IT Sicherheit

Universitatea “Transilvania” din Brasov

Agenda Sicherheit in der Informationstechnologie

6 IT-Sicherheitspolitik

6.1 Risikoanalyse

6.2 Sicherheitskonzept

6.3 Risikomanagement

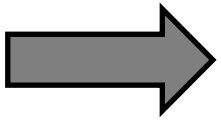
6 Bewertung von IT-Sicherheit

6 Bewertung von IT - Sicherheit

Bewertung der Sicherheit von IT-Systemen

Existenz von unterschiedlichen Kriterienwerken für die Bewertung der IT-Sicherheit von IT-Systemen (Produkte und Gesamtlösungen)

- Existieren nebeneinander
- Setzen unterschiedliche Schwerpunkte
- Teilweise überschneidend
- Verschiedene Zielgruppen
- Beispiele: BSI-Grundschutzhandbuch, BS 7799, ITSEC, Common Criteria ISO/IEC 15408



Hersteller und Benutzer von IT-Systemen benötigen weltweit akzeptierte einheitliche Evaluationskriterien zur Bewertung der IT-Sicherheit der IT-Systeme!

6 IT-Sicherheitspolitik

Kriterienwerk für IT-Sicherheit

Leitfaden als Prüf- und Bewertungsschema

der IT-Sicherheit von IT-Systemen

Benutzer

- Unterstützung bei der Festlegung von IT-Sicherheitsanforderungen
- Unterstützung bei der Auswahl von IT-Systemen entsprechend ihrer Sichherheitsbedürfnisse
- Vergleich von (ggf. zertifizierten) IT-Systemen

Hersteller

- Unterstützung bei der Produktentwicklung
- Unterstützung bei der Prüfung und Bewertung der Produkte anhand von Sicherheitsanforderungen
- Festlegung von Sicherheitszertifikaten der Produkte

Evaluatoren von IT-Systemen

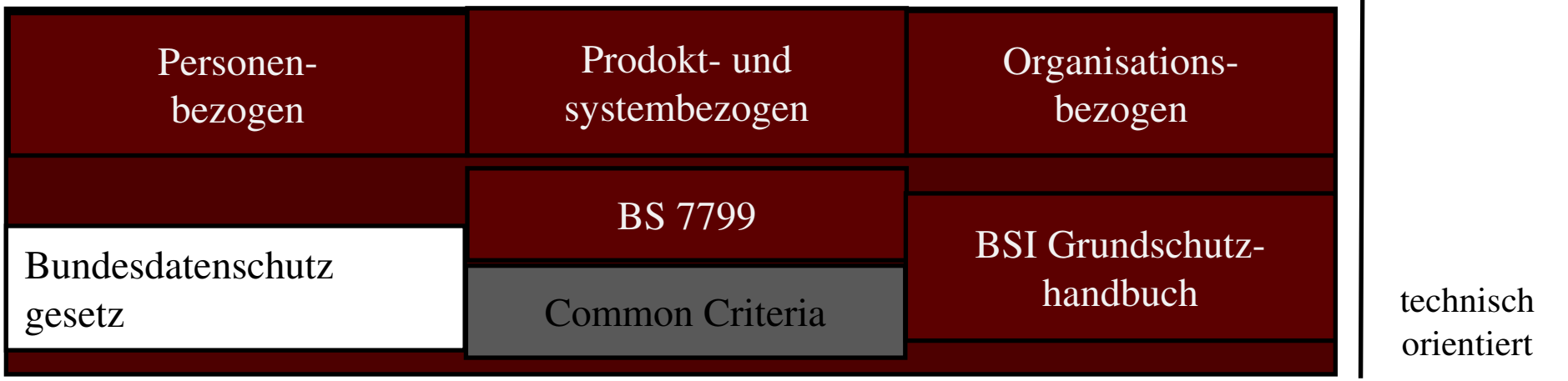
6 Bewertung von IT - Sicherheit

Bewertung der Sicherheit von IT-Systemen...

IT-Sicherheit bezieht sich auf die Bereiche

- **Personenbezogene Sicherheit**
- **Produkt- und systembezogene Sicherheit**
- **Organisationsbezogene Sicherheit**

Klassifizierung der Kriterienwerke nach ihrem Fokus auf diese Bereiche:



6 Bewertung von IT - Sicherheit

Bewertung der Sicherheit von IT-Systemen...

(A) Kriterienwerk TCSEC (Orange Book)

- *Trusted Computer System Evaluation Criteria*
- Anfang 1980 am US National Computer Security Center entwickelt
- Klassifizierung der Sicherheit von IT-Systemen nach 4 Hierarchiestufen D, C, B, A (höchste Stufe)
- Nachteile u.a.:
  - einseitige Ausrichtung auf zentrale Betriebssysteme, so dass verteilte Systeme nicht erfasst werden
  - Vernachlässigung von benutzerspezifischen Sicherheitsinteressen
  - Erfüllung einer Sicherheitsfunktionalität kann nicht nach der Wirksamkeit der Schutzmechanismen gegenüber Bedrohungen bewertet werden (Maß an Vertrauenswürdigkeit fehlt)

6 Bewertung von IT - Sicherheit

Bewertung der Sicherheit von IT-Systemen...

(B) Kriterienwerk ITSEC

- *Information Technology Security Evaluation Criteria*
- Seit 1991 als europäische Kriterien der Länder UK, F, NL, D
- Funkionklassen mit Sicherheitsanforderungen für spezifische Anwendungsklassen
- Klassifizierung der Sicherheit nach 7 Evaluationsstufen von E0 (unzureichend) bis E6 (ausgezeichnet)
- Es können Hardwarekomponenten und Software für unterschiedliche Anwendungsbereiche bewertet werden
- Nachteile u.a.:
  - Nach wie vor Konzentration auf zentrale Systeme
  - Zertifikate sind nicht weltweit anerkannt

6 Bewertung von IT - Sicherheit

Bewertung der Sicherheit von IT-Systemen...

(C) Kriterienwerk ISO/IEC 17799 (BS 7799-1)

- *Code of practice for Information security management*
- Seit Dezember 2000 durch die ISO als internationaler Leitfaden (Standard 17799) für das Management der IT-Sicherheit von dem Britisch Standards Institute (BS 7799-1) übernommen (Sammlung optimaler Maßnahmen nach dem Best-practice-Ansatz)
- Neben technischen präventiven Maßnahmen werden alle Elemente des Kommunikationsflusses innerhalb des Unternehmens (Prozesse) zur Erhöhung der IT-Sicherheit berücksichtigt
- organisatorische Maßnahmen, die durch das Management getragen werden (Security policy), sind in den Kriterienkatalog aufgenommen (Technik-Prozesse-Management)
- enthält zahlreiche generische Komponenten
- Umsetzung einer Sicherheitsmaßnahme obliegt voll und ganz der Organisation; schreibt keine konkreten Technologien vor

6 Bewertung von IT - Sicherheit

Bewertung der Sicherheit von IT-Systemen...

(D) Kriterienwerk Common Criteria

- *Common Criteria for Information Technology Security Evaluation*
- Standard ISO/IEC 15408 (kurz: CC) bestehend aus den3 Teilen: Teil 1: *Introduction and general model*, Teil 2: *Security functional requirements* und Teil 3: *Security assurance requirements*
- Seit 1996 vom gemeinsamen Technischen Komitee JTC 1 der ISO (International Organization for Standardization) und IEC (International Electrotechnical Commission) als internationaler Standard erarbeitet
- Version 2.1 ist seit August 1999 veröffentlicht und wird in Deutschland vom BSI zur Evaluierung verwendet
- Klassifizierung der Sicherheit nach 7 Vertauenswürdigkeitsstufen (Evaluation Assurance Level) von EAL1 (gering) bis EAL7 (sehr hoch)

6 Bewertung von IT - Sicherheit

Common Criteria...

Prinzip

- Der Evaluierungsgegenstand (TOE – Target of Evaluation) wird zunächst in Schutzprofilen(PP – Protection Profile) unabhängig von der Einsatzumgebung beschrieben und dann entsprechend der konkreten Anwendung erweitert bzw. präzisiert
- Anschließend erfolgt die Einstufung des TOE in eine der Vertrauenswürdigkeitsstufen (EAL) entsprechend der spezifischen Sicherheitsvorgaben (ST – Security Target)
- Zertifizierung des TOE, wobei Gültigkeitsbereiche angegeben werden, in denen sich das Evaluierungsergebnis trotz nachträglicher Änderungen am TOE bzw. dessen Einsatzumgebung nicht ändert (Re-Zertifizierung)

6 Bewertung von IT - Sicherheit

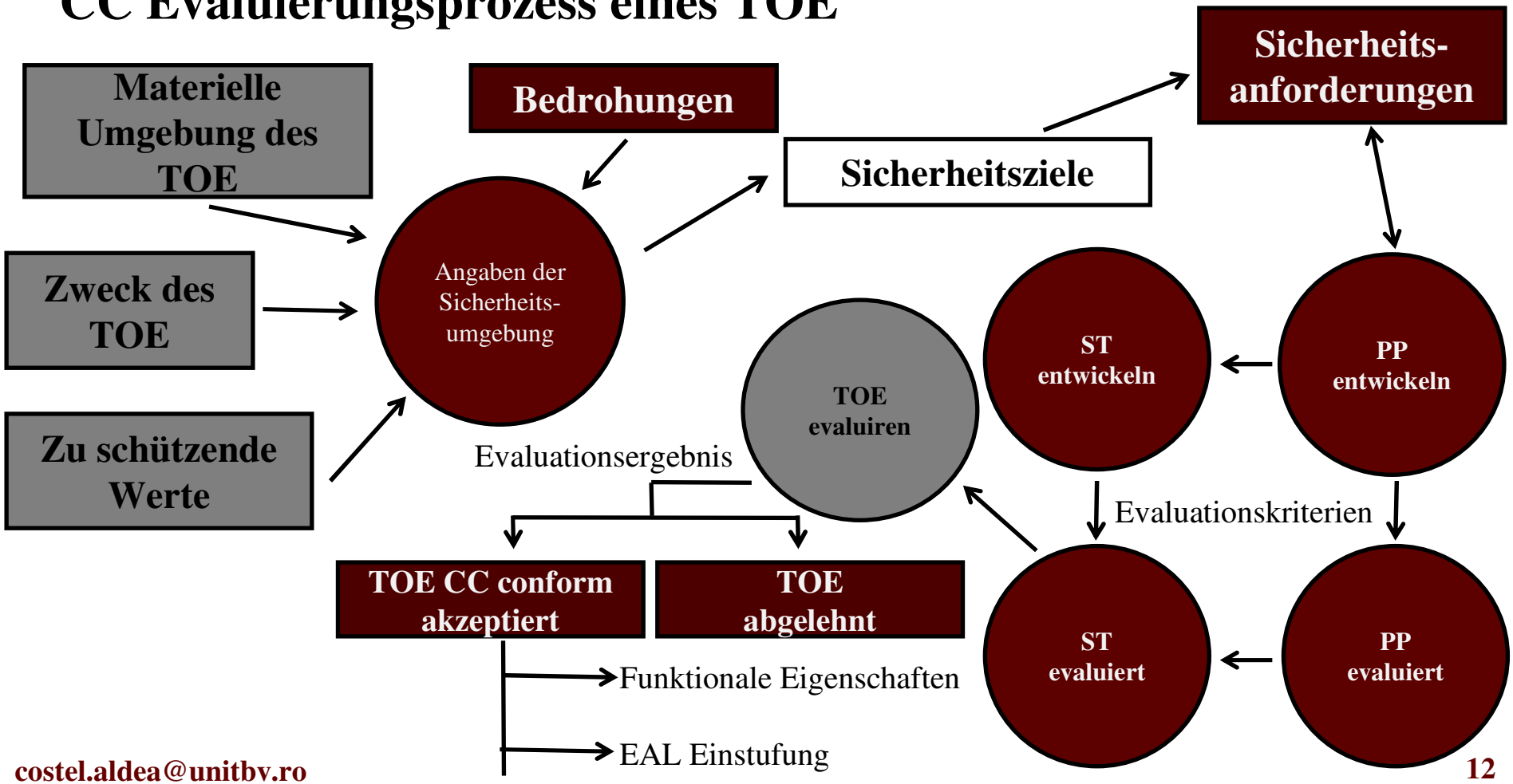
Common Criteria...

Prinzip

- Kriterien für die Evaluierung von Schutzprofilen (PP) und Sicherheitsvorgaben (ST) enthält der Teil 3
- Sicherheitsanforderungen an die Vertrauenswürdigkeit sind mittels Klassen, Familien und Komponenten definiert
- Teil 2 enthält einen Katalog vordefinierter Funktionalitäten mit Sicherheitsanforderungen; auch eigene Sicherheitsvorgaben können aufgenommen werden
- Der TOE wird nach seinen funktionalen und qualitativen Eigenschaften bewertet:
  - Funktionale Eigenschaften beziehen sich auf das Vorhandensein technischer Funktionen,
    mit deren Hilfe sichere Systeme aufgebaut werden können
  - Qualitative Eigenschaften beziehen sich auf den Entwicklungsvorgang selbst, so dass die Wirksamkeit der vorgesehenen Schutzmaßnahmen gewährleistet werden soll

6 Bewertung von IT - Sicherheit

CC Evaluierungsprozess eines TOE



6 Bewertung von IT - Sicherheit

Common Criteria...

- **Die Evaluierung des PP muss zu der Aussage „akzeptiert“ oder „abgelehnt“ führen (Kriterien in Teil 3 des Standard); im Falle der Akzeptanz ist ein PP vollständig, konsistent und technisch stimmig**
- **Ein durch Prüfung und Bewertung akzeptiertes TOE erhält ein „Label“, woraus hervorgeht, inwieweit dem TOE vertraut werden kann, die Anforderungen zu erfüllen:**
  - **Konform zu Teil 2: Funktionale Anforderungen aus Teil 2 werden erfüllt**
  - **Teil 2 erweitert:** auch funktionale Anforderungen, die nicht aus Teil 2 sind, werden erfüllt
  - **Konform zu Teil 3**: Anforderungen an die Vertrauenswürdigkeit in Form einer EAL werden erfüllt
  - **Teil 3 mit Zusatz**: Anforderungen an die Vertrauenswürdigkeit in Form einer EAL und zusätzlich andere Vertrauenswürdigkeitskomponenten aus Teil 3 werden erfüllt
  - **Teil 3 erweitert**: Anforderungen an die Vertrauenswürdigkeit in Form einer EAL und zusätzlich nicht im Teil 3 enthaltene Vertrauenswürdigkeitskomponenten werden erfüllt
- **Ist bzw. wird ein TOE Bestandteil eines installierten IT-Systems, das einer Prüfung und Bewertung unterzogen wurde, so sind diese Evaluationsergebnisse zu berücksichtigen**