ZUSAMMENFASSENDE EMPFEHLUNGEN

Das Ziel dieser Kurzstudie ist es, einen einführenden Überblick über die gängigsten Sicherheitsstandards für Cloud-Dienste zu geben und somit öffentlichen Institutionen und Nicht-Experten im Bereich IT- und Cloud-Sicherheit in die Lage zu versetzen, Anforderungen an eine Cloud-Lösung zu beschreiben, diese zu überprüfen und somit eine fundierte Entscheidung für oder gegen eine bestimmte Cloud-Lösung zu treffen. Denn Cloud-Systeme bieten eine neue und ressourcensparende Form der IT-Bereitstellung, erfordern aber auch eine neuartige IT-Steuerung und verändern bzw. erhöhen ggf. die Anforderungen an Sicherheit, weil eine neuartige Komplexität und Verantwortungsketten entstehen. Eine der größten Herausforderungen, um Cloud Computing im öffentlichen Sektor voranzutreiben, ist die sichere und datenschutzrechtlich konforme Verarbeitung von personenbezogenen Daten.

Die wesentlichen Erkenntnisse und Empfehlungen der Kurzstudie lauten:

Die Landschaft der existierenden (de facto) Standards zu IT-Sicherheit und Datenschutz bei Cloud-Diensten ist komplex. Zertifikate bieten zwar Orientierung, sind jedoch schwer zu beurteilen, da eine allgemein anerkannte Basis-Linie für Sicherheit im Cloud Computing noch nicht existiert.

Die vom BSI formulierten Mindestanforderungen lenken zwar den Blick auf wichtige Aspekte bei Sicherheit in der Cloud, sind allerdings für eine Leistungs- und Anforderungsbeschreibung zu vage und abstrakt, da sie auf einer oberen Ebene bleiben und nicht spezifiziert werden.

Die in der Kurzstudie beschriebenen Kriterienkataloge können dazu dienen, die Anforderungen an IT-Sicherheit und Datenschutz zu definieren, da sie sie sehr dezidiert und genau die Mindestanforderungen des BSI operationalisieren. Wichtig ist, dass die wesentlichen Aspekte genauestens formuliert sind und einen Nachweis der Erfüllung seitens des Cloud-Anbieters ermöglichen.

Sollten mehrere Kriterienkataloge herangezogen werden, sind die einzelnen Kriterien voneinander abzugrenzen bzw. zu matchen. Denn die meisten Kataloge decken zum größten Teil identische Aspekte ab, sind aber unter Umständen anders formuliert. Hier kann es sinnvoll sein, die Unterstützung des IT-Dienstleisters zu nutzen und sich selbst zu informieren, um ein besseres Gefühl für das Thema zu bekommen. Nur so können informierte Entscheidungen getroffen werden.

Liegen entsprechende Angebote von möglichen Cloud-Anbietern vor, sind die Angebote miteinander zu vergleichen und vor allem zu überprüfen, ob und wie die definierten Anforderungen, insbesondere bzgl. der Sicherheit, jeweils erfüllt werden. Ein Weg ist, auf die vom Anbieter ausgewiesenen Zertifizierungen und Testate zu vertrauen.

In aller Regel kann man sich als Anwender auf Zertifikate verlassen, weil diese meist von unabhängigen und akkreditierten Dritten ausgestellt werden. Dennoch wird Kommunen und öffentlichen Verwaltungen dringend geraten, auch den Prüfbericht zu lesen oder zumindest sich über den genauen Gegenstand und Umfang der Zertifizierung umfassend zu informieren, um diesen mit den eigenen Anforderungen abzugleichen.

Die zunehmend an Bedeutung gewinnenden Selbsterklärungen auf Basis von anerkannten Verhaltenskodizes sollten kein Misstrauen wecken. Sie bilden die Einstiegsstufe des Nachweises, den man häufig bei kleineren Anbietern findet, da Zertifizierungen durch Dritte teuer und aufwändig ist.

Der Weg zu einer Auftraggeberkompetenz führt über die Auseinandersetzung mit entsprechenden Anforderungen an IT-Sicherheit und Datenschutz in der Cloud, welche nicht nur für die Auftragsvergabe, sondern auch für die spätere Steuerung des Dienstleisters notwendig ist.

Diese Auftraggeberkompetenz im Bereich Cloud und Cloud-Sicherheit ist vor dem Hintergrund der weiteren technischen Entwicklung dringend erforderlich, um auch die Abhängigkeit von IT-Anbietern und -Beratern von vornherein zu verringern. Nur so kann die dringend erforderliche Konsolidierung insbesondere der kommunalen IT erreicht werden.

Um diesen Kompetenzaufbau zu unterstützen, sollten in einem nächsten Schritt die zahlreichen Anforderungen konsolidiert und anwendergerecht operationalisiert werden. Auf diesem Weg werden öffentliche Verwaltungen und Kommunen besser als bisher in die Lage versetzt, die Prüfung der Sicherheitsanforderungen möglichst selbstständig vorzunehmen.

Schlagworte: Cloud, Cloudsicherheit, DSGVO Compliance, Anforderungen, Zertifizierung