Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Sichere Nutzung von Cloud-Diensten mit dem BSI C5

Wie geht die Bundesverwaltung hier vor?

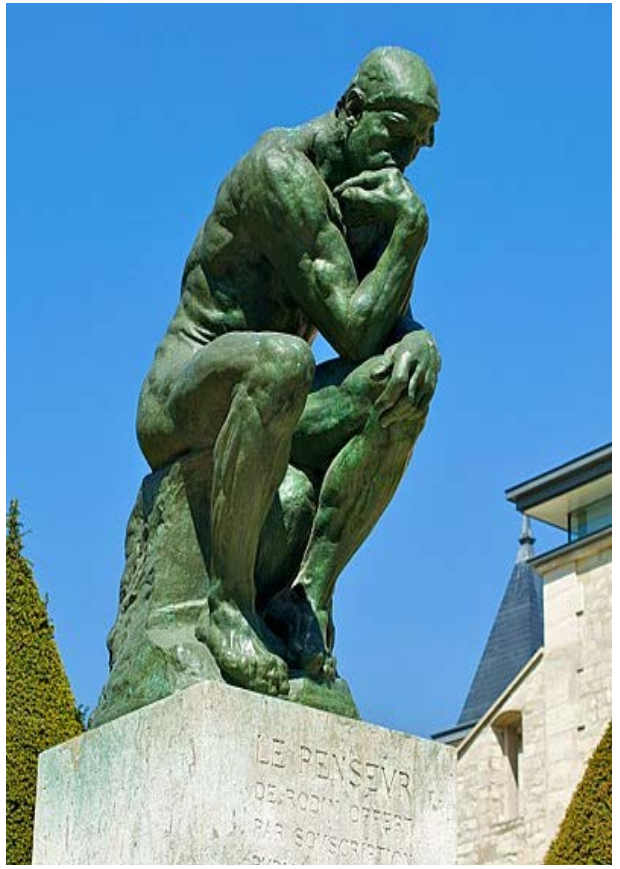
Dr. Patrick Grete, Referat TK 22, BSI, ISACA Fokus Event Bonn,
03.11.2022

1. Das BSI
2. Wie geht man vor, um Cloud-Dienste sicher zu nutzen? (Was ist (un)sicher genug?
3. Allgemeines Vorgehen
4. Vorgehen in der Bundesverwaltung
5. Zentraler Baustein: Der Cloud Computing Compliance Criteria Catalogue – C5
   - Hintergrund
   - Erfolgsgeschichte des C5
   - Aufbau eines C5 Berichts
   - Auswertung eines C5 Berichts
6. Fazit
7. Fragen und Antworten

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft

Was ist Cloud?
Und was gibt es für ein Problem damit?

- Cloud bezeichnet das an dem eigenen Bedarf angepasste Nutzen von standardisierten Diensten über standardisierte Schnittstellen eines Netzes.
- Beispiel: Online-Speicher über den Browser (oder App, die die Browserschnittstelle nutzt)
- Gegenbeispiel: Ein RZ nimmt Ihre Server-Hardware zum Betrieb auf
- Gegen-Gegenbeispiel: Sie mieten Serverdienste und schieben die bisherigen Server-Anwendungen auf diese gemieteten Dienste
- Herausforderungen:
  - Daten werden ausgelagert (Datenschutz, Verfügbarkeit)
  - Das Netz wird zur kritischen IT-Ressource
  - Abhängigkeit vom Anbieter
  - Geteilte Verantwortung oder organisierte Verantwortungslosigkeit?
  - Nutzungsbedingungen sind unbekannt oder werden nicht eingehalten
  - Werden die eigenen Vorgaben durch den Cloud-Dienst eingehalten?
  - Habe ich selbst die nötige Kompetenz, die Cloud sicher zu nutzen?



Allgemeine Vorbereitungen

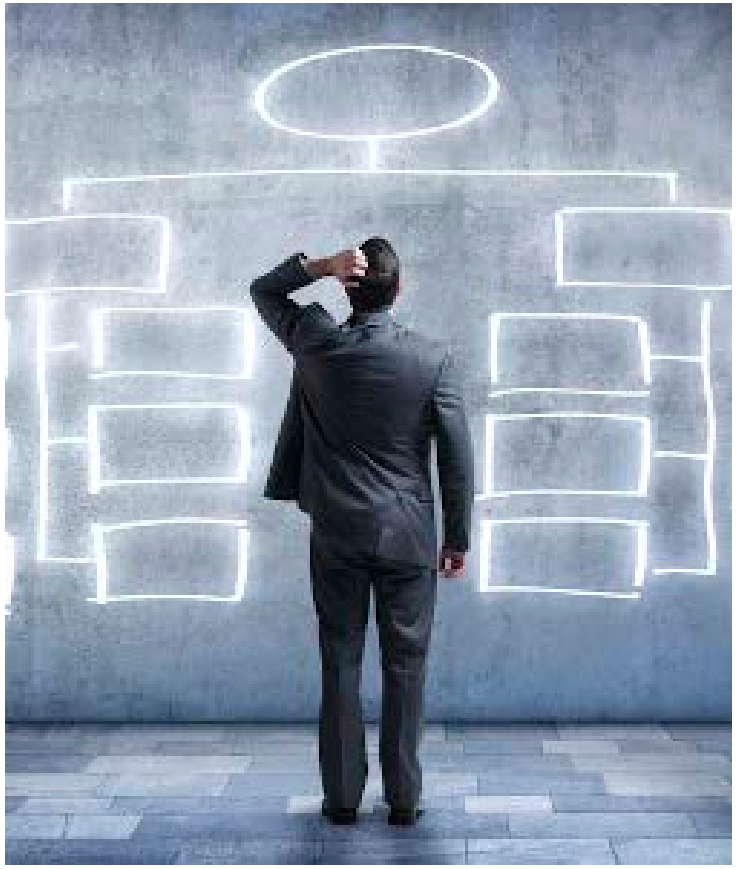
- Beantwortung der folgenden Fragen:
  - Was für Daten sollen in der Cloud verarbeitet werden? (Offene Daten, personenbezogene Daten, besondere Personenbezogene Daten, andere sensitive Daten)
  - Welche Rahmenbedingungen/Regulierungen gelten für diese Daten?
  - Sind die technischen und organisatorischen Voraussetzungen für die Cloud-Nutzung gegeben (Endgeräte, Internetverbindung)
- Durchführung einer Risiko-Analyse für den jeweiligen Anwendungsfall
  - Welche Risiken entstehen, wenn diese Art von Daten, im gegebenen Anwendungsfall, mit den Endgeräten, durch die jeweiligen Personen, über die bestehende Netzverbindung, verarbeitet werden?

Vor Beginn der Cloud-Nutzung

- Diese Risiken führen zu verschiedenen Fragen, die auf den ersten Blick, nicht leicht zu beantworten sind:
  - Bietet der infrage stehende Cloud-Dienst **nachweislich** die benötigte Leistung?
  - Verfügt der Cloud-Dienst nachweislich über **ausreichende** Sicherheit?
  - Was müssen Sie als Anwender zur Sicherheit beitragen?

- Aus Überforderung (oder zeitlichem oder finanziellen) Druck kann vorher oder spätestens jetzt „Planlose Cloud-Nutzung“ entstehen.

- Präferierte Methode des BSI: Nutzen Sie den Cloud Computing Compliance Criteria Catalogue (C5) des BSI



Wie verfährt die Bundesverwaltung bei der Cloud-Nutzung?

Behörden haben ein ISMS nach IT-Grundschutz

Baustein OPS 2.2 Cloud-Nutzung
(gute Inspiration für ISO 27001 native ISMSe)

Bundesbehörden folgen dem Mindeststandard des BSI „Nutzung externer Cloud-Dienste“

- Konkretisiert & Erweitert die **Anforderungen an Behörden bei Cloud-Nutzung**
- Betrifft Informationssicherheit bei **Marktsichtung**, **Beschaffung**, **Nutzung** und **Beendigung** der Cloud-Nutzung (Strategie, Risikoanalyse, Einbindung ins ISMS, Rückgabe der Daten)
- Fordert von Behörde, Cloud-Dienste zu beschaffen, die ein **C5 Testat** aufweisen
- Behörde muss Cloud-Dienst sicher nutzen (**korrespondierende Kontrollen**) und Leistungsfähigkeit nachprüfen

Neu: EVB-IT Cloud

- **Ergänzende Vertragsbestandteile IT zum Thema Cloud**, verpflichtend gemäß Bundeshaushaltsordnung (BHO) und Landeshaushaltsordnungen (LHO)
- Wichtig für den **Beschaffer** bei der Behörde und dem **Vertrieb** beim Cloud-Anbieter

➔ Artikel BSI-Magazin 2022/01

Was ist der C5?

C5 im Überblick

- C5 (Cloud Computing Compliance Criteria Catalogue)
- erstmalige Veröffentlichung des C5 Frühjahr 2016
- aktualisierte Fassung (C5:2020) Januar 2020
- umfassende Sammlung von Sicherheitskriterien für Cloud-Dienste
- Nutzer kann mit dem C5-Bericht anhand folgender Inhalte beurteilen, ob der Dienst seinen (eigenen) Sicherheitsanforderungen genügt:
  - Wie setzt der CSP (Cloud Service Provider) den C5 um?
  - Wie wurde das geprüft?
  - Was ist das Ergebnis (pro Kontrolle des CSP)?
- Standardisierte Kriterien, Prüfungen und Berichte ermöglichen die Vergleichbarkeit von Angeboten (Diensten) am Markt
- Prüfberichte von unabhängigen Dritten schaffen höheres Vertrauen beim Nutzer

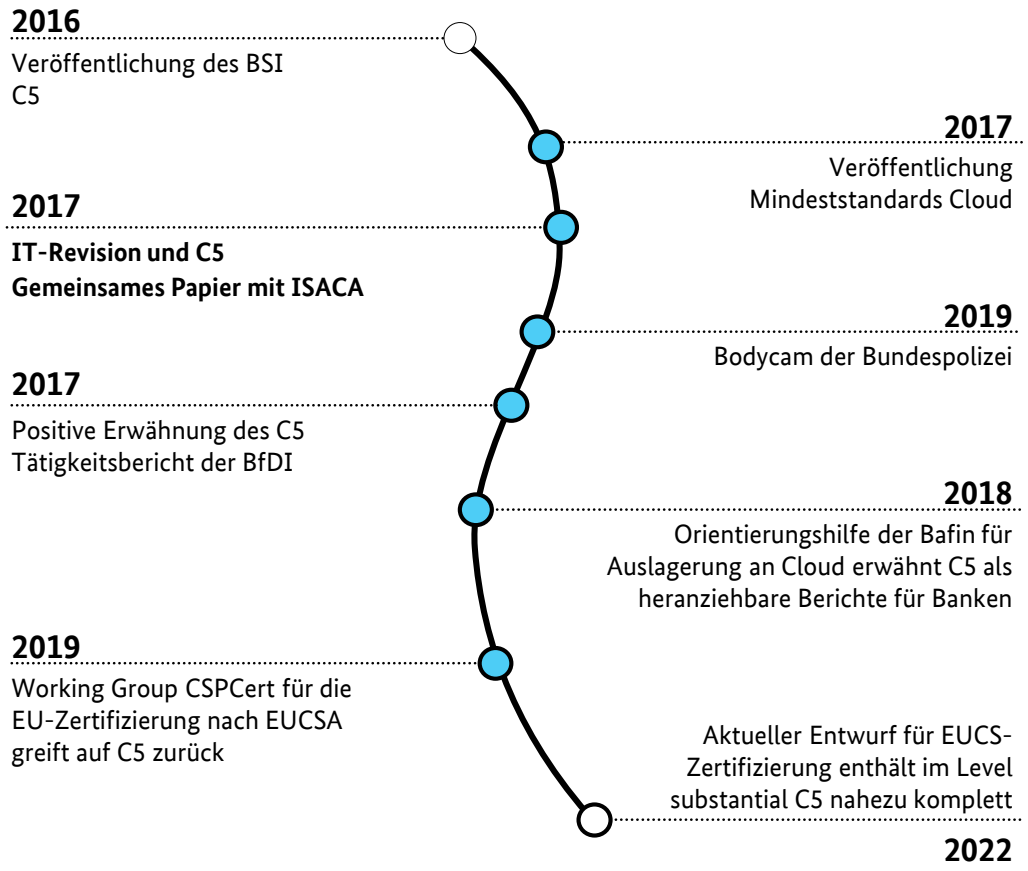
Bilder: © BSI, sdecoret/Fotolia, cherries/Fotolia

Hintergrund zum C5

- Neuer Weg:
  - Sicherheitskriterien vorgeben NICHT deren konkrete Umsetzung (was und nicht wie)
  - Fokus auf die Sicherheit des Services NICHT nur auf das ISMS
  - Verwendung eines existierenden Prüfstandard (ISAE 3000) und deren danach arbeitenden Prüfer (Wirtschaftsprüfer)
  - audit once - certify many Prinzip um auch die Akzeptanz bei den Anbietern sicherzustellen
  - Keine neue/weitere Zertifizierungsstelle SONDERN Bewährung am Markt
- Warum?
  - Sicherheit des Cloud-Services ist wichtig für Kunden
  - Gebraucht wurde ein Prüfbericht über alle Anforderungen, damit deren Umsetzung vergleichbar bewertet werden können, NICHT nur ein Stempel
- Vorteil für die Vertragsgestaltung (Nutzer – CSP)
  - Aufnahme von Sicherheitskriterien über verpflichtende Einhaltung des C5-Testats (Anforderungen und Prüfaussagen werden damit verbindlicher Vertragsgegenstand)

Erfolgsgeschichte des C5

Öffentlichkeitswirksame Umsetzung



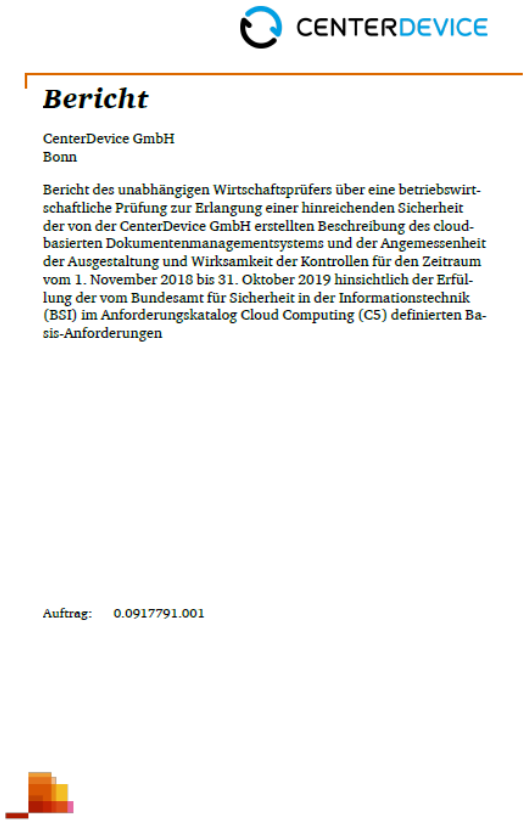
Cloud-Anbieter mit C5 (Auswahl)

Alibaba Cloud, DRACOON, box, CISCO, MINDBREEZE, amazon web services, GENESYS, plusserver, Fabasoft, CENTERDEVICE, ARIBA, Tencent Cloud, HUAWEI, salesforce, KINAXIS, Google Cloud Platform, NETFILES, CANCOM Pironet, FUJITSU, success factors, evoila, LogMeIn Be Limitless., Microsoft Azure, CLOUDFLARE, netskope, everbridge, Fieldglass, paloalto NETWORKS, servicenow, CLOUD1X, ORACLE, RingCentral, CloudFerro, OVHcloud, SAP S/4 HANA, T-Systems, SOFTLAYER an IBM Company, SAP Business ByDesign, SAP Cloud Platform, Dropbox

Aufbau eines C5-Berichts

- Deckblatt
- Bescheinigung des Prüfers (Was war der Auftrag? Prüfurteil (Testat))
- Erklärung der gesetzlichen Vertreter (rechtsverbindliche Aussagen)
- Systembeschreibung des Cloud-Dienstes
  - Rahmenbedingungen, Sub-Dienstleister
- Abbildung von Maßnahmen des Cloud-Dienstes zu C5 Kriterien
- Korrespondierende Kontrollen (Was hat der Kunde zu tun?)
- Prüfungsdetails (WAS wurde WIE mit WELCHEM Ergebnis geprüft?)
- Sonstige Informationen

- Aussagenmechanik: Der Prüfer bescheinigt, dass die Sicherheitsmaßnahmen im beschriebenen System, anhand der dargelegten Prüfungshandlung über den angegebenen Zeitraum wirksam waren, falls die Kunden Ihre Pflichten eingehalten haben.


CENTERDEVICE

Bericht

CenterDevice GmbH
Bonn

Bericht des unabhängigen Wirtschaftsprüfers über eine betriebswirtschaftliche Prüfung zur Erlangung einer hinreichenden Sicherheit der von der CenterDevice GmbH erstellten Beschreibung des cloud-basierten Dokumentenmanagementsystems und der Angemessenheit der Ausgestaltung und Wirksamkeit der Kontrollen für den Zeitraum vom 1. November 2018 bis 31. Oktober 2019 hinsichtlich der Erfüllung der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im Anforderungskatalog Cloud Computing (C5) definierten Basis-Anforderungen

Auftrag: 0.0917791.001

Wie die C5 Kriterien funktionieren (1/2)

Bundesamt
für Sicherheit in der
Informationstechnik

OPS-08 Datensicherung und Wiederherstellung – Regelmäßige Tests

Basiskriterium

Wiederherstellungsverfahren werden vom Cloud-Anbieter regelmäßig, mindestens jährlich, getestet. Die Tests erlauben eine Beurteilung darüber, ob die vertraglichen Vereinbarungen sowie die Vorgaben zur maximal tolerierbarer Ausfallzeit (Recovery Time Objective, RTO) und zum maximal zulässigem Datenverlust (Recovery Point Objective, RPO) eingehalten werden (vgl. BCM-02).

Abweichungen von den Vorgaben werden an das dafür zuständige Personal oder die dafür zuständigen Systemkomponenten beim Cloud-Anbieter berichtet, damit diese die Abweichungen umgehend beurteilen und erforderliche Maßnahmen einleiten können.

Kontrolle eines Mandanten zum Erfüllen des Kriteriums OPS-08

ABC GmbH führt eine wöchentliche, vollautomatische Prüfung der Wiederherstellungsverfahren inklusive einem Funktionstest der Daten basierend auf dem letzten Backup durch.
Jede Wiederherstellungsprüfung wird vollautomatisch überwacht und protokolliert. Bei Abweichungen werden DevOps-Bevollmächtigte alarmiert, führen eine anschließende manuelle Prüfung durch und leiten ggf. Maßnahmen zur Fehlerbehebung ein.

Wie die C5 Kriterien funktionieren (2/2)

Kontrolle eines Mandanten zum Erfüllen des Kriteriums OPS-08

ABC GmbH führt eine wöchentliche, vollautomatische Prüfung der Wiederherstellungsverfahren inklusive einem Funktionstest der Daten basierend auf dem letzten Backup durch.
Jede Wiederherstellungsprüfung wird vollautomatisch überwacht und protokolliert. Bei Abweichungen werden DevOps-Bevollmächtigte alarmiert, führen eine anschließende manuelle Prüfung durch und leiten ggf. Maßnahmen zur Fehlerbehebung ein.

Prüfungshandlungen zum Beurteilen der Angemessenheit und Wirksamkeit der Kontrolle

Befragung eines DevOps-Bevollmächtigen über die regelmäßige Prüfung der Wiederherstellungsverfahren sowie deren Überwachung.

Durchsicht der Konfiguration zum Erzeugen der für den Funktionstest genutzten virtuellen Maschine sowie der im Telemetrie-Überwachungssystem definierten Regeln zum Überwachen des Funktionstests und Alarmieren der DevOps-Bevollmächtigten.

Durchsicht der Aufzeichnungen zu einer Stichprobe von Alarmen des Telemetrie-Überwachungssystems zu Funktionstests im Prüfungszeitraum, um die sachgerechte Nachbearbeitung der Alarme durch das DevOps Team zu beurteilen.

Angeforderte Nachweise

<u>Angemessenheit:</u>

- Konfiguration der Auto Scaling Group auf wöchentliche Erzeugung der VMs
- Ausgestaltung der Metriken im Telemetrie-Überwachungssystem

<u>Wirksamkeit:</u>

- Nachweise über etwaige Änderungen an der Konfiguration im Prüfungszeitraum
- Protokollierungsdaten (Log) aus Telemetrie-Überwachungssystem für den Prüfungs-zeitraum, ob Test wöchentlich durchgeführt wurde und welche Abweichungen dabei aufgetreten sind, einschl. Nachweis der Vollständigkeit des Logs.
- Für Stichprobe von Abweichungen: Tickets/sonst. Aufzeichnungen über deren Behandlung durch DevOps-Bevollmächtigte

Wie wird eine Auswertung dokumentiert?

- Ein Excelbasierter Auswerteleitfaden wurde erstellt
  - Führt strukturiert durch einen Bericht
  - Informationen zu Umfeldparametern/Rahmenparametern werden aufgenommen
  - Geprüfte Kontrollen, Prüfungshandlungen und Abweichungen können dokumentiert werden
  - Korrespondierende Kontrollen werden aufgenommen und können für den eigenen Anwendungsfall (mit dem ISB) konkretisiert werden.
    - **Guter Ansatz für Innenrevision**
  - Gegencheck mit korrespondierenden Kriterien (ab C5:2020)
  - Erstaufwand ist hoch. Wiederverwendung (andere Abteilungen) und Weiterverwendung (neue Berichte) ist leicht möglich (Skalierbarer Aufwand)
  - Führt zu guter Aktenlage → **Gute Grundlage für Innenrevision**

4. Fazit

Fazit

- Die Herausforderungen der Cyber-Sicherheit wurden und werden durch den C5 adressiert.
- Der C5 ist
  - Geeignete Basis für das Sicherheitsniveau des Cloud-Dienstes
  - Nachweis der Cloud-Sicherheit für Kunden
  - Katalysator für Aushandlung der Sicherheitseigenschaften
  - Mit den korrespondierenden Kriterien noch besserer Katalysator für die gemeinsame Verantwortung für die Sicherheit
  - Lässt sich gut und wiederverwertbar auswerten
  - Ist (nicht nur) für Revision eine gute Grundlage

Bild: © ArturDebat/ Getty Images

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/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/C5_AktuelleVersion/C5_Auswertung_node.html
- 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/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/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

Vielen Dank
für Ihre Aufmerksamkeit! Fragen?

Kontakt

Dr. Patrick Grete
Referat TK 22, Cloudsicherheit und Virtualisierung

patrick.grete@bsi.bund.de
Tel. +49 (0) 228 9582 5932
Fax +49 (0) 228 10 9582 5932

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