XV. Sicherheitsbewertung/Zertifizierung

Beurteilung durch eine vertrauenswürdige Instanz (bescheinigt Eigenschaften) \rightarrow meist wird allerdings nicht ein Produkt, sondern der Entwicklungsprozess zertifiziert

XV.1. Gründe für eine Zertifizierung

- gesetzliche Bestimmungen (Datenschutz)
- Werbung
- überzeugt Nichtexperten
- günstigere Versicherung
- Vergleich von Produkten "einfacher"

XV.2. Common Criteria (ISO 15408)

Zertifizierungsstelle in Deutschland: BSI (Bundesamt für Sicherheit in der Informationstechnik)

- ToE (Target of Evaluation)
- ullet Protection Profile o Forderungen an das ToE
 - Descriptive Elements:
 - * worum geht es? (Smartcard, Firewall, ...)
 - * was ist das Problem, das damit gelöst werden soll?
 - Rationale (Zuordnung zwischen Bedrohungen/Angriffen und Sicherheitseigenschaften):
 - * welche Betriebsumgebung?/welches Einsatzszenario?
 - * welche Bedrohungen/Angriffe?
 - * welche Sicherheitseigenschaften?
 - Functional Requirements: funktionale Spezifikation des ToE
 - Evaluation Assurance Requirements:
 - * wie/was wird evaluiert? (es gibt umfangreiche Beispielkataloge)
 - * wie intensiv wird evaluiert?

XV.2.1. Evaluation Insurance Levels

numerische Bewertung der Prüfstrenge

- EAL 1: funktional getestet
- EAL 2: strukturell getestet

XV. Sicherheitsbewertung/Zertifizierung

- $\bullet~{\rm EAL}$ 3: methodisch getestet und überprüft
- EAL 4: methodisch entwickelt, getestet und durchgesehen
- EAL 5: semiformal entworfen und getestet
- EAL 6: semiformal verifizierter Entwurf und getestet
- EAL 7: formal verifizierter Entwurf und getestet