

IT-Sicherheit im Wintersemester 2016/2017

Übungsblatt 2

Termin: 15.11.2016 - 12:00 Uhr

Aufgabe 4: (K) Angreifermodell

- 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: (K) DoS & DDoS

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?