Empfehlungen und Vorschläge für die Nutzung der Hessenbox

Allgemeines

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. Die Hessenbox ist ein durch einen Verbund hessischer Hochschulen zur Verfügung gestellter Cloud-Dienst, der auf der Software eines kommerziellen Anbieters basiert aber lokal an den Hochschulen betrieben wird. Er soll es den Angehörigen hessischer Hochschulen ermöglichen, Daten sicher zu speichern und mit anderen internen oder externen Personen zu teilen ohne gleichzeitig die Hoheit über die Daten zu verlieren. Die Förderung der Hessenbox durch das Hessische Ministerium für Wissenschaft und Kunst (HMWK) zeigt hier wie wichtig das Thema einer sicheren Ablage und Übertragung von über das Internet zu teilenden Dateien auch für den Gesetzgeber ist.

In diesem Dokument werden Empfehlungen sowie praktische Vorschläge für die Nutzung der Hessenbox vorgestellt.

Sync & Share vs. Backup

Die Hessenbox ist eine reine Sync & Share-Lösung. Jede Veränderung die an einer Datei durchgeführt wird, wird zeitnah an alle betroffenen und verbundenen Clients weitergegeben. Es ist daher davon abzuraten, die Hessenbox als Backup und/oder Archivsystem nutzen zu wollen.

Schutzbedarf von Daten

Daten kann (und soll) ein Schutzbedarf zugeordnet werden. Man kann diesen Schutzbedarf umgangssprachlich mit der „Brisanz“ bzw. „Sensibilität“ der in Daten enthaltenen Informationen vergleichen. Abhängig von diesem Schutzbedarf muss abgewogen werden ob und, wenn ja, wie Daten allgemein behandelt werden (Erfassung, Speicherung, Übertragung). Die Kategorisierung des Schutzbedarfs von in Dateien befindlichen Daten kann im Regelfall nur die Person durchführen, die diese Dateien erstellt bzw. nutzt. Eine Hilfestellung soll die folgende Tabelle geben, die sich an den Schutzkategorien des BSI IT-Grundschutz-Standard 100-2 orientiert:

Beispiele (ohne Anspruch auf Vollständigkeit)	Schutzbedarf
Daten ohne Personenbezug aus öffentlich zugänglichen Quellen	Kein
Regelungen der Fakultäten und Einrichtungen wie z. B. Umläufe	Normal
Verträge mit Partner der Universität, die keine Vertraulichkeit verlangen	Normal
Personenbezogene Daten wie z. B. private Telefonnummern und E-Mailadressen Beschäftigter oder Studierender, jedoch keine personenbezogenen Daten besonderer Kategorien nach Art. 9 DSGVO	Normal
Dienstliche (nicht wissenschaftl.) Daten (z. B. aus Verwaltung und Lehre)	Normal
Nicht publizierte Wissenschaftliche Daten (z. B. Messreihen, Untersuchungsergebnisse, etc.)	Normal
Haushaltsdaten	Normal
Wissenschaftliche Daten mit hohem Schutzbedarf durch vertragliche/rechtliche Regelungen	Hoch
Studierendenakten (z.B. Prüfungsdaten, Prüfungslisten usw.)	Hoch
Personalakten	Hoch
Personenbezogene Daten besonderer Kategorien nach Art. 9 DSGVO (z.B. Biometrische Daten, Gesundheitsdaten, ethnische Herkunft)	Sehr Hoch

Anhand des Schutzbedarfes kann nun festgestellt werden, ob und wie die entsprechenden Daten in die Hessenbox geladen werden dürfen; ergänzend soll die Spalte „Sonstige“ für allgemeine Cloud-Dienste (außerhalb der Hochschulen) stehen:

Schutzbedarf	Hessenbox	Sonstige
Kein	Zulässig	Zulässig
Normal	Zulässig	Nur verschlüsselt
Hoch	Nur verschlüsselt	Nicht zulässig
Sehr hoch	Nicht zulässig	Nicht zulässig

Verschlüsselung

Die Verschlüsselung von Daten bedeutet ihre „Unkenntlichmachung“ unter Benutzung eines Schlüssels (in der Regel ein Passwort). Nur mit Hilfe dieses Schlüssels können verschlüsselte Daten wieder „entschlüsselt“ werden. Sollte also der Schlüssel verloren (z.B. das Passwort vergessen) werden, sind die Daten nicht mehr lesbar und damit ebenfalls verloren. Die Übertragung von Daten zwischen Hessenbox-Client und –Server findet grundsätzlich maschinell verschlüsselt statt. Eine generelle, zentrale Verschlüsselung der abgelegten Daten seitens der Hessenbox ist derzeit nicht möglich und Bedarf der Lösung einer Vielzahl organisatorischer und technischer Fragestellungen. In der Hessenbox abgelegte Daten müssen somit 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/)