Thema:

Goldene Regeln der Informationssicherheit

CYDS Cybersecurity, Datenschutz Informationssicherheit Hochschule Kehl

HOCHSCHULE KEHL
UNIVERSITY OF APPLIED SCIENCES
Verwaltung - Gestalten & Entwickeln

Informationssicherheit lässt sich durch ein paar einfache Verhaltensweisen deutlich erhöhen. Dabei kann jeder Einzelne mithelfen.

Goldene Regeln der Informationssicherheit

- Computer sperren
  Sperren Sie den Rechner immer auch bei nur kurzer Abwesenheit. Hilfreiche Tastenkombination: Windows-Taste + L (Windows) bzw. CTRL + CMD + Q (Apple)

- Schließen Sie Ihre Tür bei Verlassen des Zimmers ab.
  Nutzen mehrere Personen ein Büro bitte immer daran denken, dass jeder seinen Türschlüssel dabeihat.

- Begleiten Sie Besucherinnen und Besucher im Gebäude. Sprechen Sie Fremde an, die sich allein aufhalten.
  In unserem eher offenen Umfeld ist es natürlich schwierig, einen „Fremden“ zu erkennen. Hierbei verlässt man sich am besten auf den gesunden Menschenverstand. Niemand wird es einen verübeln, wenn man Unterstützung bei der Wegfindung anbietet.

- Wählen Sie ein sicheres (komplexes) Passwort und teilen Sie es mit niemandem. Nutzen Sie einen Passwort-Safe.
  Dazu gehört auch, ein initial von der IT-Abteilung vergebenes Passwort zeitnah zu ändern. Für jeden Zugang sollte ein individuelles Passwort festgelegt werden z.B. für den privaten Webmail-Dienst und die Anmeldung an Ihrem dienstlichen Arbeitsplatz. Die IT-Abteilung wird nach und nach ein Programm zur Verwaltung von Kennwörtern ausbringen (KeePass), mit dem Sie Ihre Zugangsdaten verwalten können. Sie müssen sich dann nur noch ein sicheres (Master)Kennwort merken.

- Lassen Sie keine sensiblen Daten herumliegen.
  Schließen Sie wichtige Unterlagen in Ihrem Schreibtisch ein bzw. entsorgen Sie nicht mehr notwendige Papiere in einem hierfür verfügbaren abgeschlossenen Mülleimer. Schreddern ist eine weitere Möglichkeit. Nach einer Besprechung muss ebenfalls dafür gesorgt werden, dass keine sensiblen Unterlagen im Besprechungsraum zurückbleiben. Dies gilt auch für Tafelaufschriebe.

- Schließen Sie keine privaten Geräte an dienstliche Systeme.
  Über diesen Weg kann der Rechner mit Schadsoftware infiziert werden. Dies umfasst insbesondere private Datenträger wie USB-Sticks oder SD-Karten.

- Installieren Sie Programme nur nach Rücksprache mit der IT-Abteilung.
  Die Programme müssen auf den Betrieb im Netz der Hochschule abgestimmt sein. Dies sorgt für ein stabiles und von der ITS supportetes System. Lizenzrechtliche Aspekte stehen auch im Fokus.

- Halten Sie Ihre Programme und Geräte stets auf dem aktuellsten Stand.
  Am besten konfigurieren Sie Betriebssystem, Programme (Virenscanner!) und Geräte (Tablets, Smartphones) so, dass Updates automatisiert eingespielt werden.

- Bleiben Sie stets wachsam und kritisch bei der Nutzung von Internet und E-Mail.
  Schadsoftware kann über gefälschte Webseiten oder Phishing E-Mails auf Ihren Rechner gelangen. Prüfen Sie heruntergeladene Dateien oder E-Mail-Anhänge bei Unsicherheit vor dem Öffnen mit dem Virenscanner.

Noch Fragen? Wenden Sie sich gerne an die Informationssicherheit (isb@hs-kehl.de).