

IT-Sicherheit

Prof. Dipl.-Ing. Klaus Knopper

Stand: 30. August 2018

Vorlesung zu den Knoppixtagen
im Wintersemester 2018/19

Inhaltsverzeichnis

1 Organisatorisches	0
2 Einleitung	1
2.1 Einordnung IT-Sicherheit	1
2.2 Ziele der Informationssicherheit	2
2.2.1 Vertraulichkeit	3
2.2.2 Verfügbarkeit	3
2.2.3 Integrität	4

1 Organisatorisches

Organisatorisches

☞ Vorlesung mit Übungen jeweils Dienstags 16:00 Uhr

10.10.2018 Organisatorisches, Einführung

... ..

☞ <http://knopper.net/Knoppixtage/>


Folie 1

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.

Folie 2

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.

Folie 3

In der Skript-Version befinden sich neben den Folien aus der Vorlesung auch noch weitere Kommentare, Fußnoten und Links, die zur Wiederholung und Klausurvorbereitung nützlich sein können.

2 Einleitung

2.1 Einordnung IT-Sicherheit

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

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

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 Wertgleichung (Business Performance) zu erhöhen, nicht (nur) den Wert des Nenners zu reduzieren.

Folie 4

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.

Folie 5

Die Art der Investition in IT-Sicherheit muss bereits in der Planung der Infrastruktur berücksichtigt werden. Eine nachträgliche „Aufbesserung“ ist i.d.R. mit deutlich höheren Kosten verbunden als eine strukturelle Maßnahme von Anfang an. (s. Folien ☞ (??) ff.)

2.2 Ziele der Informationssicherheit

Ziele

- ☞ ☞ Vertraulichkeit
- ☞ ☞ Integrität
- ☞ ☞ Verfügbarkeit

Folie 6

2.2.1 Vertraulichkeit

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)

Folie 7

2.2.2 Verfügbarkeit

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!

Folie 8

2.2.3 Integrität

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

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

Folie 9

...

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.

Folie 10