Wir empfehlen die Nutzung von Standard-Hardware

Der Betrieb von Nicht-Standard-Hardware ist an der Universität problematisch. Unten haben wir einige Quellen gesammelt, die das unterstreichen.

- Keine der im Abschnitt "Standard-Hardware" genannten Vorteile existieren aktuell für diese Systeme. Damit fehlt auch die Grundlage um eine angemessene und skalierbare Administration umzusetzen. Daher bieten wir hier nur eine Ersteinrichtung an (siehe Reiter "IT-Arbeitsplätze").
- Stetig zeitnahes Einspielen aktueller Sicherheitsupdates/Betriebssystemupgrades durch Endnutzer wird häufig vergessen. Mit Blick auf die Gefahrenlage durch äußere Einflüsse ist dieser Zustand sehr bedenklich.
  - Hacker stahlen bei der TU Berlin Hunderte vertrauliche Dokumente
  - Wenn die Uni plötzlich offline ist - Hackerangriff auf die Universität Gießen
  - Hackerangriff auf die Bergische Universität
  - Hacker-Angriff auf die Technische Hochschule Nürnberg
  - Cyberangriffe auf Forschung: Viren im Goldrausch

Weitere Anmerkungen für Apple Geräte

- Die Nutzungsdauer der Hardware beträgt nur ca. 5-8 Jahre, danach stellt Apple erfahrungsgemäß den Support ein. Aus Sicherheitsgründen werden die Geräte danach, mit zeitiger Benachrichtigung, vom Universitäts-Kabelnetz getrennt. Die Geräte können anschließend über EDUROAM weiterhin ins Internet. Der Zugang zu Projektlaufwerken und Druckern funktioniert dann nur noch per VPN.
  - macOS version history - Releases
  - macOS endoflife.date
  - Kompatibilität des aktuellen Betriebssystems
  - "*Von Apple gibt es keine offizielle Aussage, wie lange Betriebssystemversionen überhaupt Updates erhalten sollen. Über das vergangenen Jahrzehnt hat sich eingespielt, dass jeweils die beiden der aktuellen Version vorausgehenden macOS-Versionen über* ***einen unbestimmten Zeitraum*** *weiter Sicherheitsupdates erhalten.*", unter: Offene Lücke in älteren Systemen: Apples Patch-Strategie macht Nutzer verwundbar (abgerufen am 03.11.2022)
- Nur bei dem aktuellsten Betriebssystem werden alle Sicherheitslücken geschlossen. Apple hat diese Sachlage selbst mitgeteilt.
  - Apple räumt ein: Nur aktuelles macOS stopft alle bekannten Sicherheitslücken
  - "*Aufgrund von Abhängigkeiten der Architektur und Systemänderungen in jeder aktuellen Version von macOS (beispielsweise macOS 13) werden nicht alle*

bekannten Sicherheitsprobleme in früheren Versionen behoben (beispielsweise macOS 12).", unter: About software updates for Apple devices (abgerufen am 15.12.2022)

- Kontinuierlich aktuelle Systeme sind auch bei Macs sehr wichtig
  - Offene Lücke in älteren Systemen: Apples Patch-Strategie macht Nutzer verwundbar
  - Web-Meetings: Zoom-Updates dichten Schwachstellen ab
  - macOS: ZIP-Archive können Apples Gatekeeper umgehen
  - Aktuelle Sicherheitswarnung für Macs (BUW Pinnwand, abgerufen am 27.04.2023)

Revision #6
Created 16 October 2023 13:15:23 by rweiser
Updated 14 October 2024 10:58:26 by rweiser