Handlungsempfehlung der Goethe-Universität Frankfurt zur Auslagerung von Daten in die Cloud

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt die dienstliche Nutzung von Cloud-Diensten. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[1], werden durch diese Handlungsempfehlung nicht berührt.

Vor dem Hintergrund der sich immer mehr auflösenden Trennung von privaten und dienstlichen Belangen, speziell im IT-Umfeld, soll diese Richtlinie zur Sensibilisierung gegenüber den potenziellen Risiken beitragen und entsprechende Handlungsanleitungen geben.

Cloud-Dienste werden in vielen Bereichen seit vielen Jahren bewusst oder unbewusst genutzt. Hierbei ist zu beachten, dass diese meist „kostenlosen" Dienste indirekt durch Daten der Nutzenden „bezahlt" werden. Dies kann z. B. bis zur Abtretung der Rechte an den in Cloudspeichern abgelegten Daten führen. Daher ist die Speicherung von Daten in öffentlichen Clouds zu vermeiden.

Zur Speicherung von Daten in der Cloud sind folgende Regeln des Sicherheits-Management-Teams (SMT) der Goethe-Universität zu beachten:

1) Als Cloud-Dienst zur Online-Speicherung von Dateien wird u. a. die Sync-&-Share-Lösung **Hessenbox** (https://hessenbox.uni-frankfurt.de) empfohlen. Diese wird von der Goethe-Universität Frankfurt betrieben und kostenlos angeboten. Die Hessenbox ist als zugelassenes IT-Verfahren angemeldet. Weitere Informationen finden Sie unter diesem Link: https://www.rz.uni-frankfurt.de/hessenbox

2) In der Hessenbox abgelegte Daten müssen **je nach Schutzbedarf** seitens des/der Dateneigentümer/s/in verschlüsselt werden. Hierzu können frei verfügbare Werkzeuge verwendet werden:

   - **Dateien in einer Datei**
     7-Zip (https://www.7-zip.org/)

   - **Dateien in einem Container**
     VeraCrypt (https://www.veracrypt.fr/en/Home.html)
     Cryptomator (https://cryptomator.org/de/)

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt

3) Zur Sicherheit wird empfohlen, Cloud-Dienste nur über deren **Webseiten** zu nutzen und auf Apps und andere Programme zu verzichten. Wenn die Nutzung von Apps oder anderen Programmen zur Synchronisation von Daten nicht vermeidbar ist, achten Sie darauf, dass nur die **benötigten Verzeichnisse** synchronisiert werden.

4) Selbstverständlich muss auch genau beachtet werden, an welchen Personenkreis **Freigaben** erfolgen.

5) Cloud-Dienste wie Dropbox, Google Drive, iCloud, OneDrive, Amazon Drive usw. sollten nur benutzt werden, **wenn dies unvermeidbar ist**. Hierbei sind dann einige weitere Punkte zu beachten:

   - Die dienstliche Nutzung externer Cloud-Dienste muss vom behördlichen **Datenschutzbeauftragten** der Goethe-Universität genehmigt werden (dsb@uni-frankfurt.de).

   - **Verboten** ist die Nutzung externer Cloud-Dienste für personenbezogene oder urheberrechtlich geschützte Daten.

   - Eine **Geheimhaltung** kann bei externen Anbietern **nicht gewährleistet** werden. Daten sollten daher vor der Speicherung in externen Diensten verschlüsselt werden.

6) Bei Fragen, können Sie sich an Ihren zuständigen IT-Support bzw. an Ihre/n IT-Sicherheitsbeauftragte/n wenden.

Informationsquellen

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) der Goethe-Universität
  https://www.uni-frankfurt.de/smt

- Goethe-Universität Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) der Goethe-Universität
  https://www.uni-frankfurt.de/hrz/it-sicherheit