

# IT-Sicherheit im Wintersemester 2015/2016

## Übungsblatt 2

**Abgabetermin:** 03.11.2015 bis 12:00 Uhr

**Achtung:** Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (über Uniworx als **Einzelabgabe**). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) erfolgt ein Bonus von zwei Drittel Notenstufen auf die Klausurnote, bei nur drei oder zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer Drittel Notenstufe.

Bei Fragen zu Übungsaufgaben sowie generellen Anregungen, Verbesserungsvorschlägen, ... zum Übungsbetrieb wenden Sie sich bitte per Email an **uebung-itsec@lrz.de**.

### Aufgabe 4: (H) Angreifermodell (10 Punkte)

- a. Nach welchen Kriterien lassen sich mögliche Angreifer charakterisieren? Nennen und erläutern Sie mindestens drei Beispiele.
- b. Definieren Sie für die folgenden Beispiele ein Angreifermodell, ordnen Sie Ihren Angreifer mit Hilfe Ihres Schemas ein und beschreiben Sie welche Schutzziele der Angreifer verletzen würde.
  - Weltweit zugänglicher Mail-Server eines Unternehmens
  - Lehrstuhlwebseite zu einer Vorlesung
  - Zentraler Internet-Knoten
- c. Inwiefern beeinflusst das Angreifermodell die Risikobewertung und das Risikomanagement?

### Aufgabe 5: (H) DoS & DDoS (7 Punkte)

In der Vorlesung wurden verschiedene Angriffstechniken vorgestellt, u.a. auch DoS und DDoS-Attacken.

- a. Erläutern Sie in Stichpunkten den Ablauf von DoS- und DDoS-Angriffen und zeigen Sie wirksame Gegenmaßnahmen auf.
- b. Erläutern Sie konkret die Funktionsweise von Syn-Cookies und zeigen Sie, wie dadurch Syn-Flooding Attacken vermieden werden können!
- c. Welche Nachteile haben Syn-Cookies?