

GSS-Übungsblatt 1 zum 16.04.2014

A. Struck, A. Dammer, S. Haase, E. Böhmecke

15. April 2014

Aufgabe 1

1.

Ein nicht-verteiltes System benötigt kein Netzwerk, um effizient Rechnen zu können. Damit ist es nicht von außen angreifbar. Ein verteiltes System teilt sich mit vielen anderen Rechnern privaten Speicher. Damit können gleichzeitig viele Systeme angegriffen werden, falls eines der Systeme kompromittiert wurde.

2.

- wenig Zeit und Rücksicht für eigene IT-Infrastruktur
- Inkompetenz
- Profitstreben auf kurze Zeiträume

3.

a)

Optional

b)

Optional

Aufgabe 2

1.

- a) Anonymität: Nutzer können Ressourcen und Dienste benutzen, ohne ihre Identität zu offenbaren. Selbst der Kommunikationspartner erfährt nicht die Identität.
Pseudonymität: Nutzer können Ressourcen und Dienste benutzen, ohne echte Identität zu veröffentlichen, sondern ein Kennzeichen (Pseudonym) wird verwendet. (Pseudonym ist mit der Identität verknüpft)
Unbeobachtbarkeit: Nutzer können Ressourcen und Dienste benutzen, ohne dass andere dies beobachten können. Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.

Manche Anwendung erfordert trotz anonymer und unbeobachtbarer Kommunikation auch die Zurechenbarkeit von Aktionen zu ihrem Akteur. Pseudonymität gestattet die Verknüpfung von Anonymität und Zurechenbarkeit.

- b) Vertraulichkeit: Geheimhaltung von Daten während der Übertragung.
Verdecktheit: Versteckte Übertragung von vertraulichen Daten.
Die Vertraulichkeit bedeutet, dass nur Kommunikationspartnern den Inhalt der Nachricht erkennen können. Und im Vergleich zu Vertraulichkeit bedeutet die Verdecktheit, dass Nachrichtaustausch "besutzt" - nur Kommunikationspartnern wissen, dass Nachricht existiert.

2.

•

Optional

3.

Optional

Aufgabe 3

1.

Ein Angreifermodell ist ein Modell, welches den stärksten Angreifer auf ein System (mit einem in dem Modell spezifizierten Angriffsvektor), den der Systemschutz noch gerade abwehren kann. Ein solches Modell wird aufgestellt, um aufzuzeigen, wie gut bzw. schlecht ein System ungefähr geschützt ist.

Es werden die folgenden Kriterien berücksichtigt:

- **Rollen:** Unterteilt in In- und Outsider, enthält das Rollen-Kriterium die Position des Angreifers in Relation zum System.
- **Verbreitung:** Beschreibt die Verbreitung des Angriffs, beispielsweise lokal oder netzweit.
- **Verhalten:** Unterteilt in aktiv und passiv bzw. beobachtend und verändernd, beschreibt das Verhaltens-Kriterium, welche Eingriffe vorgenommen werden.
- **Rechenkapazitäten:** Beschreibt die ungefähre Rechenkapazität des Angreifenden (Ausprägungen sind beispielsweise beschränkt und unbeschränkt)

2.

Rolle: Outsider

Aufgabe 4

1.:

Optional

2.:

Optional

3.:

Optional

4.:

Optional

5.:

Optional