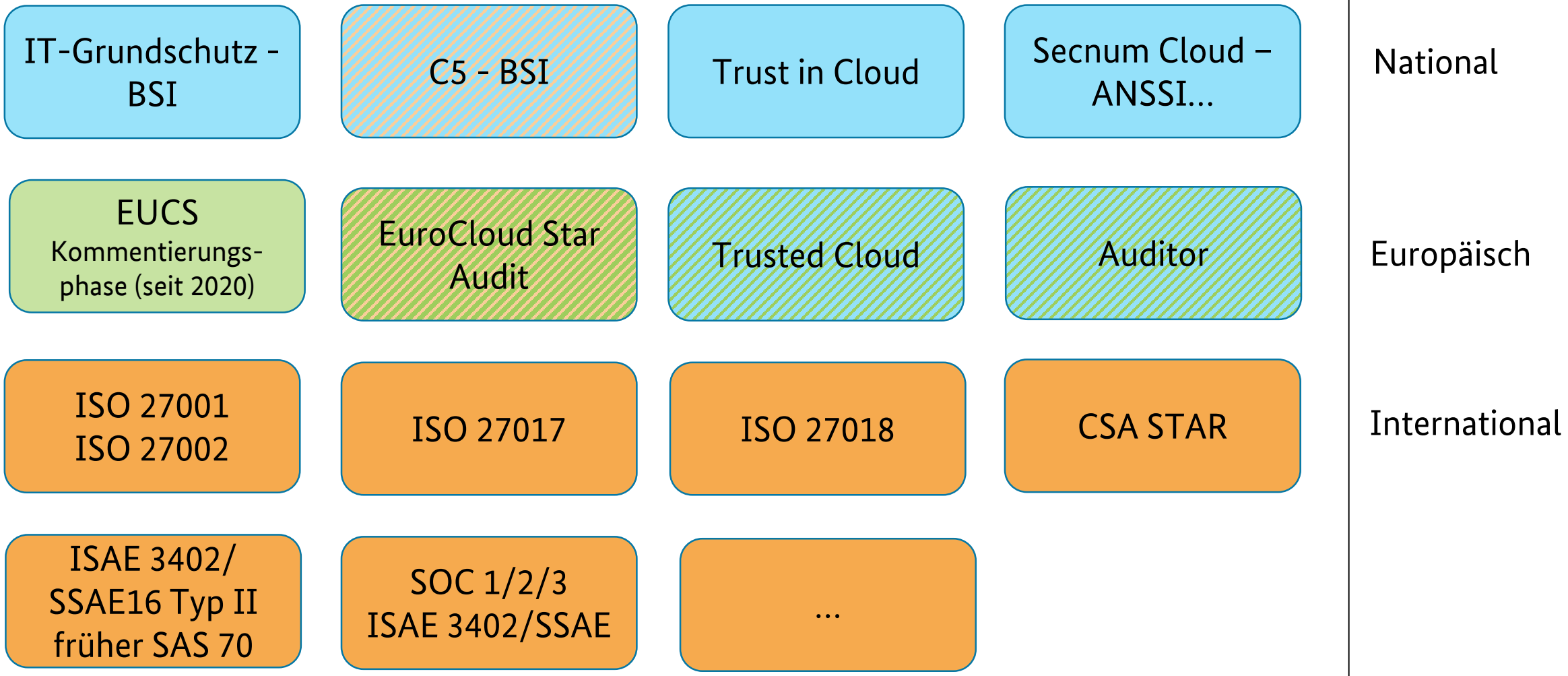
Cloud Sicherheit

Hundertprozentige Sicherheit gibt es nicht!
Aber der Cloud-Anbieter kann nachweisen, dass er sich beim Aufbau und Betrieb seiner Dienste an vereinbarte Kriterien hält.

Bild: © Coloures-pic/ Fotolia

Cloud (Security) Standards im Überblick

Standards für Cloud-Dienste im Überblick



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

Cloud Standards

Das sind ganz schön viele, welcher ist der Beste?

Bild: © gpointstudio/ Fotolia

Cloud Standards

Das kommt auf den Kontext an

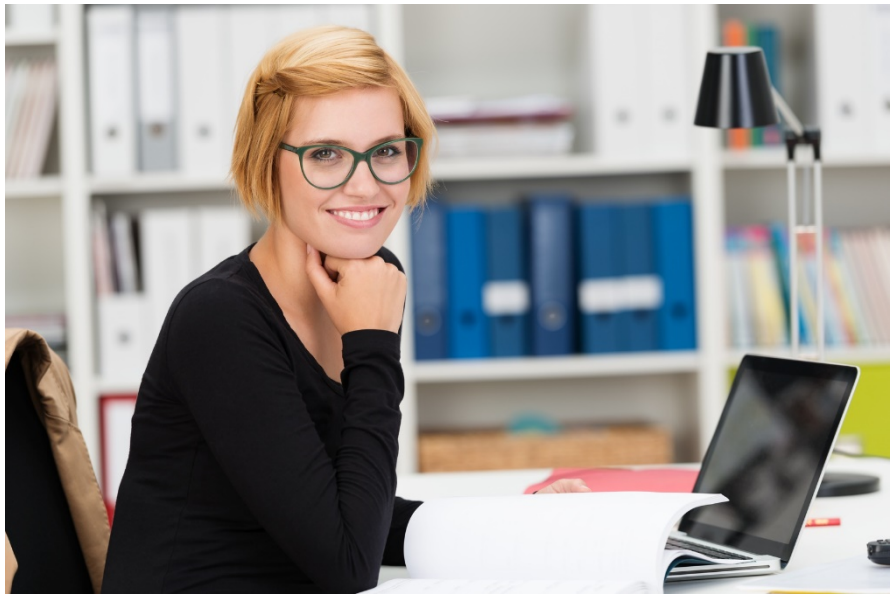


Bild: © contrastwerkstatt / Fotolia

Worauf kann ich achten?

Auswahlkriterien	Beschreibung
Wirkungskreis, Reichweite	National, Europäisch, International
Kontext	Übergreifend, Fachspezifisch (Finanzwesen) oder Cloud spezifisch
Prüfer/Zertifizierer	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, SLAS
Prüfobjekt	Cloud-Service, Cloud-Experte, Cloud-Partner
Konsequenzen	Haftung (grob fahrlässig, fahrlässig)

Auswahlkriterien: eigene + Buch Cloud-Service-Zertifizierung von Sebastian Lins, Stephan Schneider und Ali Sunyaev

Cloud Computing Compliance Criteria Catalogue (C5)
BSI

C5 im Überblick

- 1. Version Frühjahr 2016, Update Januar 2020
- Umfassende Sicherheitskriterien für Cloud-Dienste
- Prüfung durch Wirtschaftsprüfer nach Prüfstandard (ISAE 3000)
- Bericht zeigt Kunden,
  - Wie setzt der CSP (Cloud Service Provider) den C5 um?
  - Wie wurde das geprüft?
  - Was ist das Ergebnis (pro Kontrolle des CSP)?
- Vergleichbarkeit von gleichwertigen Diensten am Markt
- Alle großen Anbieter haben C5 Testat für mindestens einen Dienst

Struktur des C5

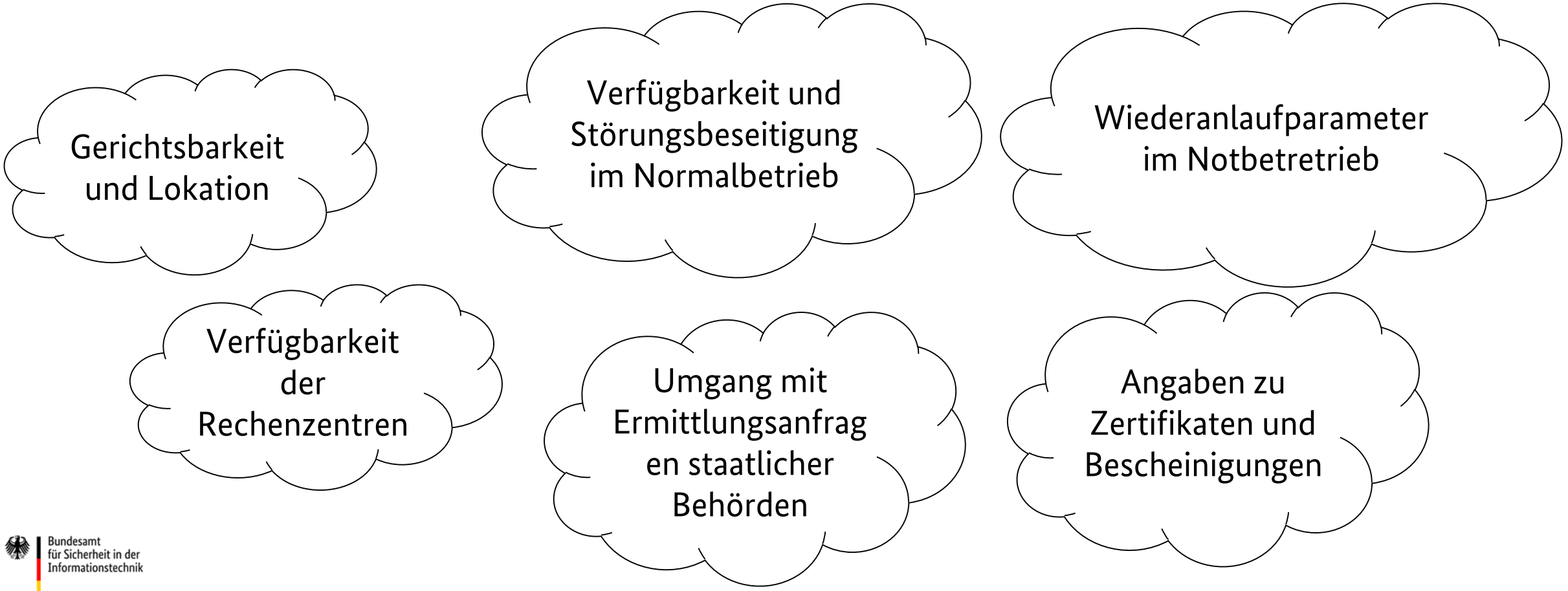
17 Bereiche

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

Bild: © JakubJirsak/ Fotolia

Mitprüfung von Rahmenbedingungen

- zusätzliche Information für Kunden
- Beurteilung der anwendungsfallspezifischen Eignung eines Cloud-Dienstes



Bereiche des C5

- 01 Organisation der Informationssicherheit (OIS)
- ..
- 06 Regelbetrieb (OPS)
- 07 Identitäts- und Berechtigungsmanagement (IDM)
- 08 Kryptographie und Schlüsselmanagement (CRY)
- 09 Kommunikationssicherheit (COS)
- ..
- 14 Kontinuität des Geschäftsbetriebs und Notfallmanagement (BCM)
- 15 Compliance (COM)
- 16 Umgang mit Ermittlungsanfragen staatlicher Stellen (INQ)
- 17 Produktsicherheit (PSS)

Kriterien des C5

z.B. aus der 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-Dienste

Bild: © Nmedia/ Fotolia

6. Fazit

Fazit

- Vorbereitungszeit für Planung einkalkulieren
- Eigene Pflichten berücksichtigen
- Anforderungen unter Berücksichtigung von Compliance definieren
- Passendsten Anbieter heraussuchen (Zertifikate, Testate)
- Vertrag entsprechend der Pflichten definieren
- Shared Responsibility leben

Bild: © ArturDebat/ Getty Images

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Marion Demand
Referat TK 22, Cloudsicherheit und Virtualisierung
Marion.demand@bsi.bund.de
cloudsecurity@bsi.bund.de
Tel. +49 (0) 228 9582 5250
Fax +49 (0) 228 10 9582 5250

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

Bundesamt
für Sicherheit in der
Informationstechnik

Links

- Der C5 auf Deutsch: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2
- Die C5 Kriterien als Excel-Datei: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020_Editierbar.xlsx?__blob=publicationFile&v=3
- Auswerteleitfaden: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020_Auswertungsleitfaden.xlsx?__blob=publicationFile&v=1
- Kreuzreferenztabelle (zu anderen Standards): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020_Referenztabelle.xlsx?__blob=publicationFile&v=4
- Neuerungen gegenüber C5:2016: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_Neuerungen_node.html
- Englische Seiten: https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/C5_NewRelease/C5_NewRelease_node.html
- Grundschutzbaustein https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2020.pdf

Exemplarische Anwendung Auswahlkriterien Standards

Auswahlkriterien	Trust in Cloud	C5	Auditor
Wirkungskreis, Reichweite	Deutschland	Deutschland erstellt, Reichweite: international	Deutschland erstellt, Reichweite: europäisch
Kontext	Cloud spezifisch	Cloud spezifisch	Datenschutz
Prüfer/ Zertifizierer	Cloud-Ecosystem	Wirtschaftsprüfer	Prüfstellen, akkreditierte Zertifizierungsstellen
Durchführung, Methode	Selbsterklärung (30 Fragen), Dokumentenreview	Dokumentenreview, Vor-Ort-Audit	Dokumentenreview, Vor-Ort-Audit,
Inhalt, Abdeckung	Referenzen, nationale Vorgaben	IT-Sicherheit, Interoperabilität, Implementierung	Datenschutz
Laufzeit, Gültigkeit	12 Monate, Zukunft	12 Monate, Vergangenheit	36 Monate
Prüfobjekt	Cloud-Service, Anbieter	Cloud-Service	Cloud-Service
Konsequenzen	Haftung für Fehler in Aussagen liegt beim Anbieter	Haftung für Fehler in Aussagen liegt beim Prüfer	Haftung für Fehler in Aussagen liegt beim Prüfer

Quelle: öffentliche Informationen der Anbieter

C5 Bericht

- Prüfbericht des unabhängigen Wirtschaftsprüfers
  - Auftrag, C5 Version, Prüfumfang
  - Verantwortung Cloudanbieter/Wirtschaftsprüfer
  - Unabhängigkeitsbescheinigung Wirtschaftsprüfer/Qualitätsnachweis
  - Grenzen von Kontrollen (Subunternehmer Kontrollen sind beschrieben aber nicht Vor-Ort geprüft)
  - Prüfurteil
  - Adressat
- Erklärung Cloud Anbieter (gesetzlicher Vertreter)
- Systembeschreibung
- Darstellung der Kriterien/Kontrollen mit Prüfhandlung und Ergebnis
- Sonstiges

Bild: © squaredpixels/ Getty Images

C5 Bericht - Systembeschreibung

- Name, Art und Umfang des Dienstes
- Beschreibung Systemkomponenten
- Angaben zu Rahmenbedingungen (Folie 20)
- Anwendbare C5-Kriterien
- Kontrollen (Grundsätze, Verfahren und Maßnahmen) bezogen auf die anwendbaren C5-Kriterien
- Umgang mit Sicherheitsvorfällen
- Korrespondierende Kontrollen beim Kunden (ggf. wie der Kunde darauf aufmerksam gemacht wird)
- An Subdienstleister ausgelagerte Funktionen

Für Typ 2 zusätzlich

- Was wurde im Prüfzeitraum in Bezug auf die anwendbaren Kriterien an Kontrollen geändert
- Auftreten von Sicherheitsvorfällen im Zeitraum und wie wurde diesen begegnet

Bild: © squaredpixels/ Getty Images