Bundesamt
für Sicherheit in der
Informationstechnik

Mapping von BSI C5 auf ISO/IEC 27017

Bezieht sich auf Version 1.0 des BSI C5

Version 1.0

Inhaltsverzeichnis

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6666
E-Mail: cloudsecurity@bsi.bund.de
Internet: https://www.bsi.bund.de/C5

1 Einleitung

Der Standard ISO/IEC 27017 „Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services“ ist ein Informationssicherheitsleitfaden mit Fokus auf Cloud Services. Er ergänzt den Standard ISO/IEC 27002 „Information technology - Security techniques - Code of practice for information security controls“ um Cloud-spezifische Aspekte.

Die Erweiterung geschieht auf zwei verschiedene Arten. Zu den "Implementation Guidelines" (Umsetzungsrichtlinien) des Standards ISO/IEC 27002 werden weitere Beispiele aus dem Bereich Cloud Computing hinzugefügt. Hierbei wird sowohl die Kunden als auch aus Anbieter-Sicht betrachtet. Alle Umsetzungshinweise von ISO/IEC 27002 sind weiterhin gültig und werden in ISO/IEC 27017 referenziert.

ISO/IEC 27017 führt aber auch neue Controls für Cloud Computing ein. Sie sind mit dem Prefix „CLD“ ausgezeichnet und erweitern den Standard ISO/IEC 27001 „Information technology - Security techniques - Information security management systems – Requirements“ um sieben weiter Controls (Anforderungen). Zu diesen werden auch Umsetzungshinweise für Cloud-Anbieter und Cloud-Nutzer gegeben.

Zum BSI C5 (Cloud Computing Compliance Controls Catalogue) existiert schon ein Mapping der Anforderungen auf ISO/IEC 27001. Die nachfolgende Tabelle zeigt, wie die zusätzlichen Controls von ISO/IEC 27017 durch die Anforderungen des C5 abgedeckt werden. Wie auch die anderen Mappings auf den Internetseiten des BSI, ist auch diese Tabelle hier als erster Überblick gedacht und kann keine eigene tiefer gehende Analyse im Vorfeld eines Audits ersetzen.

2 Tabelle

ISO 27017	C5	Erläuterung
CLD.6.3.1	OIS-03	CLD.6.3.1 schreibt vor, dass in einer Cloud-Computing-Umgebung Rollen auf Provider und Kundenseite definiert werden müssen. Die Anforderung OIS-03 deckt dies ab.
CLD.8.1.5	PI-05, PI-02	CLD.8.1.5 behandelt die Löschung und Herausgabe von Kundenassets bzw. Kundeninhaltsdaten. In C5 sind diese Punkte durch die Anforderungen PI-05 und PI-02 abgedeckt. Kommentar: im Anforderungsbereich AM (Asset Management) des BSI C5 geht es um Assets, die zur Erbringung eines Cloud-Dienstes relevant sind und nicht um Kundendaten. Diese Controls können hier somit nicht herangezogen werden.
CLD.9.5.1	RB-23	Das Control CLD.9.5.1 beschreibt die Trennung von Daten in virtuellen Umgebungen. RB-23 entspricht diesen Anforderungen.
CLD.9.5.2	RB-22	In CLD.9.5.2 geht es um die Härtung virtueller Maschinen. Da der C5 keine Unterschiede zwischen virtuellen und physikalischen Ressourcen macht, existiert kein extra Punkt für virtuelle Ressourcen in C5. Abgedeckt wird der Punkt durch die Anforderung RB-22.
CLD.12.1.5	IDM-01, IDM-05, IDM-06	CLD.12.1.5 umfasst Anforderungen an die operative Sicherheit für Administratoren. Der ISO Standard bezieht sich in diesem Control eher auf die Kundenseite. Mit Fokus auf die operative Sicherheit auf Providerseite deckt der C5 die Anforderungen in den Punkten IDM-01, IDM-05 und IDM-06 ab.
CLD.12.4.5	Bisher nicht im C5 enthalten	In der Control CLD.12.4.5 geht es um das Thema Monitoring. Der Provider sollte dem Kunden Monitoringfunktionalität zur Verfügung stellen. Dies ist so im C5 nicht enthalten.
CLD.13.1.4	KOS-01 bis KOS-08	CLD.13.1.4 behandelt die Abstimmung der Netzwerksicherheit zwischen virtuellen und physikalischen Umgebungen. Der C5 unterscheidet nicht zwischen virtuellen und physikalischen Ressourcen. Anforderungen an die Netzwerksicherheit sind im C5 in den Punkten KOS-01 bis KOS-08 definiert.

3 Fazit

Das oben dargestellt Mapping zeigt, dass der C5 die zusätzlichen Controls aus ISO/IEC 27017 aus Provider-Sicht bereits sehr umfassend abdeckt. Die Anforderung des Monitorings für den Kunden (CLD.12.4.5) wird vom C5 aktuell nicht abgedeckt.