

IT-Sicherheitsevaluierung nach ITSEC / Common Criteria

- Was bedeutet eine IT-Sicherheitsevaluierung?
- Wie läuft sie ab / was ist das eigentlich?
- Was wird untersucht?
- Wie wird untersucht?
- Was kann sie leisten?
- Was kann sie nicht leisten?

- Eine Möglichkeit, verlässliche Aussagen hinsichtlich der Sicherheitseigenschaften von IT-Produkten zu schaffen, ist die Prüfung und Bewertung von IT-Produkten und -Systemen nach einheitlichen Kriterien durch unabhängige Stellen: Geprüfte Sicherheitsleistung, die durch ein Zertifikat bestätigt wird.

Kriterienwerke

- **ITSEC**

Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik

Anerkennungsbereich: Europa

- **Common Criteria**

Anerkennungsbereich: Europa, USA, Kanada, Australien, Neuseeland

Beteiligte Stellen

- Hersteller / Importeur
 - Stellt Evaluierungsgegenstand (EVG)
 - Liefert Evaluierungsdokumentation
- Prüfstelle
 - Prüft Evaluierungsdokumentation und EVG
 - Erstellt Prüfberichte
 - Fertigt Zertifizierungsreport
- Zertifizierungsstelle
 - Prüft Prüfberichte und Zertifizierungsreport
 - Vergibt Zertifikat

Vorgaben

- Welche Eigenschaften sollen geprüft werden?
- Man benötigt so was wie eine Spezifikation für die Evaluierung
- Was spezifiziert werden muss, wird vorgegeben
- Inhalt dennoch weitgehend vom Produkt und den Zielen des Herstellers bestimmt.
- ==> Ergebnis: Sicherheitsvorgaben

Sicherheitsvorgaben (ITSEC)

- Produktbeschreibung (oder System-Sicherheitspolitik)
 - Vorgesehene Art der Nutzung
 - Vorgesehene Einsatzumgebung
 - Angenommene Bedrohungen
 - Zusammenstellung der Sicherheitseigenschaften des Produkts
 - Alle Annahmen über die Umgebung
 - Alle Annahmen über Art der Nutzung

Sicherheitsvorgaben (ITSEC)

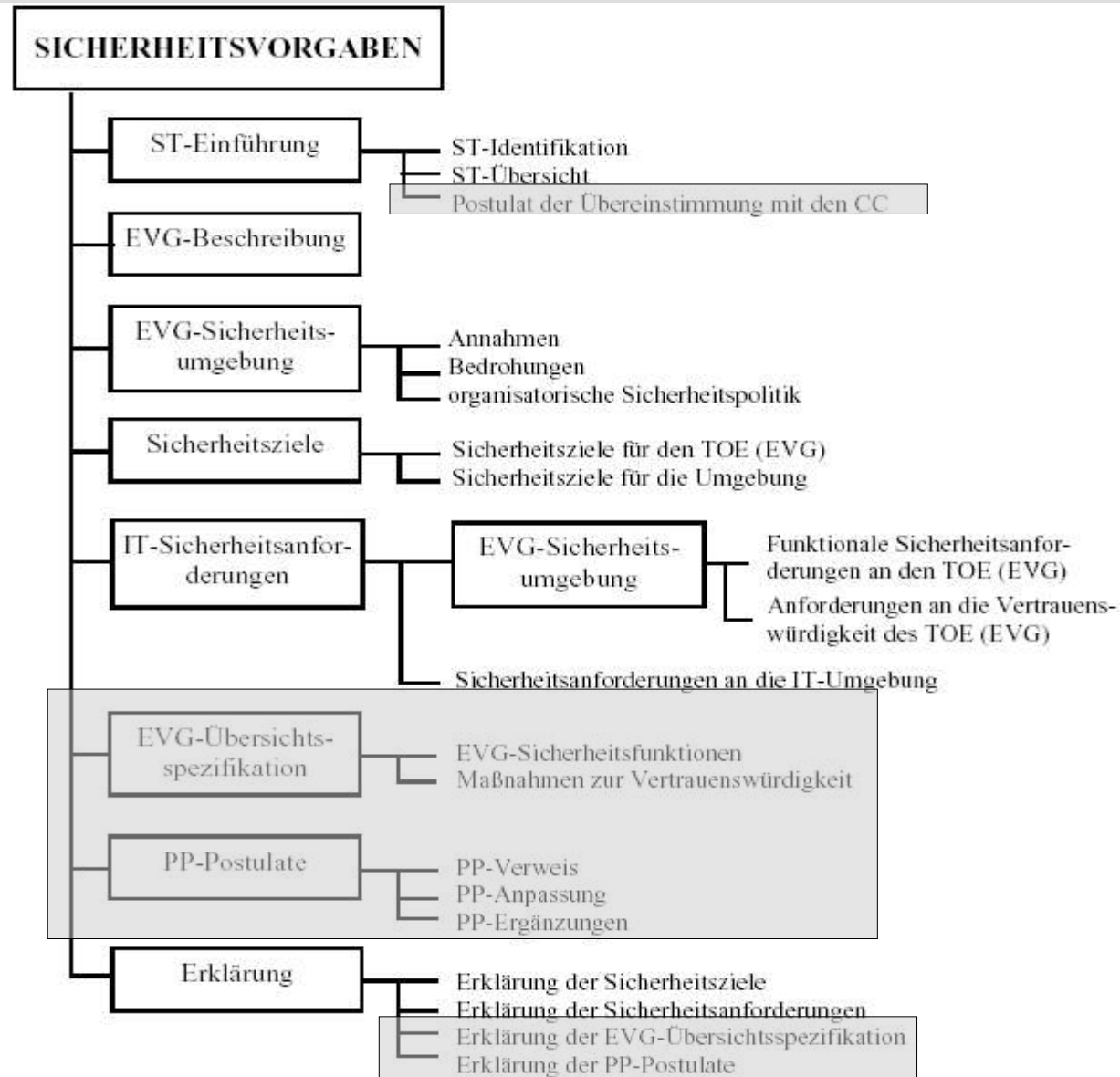
- Personelle IT-Sicherheitsmaßnahmen
- Materielle IT-Sicherheitsmaßnahmen
- Organisatorische IT-Sicherheitsmaßnahmen die notwendig sind, das Produkt einzusetzen,

Abhängigkeiten von:

- System-Hardware
- Software und / oder Firmware, die nicht zum Lieferumfang des Produkt gehören.

●
...

Sicherheitsvorgaben (CC)



Beispiel 1

Bedrohung - Sicherheitsfunktion

Bedrohung

Veränderung von Daten auf der Versichertenkarte während des Verbleibs der KVK im Kartenleser.

Sicherheitsfunktion

Es wird durch ein angemessenes Prüfsummenverfahren sichergestellt, dass eine Verfälschung der (Nutz-)Daten auf der Versichertenkarte erkannt wird und die Daten korrekt zum Kartenleser übertragen werden.

(aus: *Technische Spezifikation der Arztausstattung -portable Lesegeräte- KVT-mobil V 1.04*)

Beispiel 2

Bedrohung - Sicherheitsfunktion

Bedrohung

Fehlerhafte Übertragung der Daten von der Versichertenkarte zum Kartenleser, ohne dass dies erkannt und die Versichertenkarte durch den Kartenleser abgewiesen wird.

Sicherheitsfunktion

Bei der Übertragung der gelesenen Versichertendaten über die serielle Schnittstelle zum PC wird durch eine Prüfsumme sichergestellt, dass die Daten unverfälscht übermittelt werden.

(aus: *Technische Spezifikation der Arztausstattung -portable Lesegeräte- KVT-mobil V 1.04*)

Sicherheitsmaßnahmen

Bedrohung

Veränderung von Daten im Kartenleserspeicher durch Zugang über die in der hier vorliegenden technischen Spezifikation beschriebenen Schnittstellen oder durch fehlerhafte Bedienung des Kartenlesers.

Sicherheitsmaßnahme

Es gibt keine Möglichkeiten zum Beschreiben des Speicherbereichs der Versichertendaten im Kartenleser durch externen Programm-Aufruf oder durch die äußeren Bedienelemente oder Schnittstellen.

(aus: *Technische Spezifikation der Arztausstattung -portable Lesegeräte- KVT-mobil V 1.04*)

Organisatorische Maßnahmen

Bedrohung

Unbefugtes Sichtbarmachen oder Abrufen der im Kartenleserspeicher abgelegten Krankenversichertendaten.

Sicherheitsfunktion

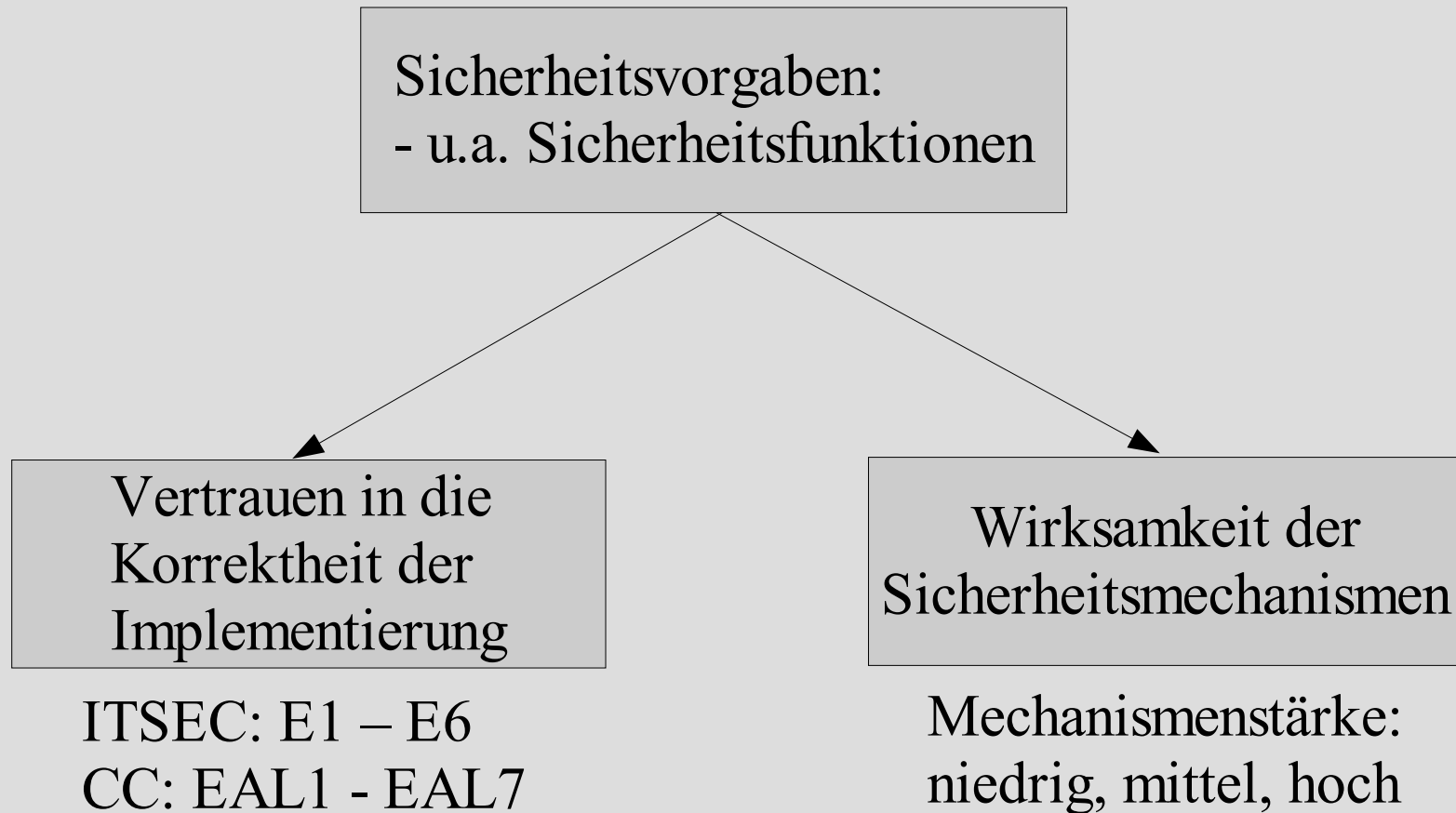
Es ist ein Schutz gegen unbefugte Nutzung der schützenswerten Funktionen bzw. Daten vorzusehen. Benutzer werden identifiziert und zur Nutzung autorisiert. Es erhalten nur berechnigte Benutzer Zugang zu den geschützten Funktionen.

Organisatorische Maßnahme

Die Zugangskarten oder Kennwörter und das Lesegerät sind getrennt und geschützt gegen den Zugriff von Unbefugten (Diebstahlgeschützt) und Missbrauch zu verwahren.

(aus: *Technische Spezifikation der Arztausstattung -portable Lesegeräte- KVT-mobil V 1.04*)

Aufteilung



Korrektheitsaspekte

Vertrauen in die
Korrektheit der
Implementierung

Implementierung
der
Sicherheitsfunktionen

Entwicklungsumfeld

Bedienen
Konfigurieren
Auslieferung

Evaluierungsstufen

ITSEC

CC

E1

EAL2

darlegen informell, geringe Prüftiefe

E2

EAL3

E3

EAL4

beschreiben

E4

EAL5

formales Sicherheitsmodell

E5

EAL6

erklären

E6

EAL7

größte Prüftiefe,
umfassende Konfigurationskontrolle (alles)

E2

- Architekturentwurf
 - Grundsätzliche Struktur
 - Externe Schnittstellen
 - Sicherheitsspezifische und andere Komponenten
- Feinentwurf
 - Realisierung sicherheitsspezifischer und -relevanter Funktionen darlegen
 - Spezifikation der Sicherheitsmechanismen
- Testdokumentation
 - Testpläne, -ziele, -verfahren und -ergebnisse
 - Testprogramme und -werkzeuge

E2 Architekturentwurf

Anforderungen an Inhalt und Form

Diese Beschreibung muß die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG darlegen. Sie muß Hard- und Firmware darlegen, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind. **Sie muß die Aufteilung des EVG in sicherheitsspezifische und andere Komponenten darlegen.**

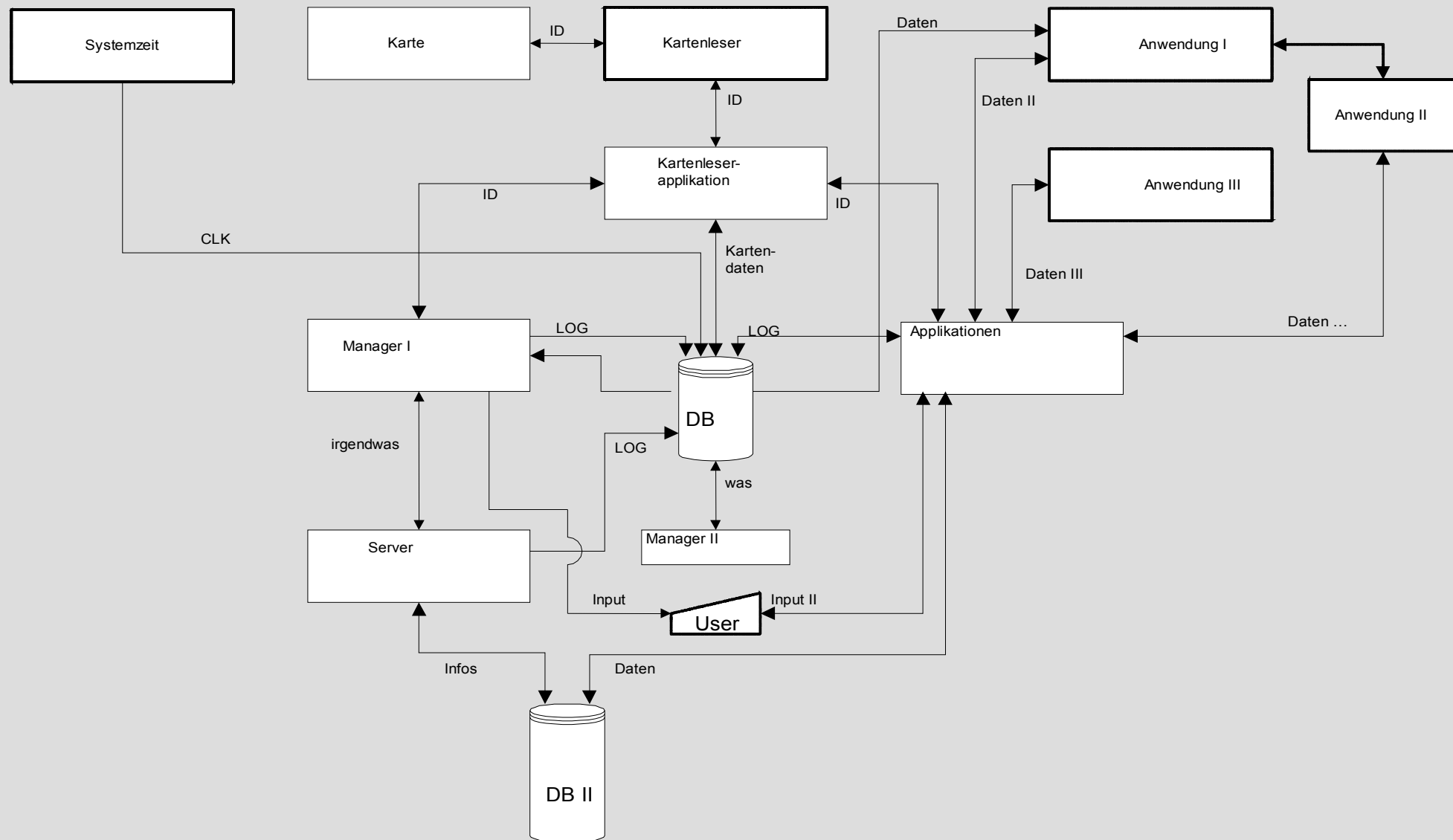
Anforderungen an Nachweise

Die Beschreibung der Architektur muß darlegen, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden. **Sie muß darlegen, wie die Trennung in sicherheitsspezifische und andere Komponenten erreicht wird.**

Aufgaben des Evaluators

Es ist zu prüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. **Es ist zu prüfen, ob die Trennung von sicherheitsspezifischen und anderen Komponenten wirksam ist.**

AE Blockdiagramm



E2 / 2

- Konfigurationskontrolle
 - Konfigurationskontrollsystem
 - Konfigurationsliste aller Basiskomponenten
 - Eindeutige Identifikation, auch der Dokumentation
- Entwicklungsumgebung
 - Schutzmaßnahmen (Integrität und Vertraulichkeit des EVG)
 - Materielle, organisatorische und personelle Sicherheitsmaßnahmen beim Entwickler

E2 / 3

- Benutzerdokumentation
 - Darlegung der relevanten sicherheitsspezifischen Funktionen
 - Richtlinien für ihre sichere Anwendung
 - Strukturierter Aufbau
- Systemverwalterdokumentation zusätzlich
 - Unterscheidung Funktionen zur Kontrolle von Parametern und zur Abfrage von Informationen
 - Darlegung aller kontrollierbarer Sicherheitsparameter
 - Darlegung aller Typen sicherheitsrelevanter Ereignisse
 - Anweisungen zur Installation und Konfiguration

E2 / 4

- Auslieferung und Konfiguration
 - Auswirkungen einzelner Konfigurationen auf die Sicherheit
 - Verfahren der Auslieferung und Systemgenerierung
 - Protokollierung aller Generierungsoptionen
 - Verwendung eines vom BSI zugelassenen Auslieferungsverfahrens zur Garantie der Authentizität des Evaluierungsgegenstands
- Anlauf und Betrieb
 - Prozeduren für sicheren Anlauf und Betrieb
 - Ausschaltbare sicherheitsspezifische Funktionen bei Anlauf, Betrieb oder Wartung?
 - Bei sicherheitsspezifischer Hardware: Diagnoseeinrichtung erforderlich

E2 - E4, Delta

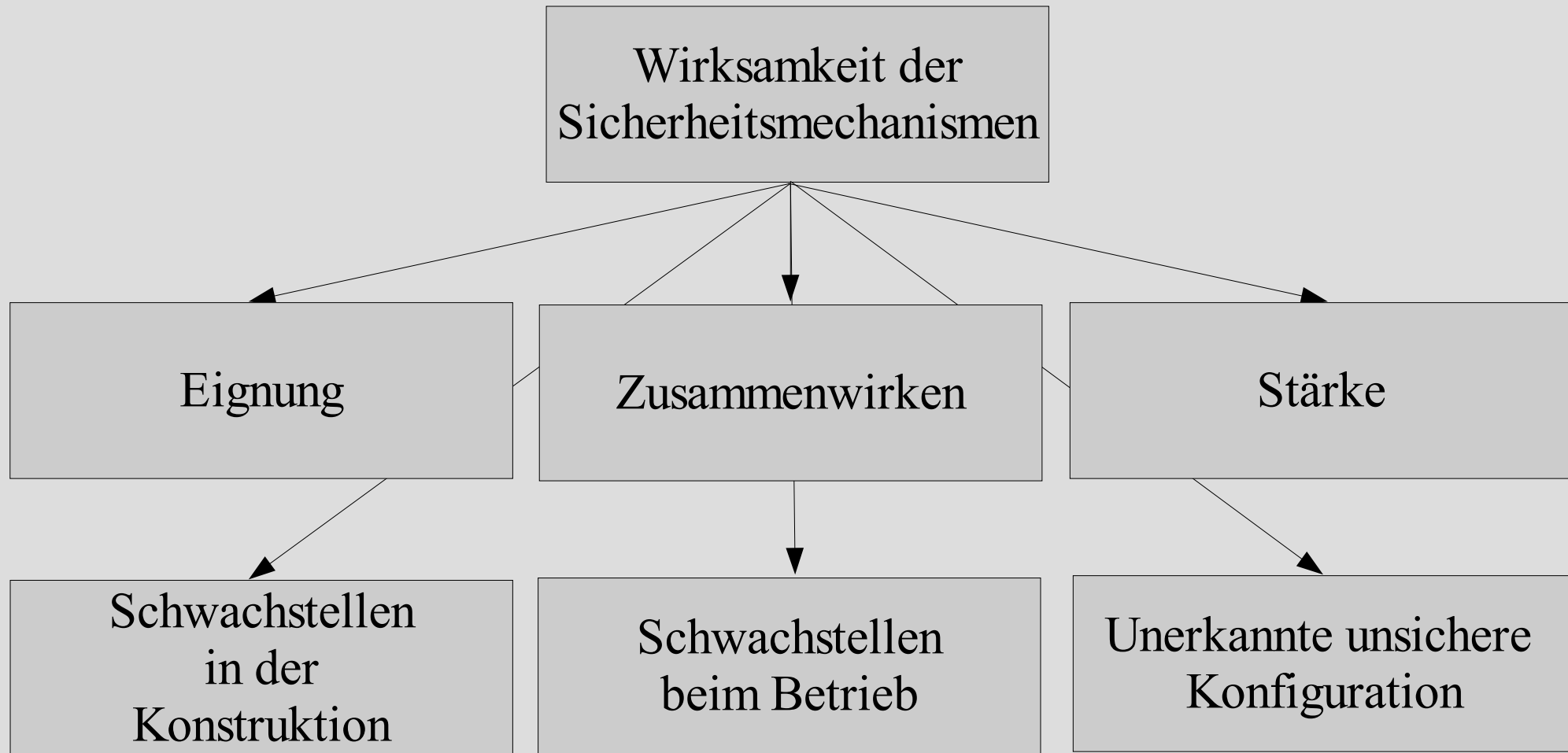
- SV: formales Sicherheitsmodell oder Verweis auf ein solches
- AE: Semiformaler Architekturentwurf
- FE: Semiformaler Feinentwurf
- IMP: Zuordnung Source <-> FE-Komponenten
Begründung warum Testabdeckung ausreicht
- KK: Werkzeugunterstütztes Konfigurationskontrollsystem
(Überwachung und Protokollierung von Änderungen)
- Com: Sprachen nach Standard
Dokumentierung der Implementierungsoptionen

- Beschreiben statt darlegen

E6 Bsp.

- SV: Formale Spezifikation der Sicherheitsfunktionen
 - AE: Formaler Architekturentwurf
 - FE: Semiformaler Feinentwurf
 - IMP: Sourcen der Laufzeitbibliotheken
 - TST: Übereinstimmung Tests \leftrightarrow formale Spezifikation
 - KK: Alle Werkzeuge unter Konfigurationskontrolle
 - A&K: Konfigurationsoptionen formal definiert
-
- Erklären statt beschreiben

Wirksamkeitsaspekte



Eignung und Zusammenwirken

Grundlage:

Bedrohungen (Sicherheitsvorgaben)

Durch Hersteller durchzuführen und zu dokumentieren:

Analyse, ob die sicherheitsspezifischen Funktionen und Mechanismen den identifizierten Bedrohungen auch tatsächlich entgegenwirken

und

Analyse aller möglichen Beziehungen zwischen den sicherheitsspezifischen Funktionen und Mechanismen

(keine Konflikte zwischen sicherheitsspezifischen Funktionen oder Mechanismen, kein Entgegenwirken, keine ungeschützten “Lücken”)

Stärke

Beurteilung der Widerstandsfähigkeit gegen direkten Angriff

Nicht überwindbare Mechanismen (z.B. Zugangskontrolle über Rechte) werden nicht untersucht

Überwindbare Mechanismen (Verschlüsselung, Hash-Funktionen, aber auch z.B. materielle Sicherheitsmechanismen ...)
werden analysiert und eingestuft in Stärke “niedrig”, “mittel”, “hoch”

Stärkekriterien

Berücksichtigt wird bei der Beurteilung der Bedarf an bestimmten Ressourcen:

Benötigte Zeit

Minuten

Tage

Monate / Jahre

Konspiratives Zusammenwirken

z.B. mit Benutzer

mit Administrator

Ausrüstung

ohne Equipment

allgemein verfügbare Ausrüstung

Spezialausstattung

Schwachstellen

- Konstruktive Schwachstellen z.B.
 - Krypto-Modul ohne Temperaturüberwachung
 - Ausgabe eines eingegebenen Passworts bei der Eingabe im Klartext
- Operationelle Schwachstellen z.B.
 - Kritische Operationen, die unterbrochen werden können und den EVG in einen unsicheren Zustand überführen
- Entgegenwirken durch technische, personelle, organisatorische oder materielle Sicherheitsmaßnahmen außerhalb des EVG

ITSEC Funktionsklassen

Standards für Sicherheitsfunktionalität

Vorbild TCSEC (Orange Book)

F-C1, F-C2, F-B1, F-B2, F-B3

spezielle Sicherheitsziele z.B. Integrität oder Verfügbarkeit

F-IN, F-AV, F-DI, F-DC, F-DX

Beispiel F-C1

Identifikation und Authentisierung

Zugriffskontrolle

CC Protection Profiles

Abstrakt gehaltene Sicherheitsvorgaben

Beschreibung des EVG

Beschreibung der Sicherheitsumgebung

Annahmen zum Betrieb

Bedrohungen

Sicherheitspolitik

Sicherheitsziele (EVG und Umgebung)

IT-Sicherheitsanforderungen

Funktionale Sicherheitsanforderungen

Anforderungen an die Vertrauenswürdigkeit

CC Protection Profiles / 2

Protection Profiles

- können evaluiert werden
- dienen als Standard für bestimmte Produkte oder Systeme
(z.B. Sesam Vitale
oder “Protection Profile Smart Card IC with
Multi-Application Secure Platform”)
- müssen immer erst zu Sicherheitsvorgaben erweitert und konkretisiert werden

Links

- Bundesamt für Sicherheit in der Informationstechnik
<http://www.bsi.bund.de/>
- Communications-Electronics Security Group (CESG)
<http://www.cesg.gov.uk>
- Löher EDV-Beratung
<http://loeher.net>