UNIVERSITÄT MANNHEIM

UNIT UNIVERSITÄTS-IT MANNHEIM

Tipps zur Verschlüsselung

Wieso verschlüsseln?

Vertrauliche Informationen befinden sich überall und werden regelmäßig über die unterschiedlichsten Wege ausgetauscht. Angreifer nutzen dies, um Informationen abzufangen und zu manipulieren. Verschlüsselung hilft dabei diese Angriffe zu unterbinden.

Was zu beachten ist?

- Immer ein sicheres Passwort zum Verschlüsseln wählen. Tipps hierzu unter: *https://tiny.uni-mannheim.de/passwortsicherheit*
- Passwortaustausch auf einem anderen Wege, wie z.B. über Telefon, Brief oder persönlich
- Sicheres Verschlüsselungsverfahren wählen: **AES-256**
- Nutzungsrichtline für Microsoft 365 beachten, insbesondere die darin definierte Datenklassifizierung

Was Sie wie verschlüsseln sollten:

Computer

- Hier sind Informationen für die tägliche Arbeit gespeichert
- Beim Verlust kann durch Ausbauen der Festplatte Zugriff auf alle Daten erlangt werden
  ➔ Festplatte mit Bitlocker verschlüsseln

Externe Speichermedien (ext. Festplatte, USB-Stick, etc.)

- Zum Sichern oder Austauschen von Informationen
- Können schnell verloren gehen oder gestohlen werden
- Bei vielen können die Daten nicht mehr zu 100% gelöscht werden
  ➔ Einzelne Ordner oder Dateien mit einem ZIP-Archiv verschlüsseln
  ➔ Erweiterbare verschlüsselter Ordner mit Cryptomator erstellen
  ➔ Gesamtes Speichermedium mit VeraCrypt verschlüsseln

E-Mails

- Einer der häufigsten beruflichen Kommunikationswege
- Versenden einer E-Mail ist mit dem einer Postkarte vergleichbar - jeder kann mit minimalem Aufwand den Inhalt lesen.
  ➔ Gesamte E-Mail-Kommunikation mit S/MIME verschlüsseln
  ➔ Anhänge mit einem ZIP-Archiv verschlüsseln

UNIVERSITÄT MANNHEIM

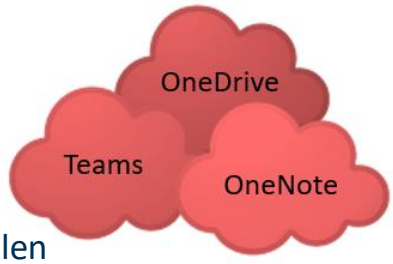
UNIT UNIVERSITÄTS-IT MANNHEIM

Netzlaufwerke der Universität Mannheim (NAS)

- Speicherung der Daten innerhalb der Universität
- Oft nicht bekannt wer alles Zugriff auf das Netzlaufwerk besitzt
  - ➔ Einzelne Ordner oder Dateien mit einem ZIP-Archiv verschlüsseln
  - ➔ Erweiterbare verschlüsselter Ordner mit Cryptomator erstellen

---

Microsoft-Cloud (OneDrive, Teams & OneNote)



- Speicherung der Daten bei Microsoft
- Microsoft besitzt jedoch ein BSI Zertifikat für sicheres Cloud Computing. Zudem existieren Verträge zwischen der Universität und Microsoft.
  - ➔ Erweiterbare verschlüsselte Ordner mit Cryptomator erstellen
  - ➔ Einzelne Ordner oder Dateien mit einem ZIP-Archiv verschlüsseln

---

Cloud Dienste (iCloud, DropBox, GoogleDrive, etc.)

- Speicherort auf den Systemen der Anbieter
- Nicht immer eindeutig bekannt wie der Anbieter mit den Daten umgeht und wer alles Zugriff auf diese hat
- Das Informationssicherheitsteam rät von der dienstlichen Nutzung solcher Dienste ab!
  - ➔ Erweiterbare verschlüsselte Ordner mit Cryptomator erstellen
  - ➔ Einzelne Ordner oder Dateien mit einem ZIP-Archiv verschlüsseln

---

Anleitungen zu Verschlüsselungs-Tools:

- 7-ZIP: *https://tiny.uni-mannheim.de/ziparchiv*
- WinRAR: *https://tiny.uni-mannheim.de/ziparchiv*
- Cryptomator: *https://tiny.uni-mannheim.de/cryptomator*
- VeraCrypt: *https://tiny.uni-mannheim.de/veracrypt*

Wissen schafft Sicherheit

Ihr Informationssicherheitsteam

- Bei Fragen und Anregungen Mail an: *infosicherheit@uni-mannheim.de*
- Sicherheitsvorfälle melden unter: *itsupport@uni-mannheim.de*
- Mehr Infos finden Sie auf: *www.uni-mannheim.de/infosicherheit*