Bayerisches Staatsministerium für
Unterricht und Kultus

Verschlüsselung

Stand: 23.10.2024

→ www.km.bayern.de / gestalten / digitalisierung / datensicherheit / verschluesselung

Inhaltsverzeichnis

Verschlüsselung

Verschlüsselung von Dateien, Wechseldatenträgern oder Container

Das Ziel einer Verschlüsselung von Dateien oder Datenträgern ist die Sicherstellung der Vertraulichkeit. Nur die Besitzer eines Schlüssels bzw. Passworts (die Begriffe werden hier synonym verwendet) können den Inhalt einer Datei lesen bzw. öffnen.

Mit anderen Worten, obwohl man Zugriff auf eine verschlüsselte Datei hat, darf es nicht möglich sein, den Inhalt zu lesen, ohne im Besitz des richtigen Schlüssels zu sein. Das bedeutet, dass ausschließlich Berechtigten der Zugriff auf die Klartextinformationen möglich ist.

Sobald vertrauliche Daten an Orten gespeichert werden, zu denen auch unberechtigte Personen Zugang haben, müssen diese verschlüsselt werden. Verschlüsselung ist auch für den Fall erforderlich, dass die Daten über einen unsicheren Transportweg (z. B. E-Mail) übertragen werden.

Wichtig: Ohne das Passwort oder den Wiederherstellungsschlüssel und ohne das zugehörige Verschlüsselungsprogramm sind die Daten nicht mehr zugänglich.

Für die Verschlüsselung sind verschiedene Aspekte zu berücksichtigen:

- Auswahl des Programms oder der Funktion zum Ver- und Entschlüsseln
- Sichere Speicherung des Schlüssels
- Beachtung der Anforderungen an die Wahl des Schlüssels
- Übertragbarkeit auf andere Systeme (Interoperabilität/Kompatibilität)
- Nutzbarkeit in der Zukunft

Zielgruppe: Schulleitung, pädagogischer Systembetreuer, Verwaltungskräfte, Lehrkräfte und sonstiges pädagogisches Personal, Schulaufwandsträger

Anforderungen an die Wahl des Schlüssels

Zum Verschlüsseln und zum Entschlüsseln in diesen genannten Verfahren wird der gleiche Schlüssel verwendet. Dieser Schlüssel muss geheim gehalten werden und „sicher“ gestaltet sein. Informationen dazu bietet das Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

Der sichere Austausch von Information ist durch die Verschlüsselung problemlos möglich. Der geheime Schlüssel ist jedoch auf einem gesonderten Kommunikationsweg zu übertragen. (Beispiel: Versand eines verschlüsselten Anhangs per E-Mail; Übertragung des Passworts per Telefon)

Verschlüsselung von Einzeldokumenten

Der Inhalt eines Dokuments wird verschlüsselt. Der Dateiname ist normalerweise im Klartext vorhanden. Beispiel: Verschlüsselung in Office-Programmen

Verschlüsselung von mehreren Dokumenten in einem verschlüsselten Container

Die Dokumente liegen in einem verschlüsselten Container (z. B. eine große Datei). Nach dem Öffnen des Containers stehen alle Dokumente im Klartext zur Verfügung. Die Sicherheit hängt in der Praxis sehr stark davon ab, wie mit dem geöffneten Container umgegangen wird. Beispiele: Veracrypt, 7-Zip.

Verschlüsselung von integrierten Festplatten und Wechseldatenträgern

Dateisysteme (Festplattenpartitionen oder mobile Datenträger) können verschlüsselt werden. Wenn ein verschlüsseltes Dateisystem hochgefahren (gemountet) wird (z. B. beim Einschalten eines Computers oder beim Einstecken einer verschlüsselten USB-Festplatte), ist ein Passwort erforderlich. Danach kann mit den Daten normal gearbeitet werden. Je nach Implementierung sind die Daten erst wieder geschützt, wenn der Benutzer abgemeldet wird, der Computer heruntergefahren oder vom Strom genommen wird. Bei mobilen Endgeräten (z. B. Smartphone, Tablet) ist bei aktiviertem Bildschirmcode der integrierte Datenträger verschlüsselt. Sobald der Bildschirmcode deaktiviert wird, liegt die integrierte Festplatte unverschlüsselt vor. Moderne Desktop-Betriebssysteme bieten integrierte Verschlüsselungsprogramme an, um die Festplatte oder ggf. auch Wechseldatenträger zu verschlüsseln.

Beispiele: Verschlüsselter USB-Stick, verschlüsselte Partitionen eines Notebooks, verschlüsseltes Dateisystem auf einem Smartphone

Beispiele für Verschlüsselungsprogramme zur Verschlüsselung von integrierten Festplatten oder Wechseldatenträgern

7-Zip

7-Zip (für Windows, Linux) ist ein Kompressionsprogramm, mit dem Dateien oder Ordner komprimiert in einer Datei (Container) gespeichert und optional auch verschlüsselt werden können.

7-Zip eignet sich sehr gut, wenn Dateien oder Ordner mit vertraulichen Inhalten verschlüsselt archiviert oder transportiert werden sollen (z. B. Dauerhaftes Speichern von vertraulichen Daten, Ablage in einer Cloud, E-Mail-Anhänge).

Keka

Für MacOS bietet das Programm Keka ähnliche Funktionen wie 7-Zip für Windows. Komprimierte und verschlüsselte Ordner sind zwischen den Programmen kompatibel.

VeraCrypt

VeraCrypt (für Windows. Linux. MacOS) ist ein sehr mächtiges Verschlüsselungsprogramm. Es arbeitet mit verschlüsselten Containern, die beim Öffnen ein Passwort erfordern. VeraCrypt gewährleistet, dass auch während der Bearbeitung keine unverschlüsselten Textteile auf der Festplatte oder in einer temporären Datei abgelegt werden und bietet daher eine sehr hohe Sicherheit.

BitLocker und Bitlocker to Go

Bitlocker ist ein Bestandteil des Windows-Betriebssystems (ab Professional), dass Teile eines Datenträgers (Partitionen) oder den gesamten Datenträger verschlüsseln kann. Es eignet sich sehr gut zur Verschlüsselung von mobilen Datenträgern (z. B. USB-Sticks), wenn mit Windows gearbeitet wird, oder zur Verschlüsselung von Datenpartitionen bei Windows-Notebooks.

FileVault

FileVault nutzt als Bestandteil des macOS-Filesystems APFS, eine Verschlüsselung, um die Daten auf dem Startvolume eines Macs zu verschlüsseln. Der Wiederherstellungsschlüssel ist an den Benutzeraccount gebunden.

Sichere Übertragung: Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung

Abhängig vom Schutzbedarf, sind geeignete Maßnahmen zur sicheren Datenkommunikation zu treffen. Die Anwendung und die Art der Datenübertragung sind bedeutsame Faktoren.

Die sog. Transportverschlüsselung wird zum Schutz der Daten zwischen Endgeräten oder Servern genutzt. Verfahren der Transportverschlüsselung schützen die Daten, so dass sie während des Transports nicht von Unbefugten gelesen oder unbemerkt manipuliert werden können. Ein Beispiel für den Einsatz einer Transportverschlüsselung ist TLS unter HTTPS (Hypertext Transfer Protocol Secure) bei einer Browserkommunikation.

Die Ende-zu-Ende-Verschlüsselung bietet einen höheren Grad an Sicherheit. Hierbei werden die Daten bereits in der Anwendung des Sendergerätes verschlüsselt und bleiben verschlüsselt, bis die Anwendung des Zielgerätes diese entschlüsselt. Selbst der Dienstanbieter, der die Daten übermittelt, kann sie nicht entschlüsseln, da nur die beiden Endgeräte die nötigen Schlüssel besitzen. Typischerweise wird diese Art der Verschlüsselung in Messenger-Apps verwendet, um die Vertraulichkeit der Kommunikation zu gewährleisten.