Dr. Philipp Kramer

Nützlicher Cloud-Datensicherheitskatalog des BSI

Der Datenschutzbeauftragte sieht sich im Datensicherheitsbereich einer Vielzahl von Gütesiegeln und sonstigen Qualitätsbestätigungen ausgesetzt. Unter Vorlage eines urkundeähnlichen Belegs wird ihm häufig mitgeteilt, dass mit der Datensicherheit alles in Ordnung sei. Ihm fehlt dann regelmäßig das Wissen, um die Wirksamkeit der Bestätigung einzuordnen. Der neue Anforderungskatalog C5 des BSI schafft hier Abhilfe.

Aktuelle Unsicherheiten bei Cloud-Services

Die Unsicherheit bei Einschaltung von Cloud-Diensten ist groß. Gerade die Verträge von Anbietern mit Sitz in anderen Rechtsordnungen (wie den USA) haben gezeigt, dass schon die Einhaltung gesetzlicher Datenschutz- und Datensicherheitsvorschriften häufig nicht gewährleistet ist. Eine Ausnahme bildet hier die Firma Amazon Web Services, die das C5-Testat bereits vorweisen kann. Der Cloud-Nutzer fragt sich, wie gut die eigenen Daten gegen Angriffe von außen (wie Industriespionage, Geheimdienste) und auch gegen den Zugriff der Administratoren des Anbieters selbst tatsächlich geschützt sind. Ein wichtiger Aspekt der Datensicherheit ist die Kontrolle der Zugriffsmöglichkeiten (siehe DSB 02/2017, Seite 36). Auch korrekte Vertragswerke und Dokumentationen werden vorausgesetzt. Gerade das wird dem Cloud-Anbieter häufig schwer fallen. Denn bisherige Testate sind nicht von sich aus zuverlässig. Man braucht Hintergrundwissen und Berichtseinsicht, um deren Nützlichkeit zu bewerten.

Standardsicherheit bei Cloud

Welche technischen Anforderungen ein Cloud-Anbieter nach Stand der Technik erfüllen muss (wie Trennung des Management-Netzwerks vom produktiven Netzwerk, physikalisch getrennte Switches, Zwei-Faktor-Authentifizierung), steht andererseits weitgehend fest. Die damit einhergehenden Anforderungen an eine Standardsicherheit hat das BSI nun im „C5 -Katalog" festgehalten. Mit ihm kann der Cloud-Anbieter also seine Standardsicherheit nachweisen.

Aufbau des Anforderungskatalogs

Der C5-Katalog hat seinen Namen von seiner vollständigen Bezeichnung Cloud Computing Compliance Controls Catalogue. Er listet 17 Anforderungsbereiche auf, denen sich ein Cloud-Anbieter stellen muss, wenn er Standardsicherheitsanforderungen erfüllen will:

1. Organisation
2. Sicherheitsrichtlinien
3. Anforderung an das Personal
4. Asset Management
5. Physische Sicherheit
6. Maßnahmen für den Regelbetrieb
7. Identitäts- und Berechtigungsmanagement
8. Kryptographie und Schlüsselmanagement
9. Kommunikationssicherheit
10. Portabilität und Interoperabilität
11. Umgang mit Informationssystemen
12. Steuerung der Dienstleister und Lieferanten
13. Security Incident Management
14. Notfallmanagement
15. Sicherheitsprüfung und -nachweis
16. Compliance und Datenschutz
17. Mobile Device Management

Umfeldparameter

Die Besonderheit dieses Anforderungskataloges ist, dass er die Umgebungsbedingungen des eigentlichen Cloud-Services berücksichtige, so Dr. Patrick Grete vom BSI. Der Cloud-Anbieter müsse eine Systembeschreibung haben, die es einem sachverständigen Dritten erlaubt, die grundsätzliche Eignung des Cloud-Dienstes für die gewünschte Anwendung zu beurteilen. Dazu gehört, darzulegen, welche staatlichen Stellen aufgrund welcher Offenbarungs- und Ermittlungsbefugnisse Zugriff auf Kundendaten haben. Auch andere Sicherheitszertifizierungen dürfen nicht einfach als Zertifikat vorgelegt werden, sondern sind durch nachvollziehbare und transparente Angaben zu ergänzen.

Testat, kein Zertifikat

Der C5-Katalog führt nicht zu einem Zertifikat des BSI, doch kann sich das Unternehmen und die Behörde von einem privaten Gutachten nach einer Prüfung bestätigen lassen, dass der Cloud-Service den Anforderungen des C5 genügt. Es sind zwei Prüfungstypen zu unterscheiden. Die einfache Typ 1-Prüfung stellt das sachgerechte interne Kontrollsystem und die Angemessenheit der Kontrollmaßnahmen dar. Für die Typ 2-Prüfung muss der Prüfer darüber hinaus die Wirksamkeit der Kontrollmaßnahmen prüfen und bewerten. Der C5 legt auch die Mindestqualifikation des Prüfungsteams fest. Mindestens die Hälfte der Mitglieder des Prüfungsteams muss über mehr als drei Jahre Berufserfahrung in der Wirtschaftsprüfung verfügen und eine bestimmte cloudspezifische Qualifikationsbestätigung wie den Certified Information Systems Auditor (CISA) der ISACA oder den ISO/IEC 27001 Lead Auditor vorweisen können.

Stichwort: C5, BSI, Cloud, Testat, Zertifikat, Auftragsverarbeitung

Autor: Dr. Philipp Kramer
Kontakt: redaktion@gliss-kramer.de