

Repetitionsblatt W1 ManSec: Intro InfoSec I

1) Definieren Sie was ein Plagiat ist und wie wir in unserem Termpaper damit umgehen wollen.

Ohne Quellenangabe kopiert; Diebstahl von geistigem Eigentum

2) Erklären Sie was die wichtigsten 4 Eckpfeiler bei der Planung einer Arbeit sind.

- Source
- Target
- Content
- Methodology

3) Wie ist eine optimale Quelle für ein Termpaper definiert?

Die Quelle sollte gleiche oder ähnliche Absichten und Ansichten haben wie die zu verfassende Arbeit haben. Der Umfang sollte in einem sinnvollen Verhältnis zur entsprechenden Arbeit stehen. Man sollte nicht vier Bücher lesen müssen, um eine Seite Text zu verfassen.

4) Beschreiben Sie den Begriff «Leserführung»

Der Leser soll durch die Arbeit geführt werden. Es sollte zu jedem Kapitel eine kurze, verständliche Einleitung und ein Schlusswort mit den wichtigsten Erkenntnissen verfasst werden.

Bilder und Grafiken sollten nicht als selbsterklärend betrachtet werden, sondern beschrieben werden.

Ein roter Faden muss durch die gesamte Arbeit erkennbar sein.

5) Wie kann ein Sicherheitsgefühl geprüft werden, sodass nachhaltig eine Aussage zur Sicherheit gemacht werden kann?

Risikoanalyse durchführen

6) Erklären Sie mindestens drei Dimensionen der Informationssicherheit.

- Technisch
- Organisatorisch
- Rechtlich

7) Welche zwei Grund-Typen von Managern kennen Sie aus der letzten Vorlesung?

- Manager (Administration)
- Leader (Führung)

8) Weshalb kann aus Sicht des Top-Managements der Eindruck entstehen, dass Information Security der grösste Flopp ist? Was sagen Sie zur Verteidigung?

Es fand ein Wettstreit zwischen Angreifern und InfoSec-Verantwortlichen statt. Dies wurde von Experten vorhergesagt, aber kaum beachtet.

9) Welchen Persönlichkeitscharakter Typ nehmen Sie erstens für einen Information Security Audit und zweitens für die Entwicklung eines neuen Security Produkts?

- Audit: *Bürokrat*
- Entwicklung: *Innovator*

10) Erklären Sie die folgenden Sichten auf die Informationssicherheit:

1. **Der Kryptologe löst das Problem**
2. **Einen Security Officer anstellen ist gut und das Problem ist gelöst.**
3. **«Commander in Charge Modell»**

1. Stammt aus einer Zeit, in der Informationssicherheit nur mit dem Schutz von Mitteilungen während der Übermittlung beschäftigt war, da noch keine Angriffe auf die Rechner ausgeführt wurden.
2. Als die Angreifer begonnen, direkt die Maschinen anzugreifen wurden CSO angestellt. Diese waren oft aber eher ein Sündenbock.
3. Ursprünglich aus dem Militär: Eine Person wird als Entscheidungsträger (Commander) eingesetzt, unabhängig von der Hierarchiestufe (Rang).

11) Beschreiben Sie eine Compliance orientierte Sicht der Security: Ist diese gut?

Compliance beschreibt das Einhalten von Regeln, Frameworks und Gesetzen. Dies sorgt für Rechtsicherheit und bietet einen gewissen Minimalschutz, muss aber mit anderen (technischen und organisatorischen) Massnahmen ergänzt werden.