Vorlesung vom 14.04.2015

1 Einführung und Grundbegriffe

Informationen sind schützenswerte Güter, z.B. hinsichtlich

- Verlust des informationellen Selbstbestimmungsrechts (Datenschutz): Informationen über Krankheiten, Einkommen
- finanzielle Verluste: Geschäftsgeheimnissen, Verträgen, Zugangsdaten zum Online-Banking
- persönlicher Unversehrtheit: Fehlfunktionen medizinischer Überwachungsgeräte, Verkehrsleitsysteme

Inf. haben untersch. Formen: gedacht, gesprochen, geschrieben, elektronisch

Daten: Repräsentieren Informationen, z.B. als

- Bytefolge gespeichert auf der Festplatte
- Netzwerkpaket bei Übertragung über das Internet

Beurteilung der Sicherheit ausgehend von den schützenswerten Daten

Sicherheit: Schutz vor negativen Konsequenzen aus

- berechtigten Handlungen (Funktionssicherheit (engl. Safety))
  Ist-Funktionalität stimmt mit der spezif. Soll-Funktionalität überein
  (alles läuft wie geplant)
- vorsätzlichen Handlungen (Informationssicherheit (engl. Security))
  Resistenz gegenüber Angriffen
  (keiner unautorisierte Gewinnung, Veränderung, Verhinderung)

Unser Ziel: Schutz von Daten hinsichtlich der **Schutzziele**

- Vertraulichkeit: Daten sind nur autoriserten Personen zugänglich

- Integrität: Daten sind vollständig und unverfälscht
  - Authentizität: Erzeuger bekannt
  - Nichtabstreitbarkeit: Gegenüber Dritten nachweisbar
- Verfügbarkeit: Daten sind (für aut. Personen) jederzeit zugänglich

Klassisches CIA-Model (Confidentiality, Integrity, Availability)

Vorgehen zum Schutz der Daten:

1. Ermittlung des Geltungsbereichs
   - Welche Daten müssen geschützt werden
   - Wo werden diese Daten verarbeitet, gespeichert, übertragen, ... Komponenten (Computer, Router,...), Netze (Internet, Intranet,...)

2. Ermittlung des Schutzbedarfs:
   Welcher Schaden entsteht, wenn Schutzziele nicht erfüllt werden?
   - Bsp.:
     - Wahrung von Geschäftsgeheimnissen (Ziel Vertraulichkeit)
     - Verbindlichkeit von Verträgen (Ziel Nichtabstreitbarkeit)
   - Daten → Komponenten → Netzen

3. Analyse der Gefährdungen

   - Gefahr: Bei ungehindertem Verlauf Eintritt eines Schadens mit gewisser Wkeit (ohne räumlichen, zeitlichen, personellen Bezug)
     - Hochwasser: Gefahr für Leib und Leben, finanzieller Verlust
     - Pest: Gefahr für Leib und Leben
   - Bedrohungen: sind potentielle Gefahren
     - Hochwasser ist eine Bedrohung an der Oder (nicht in Berlin)
     - Pest ist keine Bedrohung (Erreger ausgestorben)
   - Gefährdung: wenn eine Bedrohung auf eine Schwachstelle trifft
     - Bei zu niedrigen Deichen ist Hochwasser eine Gefährdung
   - Mögliche Schwachstellen:
     - Innentäter (Verringerung durch Need-to-Know-Prinzip)
     - Fehler in Software:
       Heutige Betriebssysteme haben ca. 100.000.000 Zeilen Code
       Untersuchungen zeigen: Fehlerquote liegt bei ca. 0,25 %
       Also ca. 250.000 potentiell ausnutzbare Fehler

4. Risikoanalyse:

   - Risiko = Eintrittswahrscheinlichkeit × Schadenshöhe
   - Ermittlung Eintrittswkeit:
     - Wissen um Schwachstellen (siehe oben)
     - Wissen um Motivation der Angreifer, Angreifertypen:
       * White-Hacker: Aufdecken von Sicherheitslücken
       * Geheimdienste: Spionage, Sabotage und Überwachung
       * Unternehmen: Wirtschaftsspionage
         teilweise Zusammenarbeit mit Geheimdiensten
       * Whistleblower: Veröffentlichung geheimer Informationen
       * Cracker: stark professionalisierte Schattenwirtschaft
         · Fälschung von PayTV-Karten
         · Abgreifen von Kreditkarteninformationen (Warenkreditbetrug)
         · Phishing-Angriffe im Bereich Online-Banking

5. Auswahl von Schutzmaßnahmen
   Sicherheit ist in erster Linie Prävention, z.B.
   - Sicherheitsmerkmale auf Geldscheinen (Ziel Fälschungssicherheit)
     Wasserzeichen, Sicherheitsfaden, Infrarot- und UV-Farben
   - Phys. und krypt. Sicherheitsmerk. bei hoheitlichen Dokumenten
     (Ziel Fälschungs- und Verfälschungssicherheit)
   - Härtung von IT-Systemen durch Penetrationstests
   - Verschlüsselung von Dokumenten, E-Mails

In der Vorlesung:

- Basistechnologie Kryptographie
- Technische Sicherheit:
  - Verschlüsselung, Authentisierung, ...
  - Zugriffskontrolle (Rechteverwaltung unter Unix und Windows)
  - Firewalls
  - Netzwerksicherheit (Internet, Mobil, ...)
  - Softwaresicherheit (Buffer Overflow, ...)
- Organisatorische Sicherheit
  - Sicherheitsstrategien
  - Bewertungskriterien (für Produkte)
  - IT-Sicherheitsmanagement (Technik, Organisation, Menschen)
- Gesetzliche und ehtische Aspekte

In allen Themen: Gefährdungen, Angriffe $\rightarrow$ Schutzmaßnahmen