Hinweise für selbst administrierte Rechner (Stand: 7. Juni 2022)

Mitarbeiter*innen die ihre Geräte selbst administrieren, übernehmen zusammen mit den Administrationsrechten auch gewisse Verantwortungen. Wir weisen daher auf einige Punkte hin, die immer wieder missachtet werden und kommen damit unserer Schulungspflicht nach.

Anders als bei der Nutzung von zentral verwalteten Rechnern (Support Variante A), wo viele Aufgaben durch das SCC automatisiert werden, müssen sich Nutzer*innen von selbst administrierten Geräten eigenständig um den richtigen Umgang mit IT-Systemen kümmern. Durch den Erhalt von Administrationsrechten werden sie somit zu IT-Verantwortlichen im Sinne des IT-Grundschutzes der Universität. Der IT-Grundschutz ist unter https://www.uni-weimar.de/de/universitaet/struktur/zentrale-einrichtungen/scc-rechenzentrum/it-sicherheit/grundschutz/ nachzulesen. Hier ein Auszug der wichtigsten Punkte:

Benutzerkonten

- Ein Benutzerkonto darf nicht von mehreren Personen verwendet werden
- Passwörter dürfen nicht weitergegeben werden
- Es darf keine automatische Anmeldung von Benutzer*innen erfolgen
- Nicht benutzte Rechner müssen gesperrt werden, um Fremdbenutzung zu verhindern
- Das Passwort sollte
    - mindestens 8 Zeichen lang sein
    - nicht aus Wörtern bestehen, die im Wörterbuch zu finden sind
    - eine Mischung aus Groß-, Kleinbuchstaben und Zahlen enthalten
    - regelmäßig geändert werden (mindestens 1x pro Jahr)
- Das Passwort darf nicht für andere Dienste verwendet werden

[Gebrauch von Passwörtern (M 1.12)]

Datensicherung

Hardwaredefekte, Verluste und versehentliche Fehlbedienungen kommen immer wieder vor und können unter Umständen fatale Folgen haben. Nicht selten kommt dabei die Arbeit von mehreren Monaten abhanden. Um solchen Unfällen vorzubeugen sollten die eigenen Daten auf einem separaten Medium (z.B. Projektlaufwerke, Nextcloud oder externe Festplatte) gesichert werden. Das Sicherungsintervall kann je nach Änderungshäufigkeit angepasst werden. Im Fall von Brand oder Diebstahl sollte eine externe Festplatte auch räumlich getrennt von den Originaldaten gelagert werden **[Datensicherung (M 1.16)]**.

Software

Beim Installieren von Software muss vorher geprüft werden ob sie aus einer Vertrauenswürdigen Quelle bezogen wurde **[Kontrollierter Softwareeinsatz (M 1.7)]**.

Das Betriebssystem des Geräts sowie sämtliche darauf installierte Software muss stets auf dem neusten Stand gehalten werden **[Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (M 2.32)]**.

Ich nehme diese Hinweise zur Kenntnis und fordere das Administrationspasswort für das Gerät an.

_____ _____

Datum, Unterschrift Druckbuchstaben

Weiter Informationen finden Sie auch auf unserer Webseite unter https://uni-weimar.de/itau.