IT-Sicherheit:

Security Engineering, Sicherheitsmanagement

Center for Computing Technologies

Security Engineering

- Evaluation gemäß Sicherheitskriterien setzt fertiges IT-Produkt voraus
- Wie erhält man die geeigneten Sicherheitsmechanismen für ein solches Produkt wie z.B. für ein Krankenhausinformationssystem?
- Wie analysiert man die Bedrohungen?
- Wie schätzt man die Risiken ab?
- Wie erhält man die geeigneten Sicherheitsanforderungen?
- Einsatz von Techniken aus dem Software Engineering und aus dem Bereich der Safety-Critical Systems

Universität Bremen

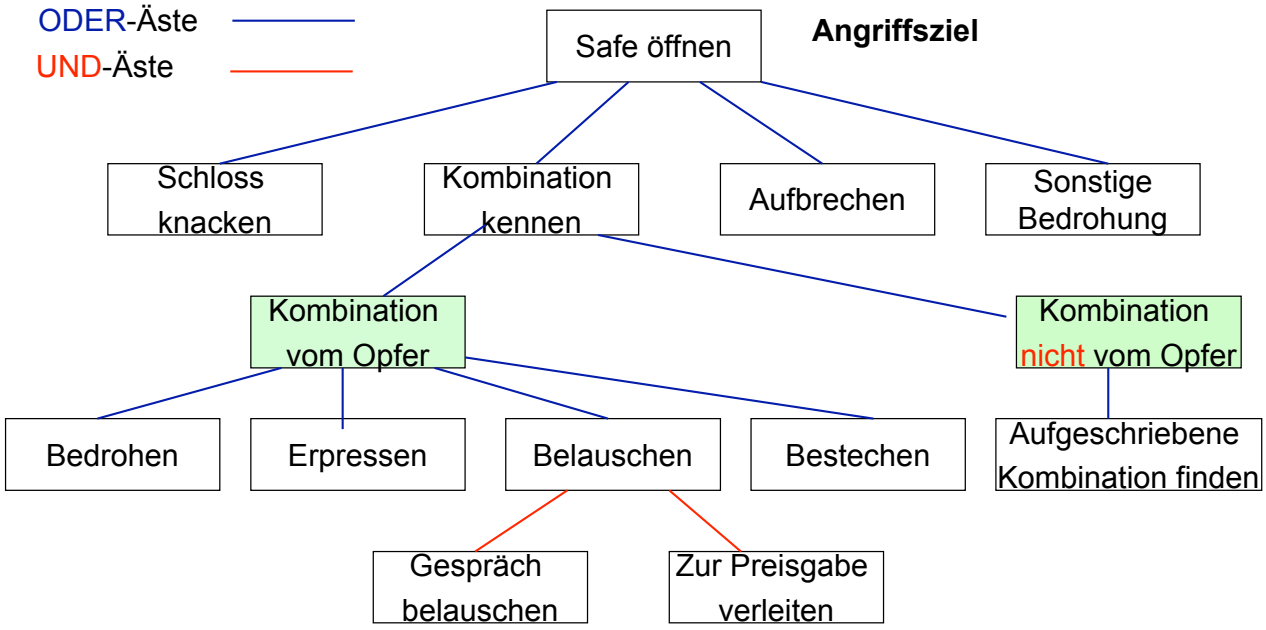
Bedrohungsanalyse

- **Ziele:**
  - Ermitteln des Sicherheits-Ist-Zustands
  - Aufdecken von Schwachstellen, potentiellen Bedrohungen
    - Nutzung publizierter Schwachstellen (CERT, Hersteller, ...)
  - Ermittlung von Gefährdungsfaktoren (organisatorische, technische, benutzerbedingte), u.a. mit Penetrationstests
- **Verwendete Methoden:**
  - Analyse mit Bedrohungsbaum/Angriffsbaum
    - Grafisch oder textuell
    - Nutzung publizierter Attack-Patterns für Standard-Szenarien
  - Analyse mit Bedrohungsmatrix (s. Buch C. Eckert, „IT-Sicherheit“)

Strukturierte Analyse mit Bedrohungsbaum

- Bedrohungsbaum (***attack tree***)
  Anlehnung an Fehlerbäume (***fault tree***) aus dem Safety-Bereich
  - Pro Angriffsziel ein Baum: (Bsp. siehe folgende Folie)
  - Wurzel beschreibt ein Angriffsziel, z.B. Safe knacken
  - Blatt: einzelner Angriffsschritt, z.B. Schloss knacken
  - Pfad von Blatt zur Wurzel: Angriff zum Erreichen des Ziels
    (z.B.: durch Erpressung an die Kombination kommen)
- Beschreibung von Situationen, in denen
  - mehrere Angriffsschritte zusammen notwendig sind: UND-Äste
  - alternative Angriffsschritte genutzt werden können: ODER-Äste (Teilbäume)
- Zur systematischen Erstellung sinnvoll:
  - Festlegen von Unterzielen, Teilzielen
  - Teilziele definieren wiederverwendbare Teilbäume

Beispiel für einen Bedrohungsbaum



Textuelle Darstellung eines Bedrohungsbaumes

- Alternative zur grafischen Darstellung eines Bedrohungsbaumes: textuelle, kompaktere Darstellung eines Bedrohungsbaums:
  - alle direkten Nachfolger werden auf einer Ebene dargestellt
  - Ebene wird als ODER- bzw. UND-Ebene annotiert
  - Jede Ebene wird durch ein textuelles Einrücken nachgebildet.

- **Beispiel:** Bedrohungsanalyse für eine verschlüsselte Nachricht
  Szenario: Alice (A) und Bob (B) tauschen verschlüsselte Daten aus
  - Nachricht M ist mit gemeinsamem Schlüssel K_AB verschlüsselt
  - Ziel: Angreifer will M im Klartext „sehen“

Ausschnitt aus einem textuellen Angriffsbaum

ODER Subziel 1: Dechiffrieren der verschlüsselten Nachricht
ODER Knacken des Kryptotextes
Kryptoanalyse
Subziel 2: Bestimmung des Schlüssels K_AB
ODER Subziel 2.1: Zugriff auf Speicher von A und auf dort abgelegten K_AB
Subziel 2.2: Zugriff auf Speicher von B und auf dort abgelegten K_AB
Subziel 2.3: Verleite A zur Preisgabe von K_AB
Subziel 2.4: Verleite B zur Preisgabe von K_AB

Risikoanalyse (1)

- **Ziel:** Identifizierte Bedrohungen bewerten!

Kosten-Nutzen-Analyse:

- Bewertung des Risikos
  - Was ist wertvoll und muss geschützt werden?
  - Wie hoch sind die zu erwartenden Schäden?
- Wie hoch sind die Kosten für Gegenmaßnahmen?

Risikoanalyse (2)

- Risiko nach DIN-VDE Norm 310000-2:
  - Quantitatives Risiko **R = S * E** mit:
    - Schadenshöhe (Schadensausmaß) S,
    - Eintrittswahrscheinlichkeit E
- Schadenshöhe S:
  - Primäre Schäden: Produktivitätsausfall, Wiederbeschaffungs-, Personalkosten, Wiederherstellungskosten, …
  - Sekundäre Schäden (schwer zu quantifizieren): Imageverlust, Vertrauensverlust bei Kunden, ….
- NIST: Annual Loss Expectancy (ALE)
  - **ALE = Schadenshöhe pro Jahr * # der Sicherheitsvorfälle**

Risikoanalyse (3)

- **Beispiele:**
  S = 1.000.000 €; E = 0,01: R = 10.000 €
  S = 1.000.000.000 €; E = 0,001: R = 1.000.000 €
  S = 30.000 € ; E = 0,5: R = 15.000 €

- Quantitative Risikoanalyse in der Praxis kaum möglich, aber oft vom Management gewünscht
- Risikoanalyse ist ein aufwendiges Verfahren
- Analyse verlangt Expertenwissen:
  - über schützenswerte Güter, Unternehmensprozesse.
  - über Angreifer, über Sicherheitstechnologien, …

Requirements Engineering

- Woher bekommt man die angemessenen Sicherheitsanforderungen (***security requirements***) für das Produkt?
- Ergebnisse der Bedrohungs- und Risikoanalyse nutzen
- Als Ausgangspunkt: Schutzprofile und Sicherheitsvorgaben durchsuchen
- Sicherheitsverantwortliche fragen und vor allem auch Nutzer des Systems:
  - In einem Krankenhaus z.B. klinisches Personal, Mitarbeiter aus der Verwaltung
- Verbesserung des Abdeckungsgrades:
  - Nicht nur ein Sicherheitsberater denkt über die Anforderungen nach, sondern eine Gruppe von Sicherheitsberatern mit unterschiedlichem Hintergrund
  - Anforderungen haben genauso (oder mehr?) Bugs wie/als Software selbst

Security Management

Security Management nach BSI-Grundschutz

- Ziel: Etablierung eines Sicherheitsprozesses in einer Organisation (wie z.B. Unternehmen, Behörden)
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- IT-Sicherheitshandbuch & Grundschutzhandbuch (GSHB)
  - Informationen: http://www.bsi.de
  - CD mit Grundschutzhandbuch (kostenlos), > 2000 Seiten!
  - Zusammengefasste Darstellung u.a. im Buch C. Eckert: „IT-Sicherheit“
  - GSTool: Hilfestellung bei der Anwendung des GSHB http://www.bsi.de/gstool/index.html

BSI-Grundschutzhandbuch (GSHB)

- sehr weit im Einsatz in Unternehmen mit niedrigem bzw. geringem Schutzbedarf
- Mehr als 50 Bausteine beschreiben verschiedene Aspekte der IT-Sicherheit (Server, PC, Firewall, E-Mail, WLAN, ...)
- organisatorische, personelle, infrastrukturelle und technische Standardsicherheitsmaßnahmen
- Gefährdungs- und Maßnahmenkataloge
- Zertifizierung: IT-Grundschutzzertifikat (verschiedene Stufen)
- Umsetzung durch lizensierten Auditor bestätigt (höchste Stufe)
- Weitere Unterstützung durch GSTOOL: u.a. Hilfen bei Strukturanalyse, Schutzbedarfsfeststellung, Berichterstellung, Revisionsunterstützung, Basissicherheitscheck

Beispiel für einen Baustein des GSHB

Beschreibung

Über ein Modem wird eine Datenendeinrichtung, z. B. ein PC, über das öffentliche Telefonnetz mit anderen Datenendeinrichtungen verbunden, um Informationen austauschen zu können. Ein Modem wandelt die digitalen Signale aus der Datenendeinrichtung in analoge elektrische Signale um, die über das Telefonnetz übertragen werden können. Damit zwei IT-Systeme über Modem kommunizieren können, muss auf den IT-Systemen die entsprechende Kommunikationssoftware installiert sein. Unterschieden werden externe, interne und PCMCIA-Modems. Ein externes Modem ist ein eigenständiges Gerät mit eigener Stromversorgung, das üblicherweise über eine serielle Schnittstelle mit dem IT-System verbunden wird. Als internes Modem werden Steckkarten mit Modem-Funktionalität, die über keine eigene Stromversorgung verfügen, bezeichnet. Ein PCMCIA-Modem ist eine scheckkartengroße Einsteckkarte, die über eine PCMCIA-Schnittstelle üblicherweise in Laptops eingesetzt wird.

Gefährdungslage

In diesem Kapitel werden für den IT-Grundschutz beim Einsatz eines Modems folgende Gefährdungen angenommen:

Gefährdungslage des Bausteines

Höhere Gewalt:
- G 1.2 Ausfall des IT-Systems

Menschliche Fehlhandlungen:
- G 3.2 Fahrlässige Zerstörung von Gerät oder Daten
- G 3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen
- G 3.5 Unbeabsichtigte Leitungsbeschädigung

Technisches Versagen:
- G 4.6 Spannungsschwankungen/Überspannung/Unterspannung

Vorsätzliche Handlungen:
- G 5.2 Manipulation an Daten oder Software
- G 5.7 Abhören von Leitungen
- G 5.8 Manipulation an Leitungen
- G 5.9 Unberechtigte IT-Nutzung
- G 5.10 Missbrauch von Fernwartungszugängen
- G 5.12 Abhören von Telefongesprächen und Datenübertragungen
- G 5.18 Systematisches Ausprobieren von Passwörtern
- G 5.23 Computer-Viren
- G 5.25 Maskerade
- G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten
- G 5.43 Makro-Viren

Beispiel: Gefährdungslage

G5.9 Unberechtigte IT-Nutzung

Ohne Mechanismen zur Identifikation und Authentisierung von Benutzern ist die Kontrolle über unberechtigte IT-Nutzung praktisch nicht möglich. Selbst bei IT-Systemen mit einer Identifikations- und Authentisierungsfunktion in Form von Benutzer-ID- und Passwort-Prüfung ist eine unberechtigte Nutzung denkbar, wenn Passwort und zugehörige Benutzer-ID ausgespäht werden. Um das geheim gehaltene Passwort zu erraten, können Unbefugte innerhalb der Login-Funktion ein mögliches Passwort eingeben. Die Reaktion des IT-Systems gibt anschließend Aufschluss darüber, ob das Passwort korrekt war oder nicht. Auf diese Weise können Passwörter durch Ausprobieren erraten werden. Viel erfolgversprechender ist jedoch die Attacke, ein sinnvolles Wort als Passwort anzunehmen und alle Benutzereinträge durchzuprobieren. Bei entsprechend großer Benutzeranzahl wird damit oft eine gültige Kombination gefunden.Falls die Identifikations- und Authentisierungsfunktion missbräuchlich nutzbar ist, so können sogar automatisch Versuche gestartet werden, indem ein Programm erstellt wird, das systematisch alle möglichen Passwörter testet...

Maßnahmenempfehlungen für den Baustein

Infrastruktur:
- M 1.25 (3) Überspannungsschutz (optional)
- M 1.38 (1) Geeignete Aufstellung eines Modems

Organisation:
- M 2.25 (2) Dokumentation der Systemkonfiguration
- M 2.42 (2) Festlegung der möglichen Kommunikationspartner
- M 2.46 (2) Geeignetes Schlüsselmanagement (optional)
- M 2.59 (1) Auswahl eines geeigneten Modems in der Beschaffung
- M 2.60 (1) Sichere Administration eines Modems
- M 2.61 (2) Regelung des Modem-Einsatzes
- M 2.204 (1) Verhinderung ungesicherter Netzzugänge

Personal:
- M 3.17 (1) Einweisung des Personals in die Modem-Benutzung

Hardware/Software:
- M 4.7 (1) Änderung voreingestellter Passwörter
- M 4.30 (2) Nutzung der in Anwendungsprogrammen angebotenen Sicherheitsfunktionen
- M 4.33 (1) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
- M 4.34 (2) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen (optional) ...

Beispiel einer Maßnahmenbeschreibung

M 4.7 Änderung voreingestellter Passwörter

Verantwortlich für Initiierung: TK-Anlagen-Verantwortlicher, IT Sicherheitsmanagement, Leiter IT

Verantwortlich für Umsetzung:Administrator

Viele IT-Systeme, TK-Anlagen und Netzkoppelelemente (bspw. ISDN-Router, Sprach-Daten-Multiplexer etc.) besitzen nach der Auslieferung durch den Hersteller noch voreingestellte Standardpasswörter. Diese sollten als erstes durch individuelle Passwörter ersetzt werden. Hierbei sind die einschlägigen Regeln für Passwörter zu beachten (vgl. M 2.11 *Regelung des Passwortgebrauchs*).

BSI = British Standards Institute

BS 7799

- **British Standard (BS) 7799**
  - Ziel: Aufbau eines IT-Sicherheitsmanagements; Verankerung in der Organisation
  - Management-orientiert, nicht technisch
  - keine detaillierten Umsetzungshinweise, sondern übergreifende Anforderungen
  - Zertifizierung gemäß BS 7799 Teil 2 möglich (durch lizensierte Auditoren)
- BS 7799 Teil 1 ist Basis für **ISO/IEC 17799**
  - Best Practice Verfahren und -methoden,
  - keine Empfehlung für konkrete Sicherheitslösungen
  - keine Hilfestellung zur Bewertung existierender Sicherheitsmaßnahmen

Themenbereiche BS 7799

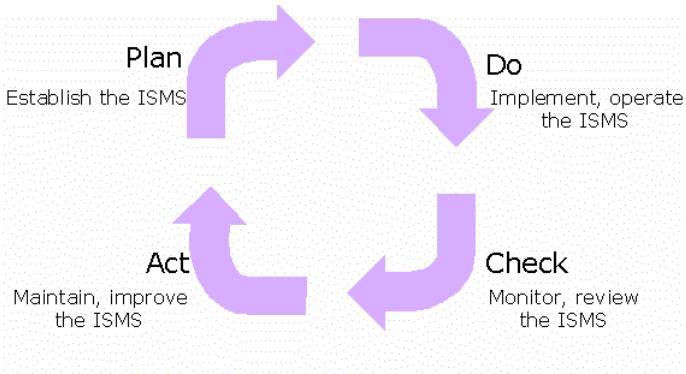
- Zehn Themenbereiche:
  1. Security policy — Provides management direction and support for information security
  2. Organisation of assets and resources — To help you manage information security within the organisation
  3. Asset classification and control — To help you identify your assets and appropriately protect them
  4. Personnel security — To reduce the risks of human error, theft, fraud or misuse of facilities
  5. Physical and environmental security — To prevent unauthorised access, damage and interference to business premises and information

Themenbereiche BS 7799

6. Communications and operations management — To ensure the correct and secure operation of information processing facilities
7. Access control — To control access to information
8. Systems development and maintenance — To ensure that security is built into information systems
9. Business continuity management — To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters
10. Compliance — To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement

BS 7799 Teil 2

- Information Security Management System (ISMS)
- „ISO 9000 für Security“
- Plan-Do-Check-Act (aus QM)
- Zertifizierbar (¥€$!)
- Noch nicht in ISO 17799



Vergleich CC/BSI GSHB/BS 7799

- CC:
  - Abstrakt
  - auf verschiedene IT-Produkte anwendbar
  - nur Technik, keine organisatorischen Maßnahmen
  - Internationaler Standard
- BSI GSHB
  - Konkrete Maßnahmen
  - Auf ganze IT-Systeme, nicht aber auf einzelne IT-Produkte anwendbar
  - Sowohl technische als auch organisatorische Maßnahmen
  - Kein internationaler Standard
- BS 7799
  - Auf ganze IT-Systeme, nicht aber auf einzelne IT-Produkte anwendbar
  - Nur organisatorische/prozessorientierte Maßnahmen
  - Internationaler Standard

Administrivia

Fachgespräche

- Fachgespräch dient zur Validierung der Ergebnisse der Übungsaufgaben
- Gegenstand: Inhalt der Lehrveranstaltung
- Durchführung am besten in der ganzen Gruppe
  - Wenn das nicht geht, andere Zusammensetzung
- Voraussetzung: Alle Übungsaufgaben bearbeitet
- Scheinformular drucken wir, bitte Name und Matrikelnummer mitbringen

Fachgespräche

- Termine
  Mo/Di 25/26.7.2005
  Mo/Di 29/30.8.2005
  Mo/Di 26/27.9.2005
- Jede Gruppe sendet bitte eine Email an np@tzi.de, in der sie angibt
  - welche/n dieser Termine sie bevorzugt
  - welche alternativ möglich wären und
  - an welchen sie nicht kann.

Mündliche Prüfungen

- Studierende nach aktueller DPO (Informatik-Diplom) oder Ba/Ma können auch eine Mündliche Prüfung ablegen
- Bitte ebenfalls alle Übungsaufgaben abgeben
- Zur Auswahl stehen die gleichen Termine, max. 2 Anmeldungen pro Stunde

Fragebogen

- Vorbereitung auf Fachgespräch/Mündliche Prüfung
- Fragen zur Selbstüberprüfung
  - Nicht zum Abgeben der Antworten
  - Nicht die abschließende Liste aller Prüfungsfragen
  - Nicht als „Lernliste“ geeignet
- Bitte in der Gruppe bearbeiten
- Verfügbar ab 15.7. in Stud.IP
  - Bis dahin bitte mit Literatur und Foliensätzen arbeiten