Grundlagen der IT-Sicherheit (TU)

Grundlagen der IT-Sicherheit sind Maßnahmen und Handlungsempfehlungen, die von allen Beschäftigten mit Computerarbeitsplätzen umgesetzt werden können und sollten. Diese werden ergänzt um Empfehlungen für spezifische Situationen.

Empfehlungen

Passwortsicherheit

- Passwort des Uni-Account ausschließlich für diesen verwenden – nirgendwo sonst.[1)]
- Passwortänderungen sind nicht in regelmäßigen Abständen erforderlich aber bei jedem Hinweis auf eine Kompromittierung.
- Passwort niemals auf Emailanforderung oder auf unbekannten Webseiten eingeben – im Zweifel -1111 anrufen und nachfragen! Drohungen, zum Beispiel mit Accountsperre, sind ein deutliches Zeichen für einen Angriff.
- Passwort nicht auf Webseiten testen.[2)]

Arbeitsplatzrechner

- Keinen physischen Zugriff zulassen (Bildschirm sperren, kein Zugriff auf USB-Schnittstellen für Unbefugte).[3)]
- Bei „selbstadministrierten“ PC trotzdem regelmäßig mit einem normalen Benutzeraccount arbeiten und nur wenn unbedingt nötig mit einem Adminaccount.[4)]
- Regelmäßige Updates zulassen - beziehungsweise bei „selbstadministrierten“ PC durchführen.
- Gerade am dienstlichen Arbeitsplatz an den Dienst-PC möglichst keine private Hardware anbinden und auch sonst Vorsicht bei Bring your own device / privater Hardware.

Datenspeicherung

- Keine Nutzung der lokalen Laufwerke („C:“) zum Speichern von Daten, insbesondere von personenbezogenen Daten. Statt dessen Netzlaufwerke und Nextcloud (TU) nutzen.[5)]
- Bei Nutzung von webbasierten IT-Systemen, Downloads von personenbezogenen Daten vermeiden und wenn unbedingt nötig, diese Downloads nicht lokal speichern.

Spezifische Empfehlungen

- Bring your own device/Private Hardware
- Email
- Telearbeit, Telearbeit (TU)

Materialien/Weblinks

- Basistipps zur IT-Sicherheit. Seite bei archive.org. Siehe auch ganz am Ende der Seite „Weiter Informationen“.
- BSI: Schadprogramme - so schützen Sie sich.; Direktlink zum PDF. Seite bei archive.org. Direktlink bei archive.org.
- BSI: Sichere Passwörter erstellen. Seite bei archive.org.
- BSI: Sicherer Umgang mit Passwörtern Schritt-für-Schritt erklärt. Seite bei archive.org.

Artikel, TU

1)

Jede Eingabe des Passworts auf einer Webseite, die nicht zur TU gehört, stellt ein Risiko dar, durch Keylogger, unzureichende oder gar nicht vorhandene Verschlüsselung bei Transport oder Speicherung des Passworts, Profilbildungen etc.

2)

Es gibt eine Vielzahl von Webseiten wie https://www.stmd.bayern.de/service/passwort-check/online-anwendung-passwort-check/, wo Passwörter eingegeben werden können, um zu überprüfen, ob sie sicher sind. Aber der Eingabe des Passworts bei einer solchen Webseite ist ein Passwort **NICHT** mehr **sicher**. Hilfreich sind solche Tools höchstens, um zu testen, welche **Typen von Passwörtern** sicher sein könnten.

3)

Kurzzeitig einen USB-Stick oder auch nur ein (vermeintliches) Ladekabel an einem USB-Port können dazu führen, dass der Benutzeraccount kompromittiert ist.

4)

Wenn ein Angreifer erfolgreich ist, ist das Gefahrenpotential deutlich geringer, wenn es sich nur um einen normalen Benutzeraccount ohne Adminrechte handelt.

5)

Hintergrund ist, dass die lokalen Laufwerke in der Regel nicht ausreichend gegen Diebstahl geschützt sind und auch bei technischen Störungen Datenverluste drohen, weil kein zentrales Backup durchgeführt wird.