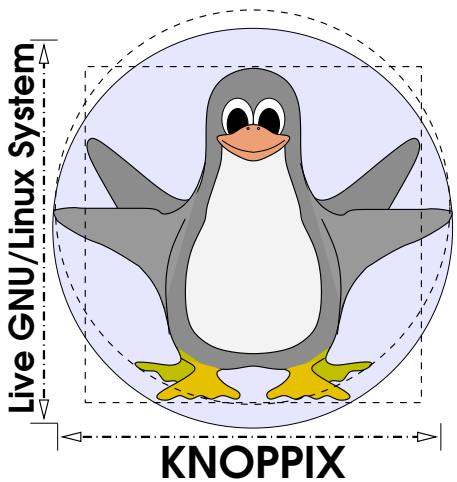
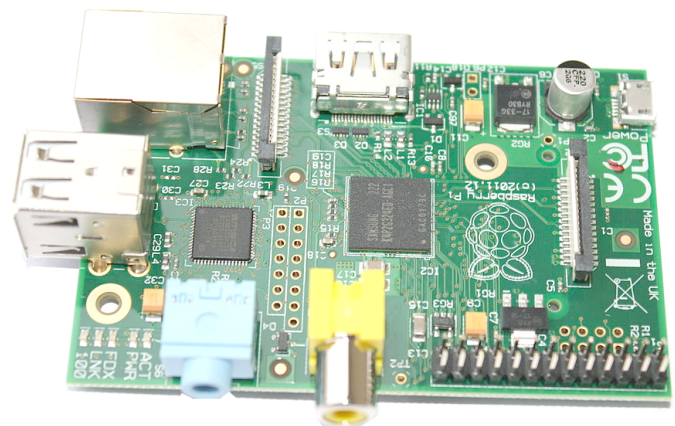
IT-Sicherheit

Prof. Dipl.-Ing. Klaus Knopper





Vorlesung zu den Knoppixtagen 2018

Organisatorisches

☞ Vorlesung mit Übungen jeweils Dienstags 16:00 Uhr

10.10.2018	Organisatorisches, Einführung
...	...

☞ **http://knopper.net/Knoppixtage/**

Kursziel

- Grundlagen der zu schützenden Güter und Schutzmechanismen kennen lernen,
- Schwachstellen und Angriffspunkte sowie Ansätze zur Verteidigung kennen lernen (praktischer Teil),
- IT-Sicherheit als integraler Bestandteil eines Gesamtkonzeptes verstehen,
- „Best Practice“ Beispiele, Normen und Anleitungen zur IT-Sicherheit kennen.

Zur Benutzung von Folien/Skript

- Der Foliensatz wird nach Bedarf während des Semesters erstellt (Work in Progress). Daher bitte Vorsicht beim Ausdrucken.
- Verweise auf sinnvolle ☞ Sekundärliteratur sind entsprechend gekennzeichnet und i.d.R. direkt anklickbar.
- Prüfungsrelevant (Klausur) sind grundsätzlich alle in der Vorlesung und in den Übungen behandelten Themen.

IT-Sec. und der Business Value of IT (1)

$$\text{BVIT} = \frac{\text{Business Performance}}{\text{IT Investment}}$$

IT Investment: Eine Investition in die **Fähigkeit, ein Geschäft zu führen**

Der **Geschäftserfolg** (Business success, business value, linke Seite der Gleichung) hängt wesentlich davon ab, den Zählerwert in der Wertegleichung (Business Performance) zu erhöhen, nicht (nur) den Wert des Nenners zu reduzieren.

IT-Sec. und der Business Value of IT (2)

Was bedeutet dies für die „IT Security", die ja als Investition im Nenner steht und sich somit grundsätzlich erst mal „negativ" auf das Ergebnis auswirkt?

☞ Die **Business Performance** hängt vom **Funktionieren der IT** ab. Ein Ausfall durch unzureichendes IT Investment in die Infrastruktur kann also den Wert des Zählers in verheerender Weise zerstören.

Ziele

- ☞ Vertraulichkeit
- ☞ Integrität
- ☞ Verfügbarkeit

Vertraulichkeit

☞ Vertraulichkeit ist die Eigenschaft einer Nachricht, nur für einen beschränkten Empfängerkreis vorgesehen zu sein. Weitergabe und Veröffentlichung sind nicht erwünscht. Vertraulichkeit wird durch Rechtsnormen geschützt, sie kann auch durch technische Mittel gefördert oder erzwungen werden.

Maßnahmen: ☞ Verschlüsselung, ☞ Digitale Rechteverwaltung (z.B. DRM)

Verfügbarkeit

Die Verfügbarkeit eines technischen Systems ist die **Wahrscheinlichkeit** oder das Maß, dass das System bestimmte Anforderungen zu einem bestimmten Zeitpunkt bzw. innerhalb eines vereinbarten Zeitrahmens erfüllt.

Als Kennzahl:

$$\text{Verfügbarkeit} = \frac{\text{Gesamtzeit} - \text{Ausfallzeit}}{\text{Gesamtzeit}}$$

Auch: Uptime = Gesamtzeit − Ausfallzeit oder „Mean Time between Failure„ (☞ MTBF)

Maßnahmen: Redundanz, Backup, Archivierung, Hot-Standby, ...

Problem: Haltbarkeit aktueller physischer Datenträger!

Integrität

s.a. Wikipedia

Alte Definition: „Verhinderung unautorisierter Modifikation von Information“

Bundesamt für Sicherheit in der Informationstechnik (BSI): „Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen“ (weiter gefasst)

Kriterien: **Korrekter Inhalt**, **Unmodifizierter Zustand** bzw. die **Möglichkeit, Modifikationen zu erkennen und zuordnen zu können**

Maßnahmen: ☞ **Prüfsummen**, ☞ **Digitale Signatur**

Ende der Vorlesung

Eingrenzung der klausurrelevanten Teile:

- Alle im Unterricht verwendeten Folien, wenn sie nicht explizit als *nicht prüfungsrelevant* deklariert wurden.
- Besprochene Handouts.
- Gemeinsam durchgeführte Übungen und Beobachtungen am Rechner.

Grundsätzlich sollen die verwendeten Begriffe beherrscht und mit eigenen Worten bzw. mit den dargestellten Stichworten erklärt werden können. Ein „wörtliches Auswendiglernen“ von Folientexten ist hingegen kaum sinnvoll.