Bundesamt
für Sicherheit in der
Informationstechnik

C5:2020: SaaS-Fallstudie

Anwendung des Community Draft C5:2020 bei SaaS-Anbietern ohne eigene Infrastruktur im Vergleich zu C5:2016

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-6666

E-Mail: cloudsecurity@bsi.bund.de
Internet: https://www.bsi.bund.de/C5
© Bundesamt für Sicherheit in der Informationstechnik 2020

Inhaltsverzeichnis

1 Ausgangssituation ... 3
2 Zielsetzung und Methodik ... 4
3 Ergebnisse ... 6
4 Fazit ... 8

1 Ausgangssituation

Als Cyber-Sicherheitsbehörde des Bundes verfolgt das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Ziel der präventiven Förderung der Informations- und Cyber-Sicherheit in Staat, Wirtschaft und Gesellschaft, um den sicheren Einsatz von Informations- und Kommunikationstechnik voranzutreiben. Informationssicherheit ist die Voraussetzung einer erfolgreichen Digitalisierung, die nur gelingen kann, wenn Anwender Vertrauen in (neue) Technologien entwickeln und diese sicher einsetzen.

Im Jahr 2016 ist das BSI dem Bedürfnis nach objektiven Prüfkriterien und Mindestanforderungen mit Veröffentlichung eines Anforderungskatalogs für die Bewertung der Informationssicherheit von Cloud-Diensten („*Cloud Computing Compliance Controls Catalogue", C5:2016*) nachgekommen. Seitdem hat das BSI Anfragen von Cloud-Anbietern, -Kunden und -Prüfern erhalten aus denen, zusammen mit der allgemeinen technischen Entwicklung, der Bedarf für die Überarbeitung des C5:2016 ersichtlich wurde.

Hierfür ist das BSI mit Anbietern, Nutzern, Prüfern und Regulatoren in einen gezielten Dialog getreten, um den Entwicklungen im jeweiligen Umfeld Rechnung zu tragen. Die neue Version C5:2020 ist das Ergebnis dieses Prozesses. Einige wesentliche Änderungen im Vergleich zum C5:2016 sind:

- Aktualisierung der Kriterien[1] hinsichtlich neuer Konzepte, z. B. „DevOps", also dem Zusammenwachsen von Entwicklung und Betrieb von IT-Systemen;
- Erweiterung der Kriterien an den Cloud-Dienst selbst und nicht nur an die Bereitstellung des Cloud-Dienstes, um die Anforderungen des EU Cybersecurity Acts abzubilden;
- Erweiterung der Kriterien zur Bereitstellung der Cloud-Dienste um Aspekte im Umgang des Cloud-Anbieters mit Ermittlungsanfragen staatlicher Stellen;
- Aufnahme korrespondierender Kriterien für Cloud-Kunden, die zeigen, an welchen Stellen eigene Maßnahmen etabliert werden müssen, um die Sicherheit des Cloud-Dienstes zu gewährleisten;
- Aufnahme ergänzender Hinweise und Informationen zum besseren Verständnis der Kriterien sowie zu deren kontinuierlicher Prüfung;
- Ergänzung des bisherigen Prüfungsverfahrens um die Möglichkeit einer direkten IT-Prüfung.

Der überarbeitete Kriterienkatalog (C5:2020) enthält 29 neue Basiskriterien sowie drei neue Transparenzkriterien zu den Rahmenbedingungen des Cloud-Dienstes[2]. Diese erweitern bestehende Bereiche (z. B. Asset Management, Physische Sicherheit, Regelbetrieb, Identitäts- und Berechtigungsmanagement, Kommunikationssicherheit, Steuerung und Überwachung von Dienstleistern und Lieferanten) und definieren zwei

1 Im überarbeiteten C5 ist von Basiskriterien, nicht mehr von Basisanforderungen, die Rede.
2 Im C5:2016 auch als „Umfeldparameter" bezeichnet.

neue Bereiche (Produktsicherheit und Umgang mit Ermittlungsanfragen staatlicher Stellen). Das BSI hat den überarbeiteten Kriterienkatalog im Oktober 2019 als „Community Draft“ zur öffentlichen Kommentierung vorgelegt. In der vorliegenden Fallstudie wurde die Anwendung der darin enthaltenen Kriterien bei der CenterDevice GmbH verprobt. CenterDevice ist ein nach C5:2016 geprüfter Dienstleister, der ein cloudbasiertes Dokumentenmanagementsystem als Software-as-a-Service (SaaS) auf der Infrastruktur eines ebenfalls nach C5:2016 geprüften Cloud-Dienstleisters betreibt.

Bei einem umfangreichen Kriterienkatalog wie dem C5 stellt sich die Frage, ob er nur von großen, globalen Cloud-Anbietern erfüllt werden kann, oder ob er auch von reinen SaaS-Anbietern mit begrenzten Ressourcen umsetzbar ist.

2 Zielsetzung und Methodik

Auf Basis der oben beschriebenen Ausgangssituation soll die vorliegende Fallstudie folgende Fragestellungen beantworten:

- Welche der Kriterien des Community Draft C5:2020 können von dem Cloud-Anbieter auf Basis seiner Kontrollen zum Erfüllen der bisherigen Kriterien (C5:2016) erfüllt werden, welche nicht und warum?
- Welche der Kriterien des Community Draft C5:2020 können nicht von dem Cloud-Anbieter selbst, sondern nur durch den Subdienstleister als Betreiber der IaaS-Umgebung des Cloud-Anbieters erfüllt werden? Und inwiefern hilft hierbei eine bestehende Testierung des Subdienstleisters?

Ziel ist dabei, einerseits Dienstleistern und Prüfern entsprechende Handlungsempfehlungen zur Vorbereitung von Prüfungen nach C5:2020 zu geben. Andererseits soll hiermit exemplarisch gezeigt werden, dass eine Prüfung nach C5 auch für reine SaaS-Anbieter, die auf einer testierten Plattform ihren Cloud-Dienst aufgebaut haben, ein erreichbares Ziel darstellt.

Die Fallstudie wurde mit der CenterDevice GmbH aus Bonn (Verprobungsunternehmen) durchgeführt, die an den Standorten Bonn und Solingen seit 2011 ein cloudbasiertes Dokumentenmanagementsystem (DMS) betreibt. Das DMS bietet Funktionen zum Auffinden und strukturierten Verwalten von Dokumenten sowie zum Teilen von Dokumenten mit internen Mitarbeitern sowie externen Kunden oder Partnern. Das dienstleistungsbezogene interne Kontrollsystem wurde im Jahr 2018 erstmals einer Angemessenheitsprüfung nach C5:2016 unterzogen (Berichterstattung vom Typ 1). 2019 erfolgte die erste Wirksamkeitsprüfung der Kontrollen (Berichterstattung vom Typ 2). CenterDevice nutzt hierfür die nach C5:2016 testierte Plattform von Amazon Web Services aus Frankfurt (Berichterstattung vom Typ 2). Um alle Basiskriterien zu erfüllen, reichen die Kontrollen der CenterDevice alleine nicht aus, sondern es werden auch Kontrollen bei diesem Subdienstleister benötigt. Dieser wurde unter Anwendung der sogenannten Carve-out-Methode von der Prüfung bei CenterDevice ausgenommen. Das heißt, die Kontrollen beim Subdienstleister, die zusammen mit den Kontrollen von CenterDevice eingerichtet sein müssen, um die Basiskriterien zu erfüllen, waren nicht Gegenstand der Prüfung. Gleichwohl erfordert die Anwendung dieser Methode, dass CenterDevice eigene Kontrollen zur Überwachung der Wirksamkeit der Kontrollen beim Subdienstleister einrichten muss.

Die Fallstudie wurde durch Mitarbeiter der PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (PwC) durchgeführt, die im Auftrag des BSI an der Erstellung des Community Draft des C5 mitgewirkt und zugleich bei CenterDevice im laufenden Jahr eine Prüfung nach C5:2016 durchgeführt haben.

Die Studie wie folgt durchgeführt worden:

- Im ersten Schritt (*initiale Bewertung*) haben die Mitarbeiter von PwC überprüft, welche der Basiskriterien des Community Draft C5:2020 durch die Kontrollen des Verprobungsunternehmens

auf Basis der Berichterstattung vom Typ 2 nach C5:2016 *erfüllt, teilweise erfüllt* oder *nicht erfüllt* werden. Neue Kriterien, denen keine entsprechende Kontrolle zugeordnet werden konnte, wurden als *unklar* oder, je nach Kriterium, als *nicht anwendbar* eingestuft. Tabelle 1 gibt einen Überblick über das angewandte Bewertungsraster und verdeutlicht, dass sich bei den Einstufungen *nicht erfüllt* sowie *teilweise* ein operativer Handlungsbedarf für das Verprobungsunternehmen ergibt, um alle Kriterien des Community Draft C5:2020 zu erfüllen.

- In einem zweiten Schritt wurde die initiale Bewertung gemeinsam mit dem Verprobungsunternehmen validiert. Hierzu wurden Mitarbeiter des Verprobungsunternehmens durch PwC befragt und exemplarische Aufzeichnungen eingesehen. Dabei wurden aufkommende Fragen, Anmerkungen und Kommentare seitens der Verprobungsunternehmens mit aufgenommen und bei der späteren Auswertung der Ergebnisse (vgl. Kapitel 3) berücksichtigt.
- Im letzten Schritt wurde der finale, identifizierte Handlungsbedarf nach Aufgabenfeldern (*Dokumentation, Technik, Prozesse und Subdienstleister*) aus Sicht des Dienstleisters kategorisiert (*finale Bewertung*).

Tabelle 2 gibt einen Überblick über die Definition der jeweiligen Handlungskategorien. Auf Basis dieser Kategorisierung kann abgeleitet werden, welcher Zusatzaufwand durch eine Prüfung nach C5:2020 für einen bereits nach C5:2016 geprüften Dienstleister in der Praxis entstehen kann. Abbildung 1 fasst die Methodik zusammen.

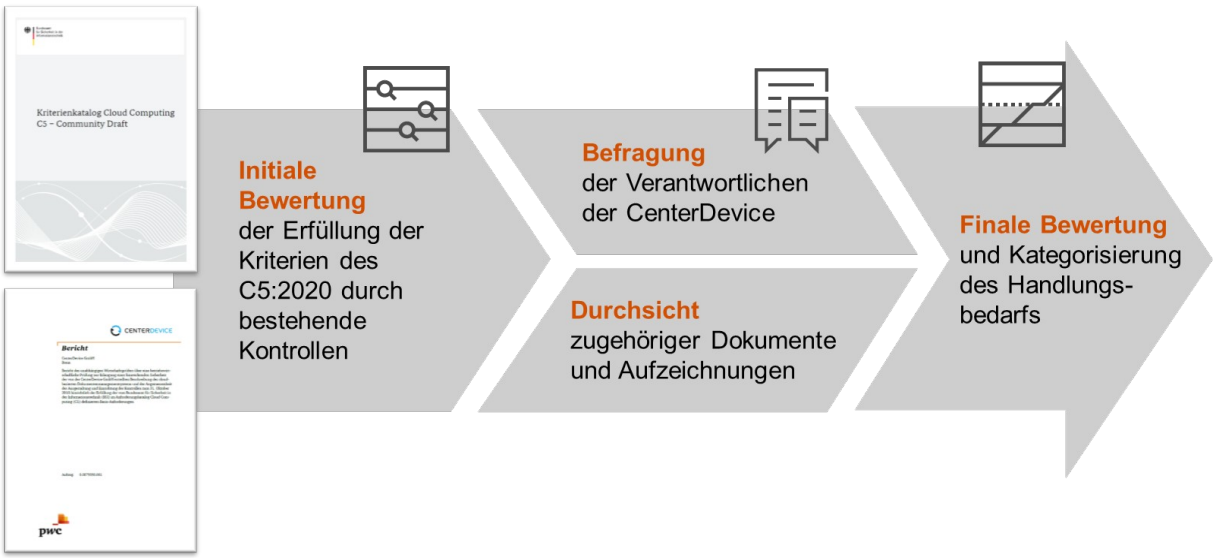

Abbildung 1: Methodik dieser Fallstudie

An dieser Stelle sei erwähnt, dass die für das Verprobungsunternehmen festgestellten Ergebnisse nur eine Indikation für andere Dienstleister sein können, die keinen Anspruch auf vollständige Übertragbarkeit erhebt. Die von den Dienstleistern in Bezug auf die Kriterien eingerichteten Kontrollen sind immer für den jeweiligen Einzelfall zu überprüfen.

Bewertungsgrad nach Erfüllung der Basiskriterien des C5:2020 durch Kontrollen von CenterDevice					
Stufen	Erfüllt	Teilweise erfüllt	Nicht erfüllt	Unklar	Nicht anwendbar
Definition	Kriterium aus C5:2020 wird durch die für C5:2016 eingerichteten Kontrollen ebenso erfüllt.	Kriterium aus C5:2020 wird durch die bestehenden Kontrollen für C5:2016 nur teilweise erfüllt.	Kriterium aus C5:2020 wird durch die bestehenden Kontrollen für C5:2016 nicht erfüllt oder es sind noch keine Kontrollen hierfür eingerichtet.	Auf Basis der vorliegenden Berichterstattung nach C5:2016 oder der Befragung war zunächst nicht ermittelbar, ob das Kriterium aus C5:2020 erfüllt werden kann. Konnte im Verlauf durch Befragung und Durchsicht ermittelt werden.	Nicht im direkten Verantwortungsbereich des Verprobungsunternehmens.
Handlungsbedarf	Nein	Ja	Ja	im Einzelfall zu betrachten	Nein

Tabelle 1: Grundlegendes Bewertungsraster für die initiale / finale Bewertung

Handlungsbedarf nach Bereich / Aufgabenfeld			
Dokumentation	**Technik**	**Prozesse**	**Subdienstleister**
Anpassung und/oder Ausweitung der bestehenden Dokumentation.	Anpassung und/oder Ausweitung der bestehenden technischen Kontrollen.	Anpassung und/oder Ausweitung der bestehenden prozessualen Kontrollen.	CenterDevice muss Kontrollen zur Überprüfung der Wirksamkeit dieser Kontrollen beim Subdienstleister einrichten.

Tabelle 2: Überblick über die Art des entstandenen Handlungsbedarfes

3 Ergebnisse

Die Kontrollen des Verprobungsunternehmens *erfüllen* 79 der 121 Basiskriterien des Community Drafts C5:2020. Hinzu kommen drei Kriterien, die für den Cloud-Dienst des Verprobungsunternehmens *nicht anwendbar* sind. Für 82 Kriterien, das entspricht 68% der Basiskriterien, besteht für das Verprobungsunternehmen somit kein Handlungsbedarf.

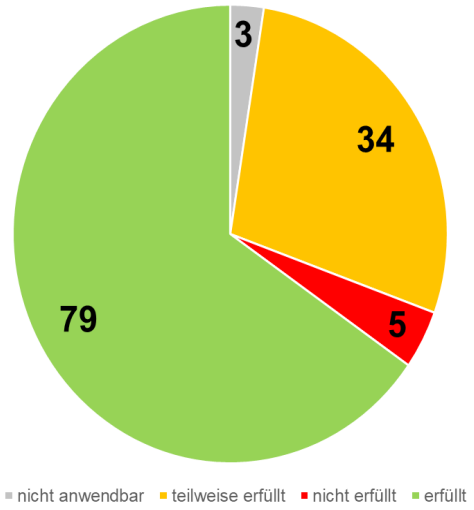

Abbildung 2: Erfüllung der 121 Basiskriterien des C5:2020 Community Draft durch Kontrollen der CenterDevice für C5:2016

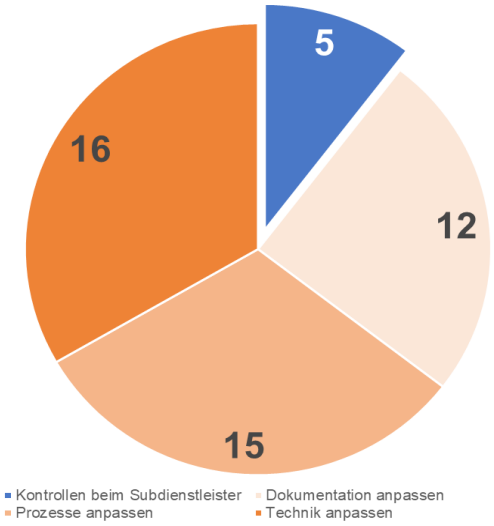

Abbildung 3: Handlungsbedarf für CenterDevice bei „teilweise erfüllt“ / „nicht erfüllt“

Bei 34 Basiskriterien ergab die finale Bewertung, dass die Kontrollen des Verprobungsunternehmens diese nur *teilweise erfüllen*. 16 dieser Basiskriterien sind neu in den Community Draft C5:2020 aufgenommen worden. Sie sind im Wesentlichen in den Bereichen „Umgang mit Ermittlungsanfragen staatlicher Stellen“ und „Produktsicherheit“ angesiedelt. Die weiteren Basiskriterien, die durch bestehende Kontrollen nur *teilweise erfüllt* werden, waren bereits im C5:2016 enthalten, weisen im Zuge der Überarbeitung aber ein höheres Sicherheitsniveau auf. Sie sind im Wesentlichen in den Bereichen „Physische Sicherheit“ und „Regelbetrieb“ angesiedelt.

Bei fünf Basiskriterien wurde festgestellt, dass das Verprobungsunternehmen zum Zeitpunkt dieser Fallstudie noch keine geeigneten Kontrollen ausgestaltet und eingerichtet hatte und diese somit *nicht erfüllt*. Bei vier dieser nicht erfüllten Basiskriterien handelt es sich um solche, die neu in den Community Draft C5:2020 aufgenommen wurden, und ein bestehendes Basiskriterium, dessen Sicherheitsniveau im Vergleich zu C5:2016 erhöht wurde (vgl. Abbildung 2).

Für die 34 *teilweise erfüllten* und 5 *nicht erfüllten* Basiskriterien besteht Handlungsbedarf. Dieser umfasst die Anpassung und / oder Ausweitung von Dokumentation, der bestehenden technischen Kontrollen sowie der prozessualen Kontrollen etwa in gleichen Maßen (vgl. Abbildung 3). Dabei können auch mehrere dieser Bedarfe auf das gleiche Basiskriterium zutreffen (z. B. sowohl prozessuale als auch technische Anpassungen).

Bei 5 dieser Basiskriterien werden zusätzliche Kontrollen beim Subdienstleister benötigt, um diese vollständig zu erfüllen. Das Verprobungsunternehmen muss für diese Basiskriterien geeignete Kontrollen einrichten, um die Wirksamkeit dieser Kontrollen beim Dienstleister zu überwachen. Da die Berichterstattung des Subdienstleisters auf C5:2016 erfolgte, gab diese keine Auskunft darüber, ob bereits entsprechende Kontrollen für diese Basiskriterien eingerichtet sind. Insoweit kann es erforderlich sein, dass auch der Subdienstleister seine bestehenden Kontrollen anpassen muss. Unabhängig davon könnte das Verprobungsunternehmen durch Einholen entsprechender Informationen seiner Verantwortung zur Überwachung der Wirksamkeit dieser Kontrollen gerecht werden.

Die detaillierten Ergebnisse je Basiskriterium können in dieser Fallstudie aus Gründen ihrer Vertraulichkeit für das Verprobungsunternehmen hier nicht dargestellt werden.

4 Fazit

Die Ergebnisse der Fallstudie zeigen, dass die Kriterien des Community Draft C5:2020 auch für kleine und mittelgroße SaaS-Anbieter anwendbar sind. Soweit bereits eine Prüfung und Berichterstattung nach C5:2016 erfolgte, kann durch Anpassung der bestehenden Kontrollen oder Ausgestaltung und Einrichtung neuer Kontrollen die Prüfbereitschaft hergestellt werden. Im Allgemeinen sind hierzu Nachbesserungen im Bereich der Dokumentation, der technischen sowie der prozessualen Kontrollen notwendig.

Die Kriterien des Community Draft C5:2020 erhöhen aus Sicht des Verprobungsunternehmens das Sicherheitsniveau[3]. Soweit in den Kriterien auch konkrete Vorgaben zur Implementierung etwaiger Kontrollen gemacht werden, kann dies für Dienstleister eine schwer zu überwindende Hürde darstellen. Aufgrund der technisch-organisatorischen Gegebenheiten beim Dienstleister, nicht vorhandener oder änderbarer Funktionen der eingesetzten Fremdsoftware oder Abhängigkeiten von Kontrollen beim Subdienstleister kann die Ausgestaltung und Einrichtung entsprechender Kontrollen einen erheblichen Aufwand darstellen. Insgesamt hat diese Verprobung aber ergeben, dass hierin kein Hinderungsgrund für eine Testierung nach Community Draft C5:2020 gegeben ist.

Aus Sicht des Verprobungsunternehmens stellen die folgenden Aspekte Erfolgsfaktoren des C5:2020 dar, die auch für kleine Cloud-Anbieter ökonomisch leistbar und umsetzbar sind:

- Der C5 adressiert den Cloud-Dienst selbst und nicht lediglich ein Sicherheitsmanagementsystem beim Cloud-Anbieter. Ein SaaS-Anbieter ist natürlicherweise auf die Erbringung seines Dienstes fokussiert und erhält mit dem C5 gute Kriterien für die sichere Erbringung seines Dienstes.
- Die C5-Kriterien definieren ein Mindestniveau an Informationssicherheit und spezifizieren nur selten konkrete Vorgaben zur technischen Implementierung von Kontrollen. Dies ermöglicht den Dienstleistern innovationsfreundliches Potential und mehr Flexibilität, insbesondere auch in der Anwendung neuer Techniken und Weiterentwicklungen im Umfeld von Cloud Computing.
- Die Prüfung nach C5 erlaubt die Verwendung von C5-Testaten von Subdienstleistern, soweit der Cloud-Anbieter geeignete Kontrollen zur Überwachung der Subdienstleister eingerichtet hat. Diese Modularität erleichtert es insbesondere SaaS-Anbietern, Sicherheit prüfbar nachzuweisen.

Dienstleister, die sich auf eine Prüfung nach C5:2020 vorbereiten möchten, wird empfohlen, die Methodik der vorliegenden Fallstudie auf ihr dienstleistungsbezogenes internes Kontrollsystem zu übertragen, um den Handlungsbedarf zu identifizieren. Die Durchführung sollte durch fachkundiges Personal erfolgen, die sowohl mit dem Kontrollsystem, als auch den Kriterien des BSI vertraut sind. Bei dieser Fallstudie erwies sich der Einsatz der bereits an der Prüfung nach C5:2016 beteiligten Personen von CenterDevice und PwC als vorteilhaft, um die Bewertung und Identifikation der oben beschriebenen Handlungsfelder innerhalb von zwei Arbeitstagen durchzuführen.

Die Erkenntnisse aus dieser Fallstudie haben dem BSI wichtige Impulse für die Finalisierung des C5:2020 gegeben.

Für die Bereitschaft zur Teilnahme an dieser Studie bedankt sich das Cloudsecurity Team des BSI bei der Geschäftsleitung der CenterDevice GmbH.

3 Ein Überblick über die erfolgten Änderungen der Anforderungen bzw. Kriterien von C5:2016 auf C5:2020 ist hier zu finden: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/C5_AktuelleVersion/C5_Neuerungen_node.html