

Systemsicherheit

Winter 2007/2008

A Einführung

A.1 Motivation

- Ziele von Sicherheit im Betriebssystem
 - Datenvertraulichkeit
 - Datenintegrität
 - Systemverfügbarkeit
 - Verbindlichkeit
- Bedrohungen
 - Aufdeckung
 - Manipulation
 - Denial-of-Service
- Angreifer
 - Personen
 - Software
- Beabsichtigte und unbeabsichtigte Schädigung des Systems

A.2 Literatur

wird noch ergänzt

Eck06. Claudia Eckert. *IT-Sicherheit. Konzepte, Verfahren, Protokolle*. Oldenbourg, München, 4. Auflage, 2006.

Schn04. Bruce Schneier. *Secrets and Lies*. dpunkt-Verlag, Heidelberg, 2004.

A.3 Grundbegriffe

- Information
 - abstrakter Begriff
 - Darstellung, Speicherung: Daten(objekte)
 - Übertragung: Informationskanäle (legitim, verdeckt)
 - Zugriff, Bearbeitung: Subjekte

- Sicherheit
 - **Safety** (Funktionssicherheit)
ein System funktioniert unter allen Betriebsbedingungen so wie es soll
 - **Security** (Informationssicherheit)
Informationen können nicht unberechtigt gewonnen oder verändert werden
 - **Protection** (Datensicherheit)
Schutz der Daten und Systemressourcen vor unberechtigtem Zugriff und Verlust
 - **Privacy** (Datenschutz, rechtlich gesehen)
Kontrolle der Weitergabe von Informationen über Personen

A.4 Schwachstellen, Bedrohungen, Angriffe

- Schwachstellen (weaknesses) und Verwundbarkeit (vulnerability)
- Gefährdungsfaktoren
- Bedrohungen (threats)
 - Nutzung von Schwachstellen oder Verwundbarkeiten gegen Schutzziele
 - kann, aber muss nicht kritisch sein
- Risiko (risk)
 - Bewertung der Wahrscheinlichkeit von Schadensereignissen und der Auswirkungen
- Angriff (attack)
 - passiv: gegen Vertraulichkeit
 - aktiv: gegen Datenintegrität
- Angreifer
 - Hacker, Cracker, Skript Kiddies, Spione