Fachhochschule Wedel

Seminarfacharbeit

über

IT-Sicherheit – Zertifizierungen

im

Wintersemester 2012/ 2013

zum

Seminar IT-Sicherheit

Autor:	Patrick Delfs
Matrikelnummer:	9028
Fachbereich:	Wirtschaftsinformatik

Betreuender Dozent:	Prof. Dr. Gerd Beuster

Inhaltsverzeichnis

Einleitung

In der heutigen Zeit befinden wir uns in einer globalen Informationsgesellschaft. Immer mehr Aufgaben, besonders im Bereich der Kommunikation und Datenverarbeitung, werden von informationstechnischen Systemen völlig selbstständig bearbeitet. Für uns, den Anwender, ist es bereits ein fester Bestandteil unseres Alltags geworden. Die immer komplexer werdenden Abläufe sind ohne fundiertes Fachwissen nicht mehr nachzuvollziehen. Durch die Risiken, die die Nutzung solcher IT-Produkte mit sich bringen, steigt ebenfalls das Sicherheitsbewusstsein des Anwenders. Um aber das Vertrauen des Anwenders in die IT-Produkte zu gewährleisten, muss das IT-Produkt über bestimmte Sicherheitseigenschaften verfügen. Bei einigen IT-Produkten, zum Beispiel bei IT-Produkten zur Erstellung digitaler Signaturen, ist es bereits sogar gesetzlich festgelegt, dass sie bestimmten Sicherheitsstandards genügen müssen. Um diese Sicherheitseigenschaften objektiv zu bewerten, wurden Standardwerke zur Prüfung und Bewertung der Sicherheit von IT-Produkten/ -Systemen entworfen. Durch die Evaluation eines IT-Produktes/- Systems durch eines solchen Standardwerkes soll gewährleistet werden, dass der Evaluierungs-gegenstand (EVG) im wesentlichen nach den Sicherheitskriterien Vertraulichkeit, Integrität und Verfügbarkeit geschützt ist.[1] Im Laufe der Zeit wurden verschiedene Kriterienkataloge für Evaluationen entwickelt.

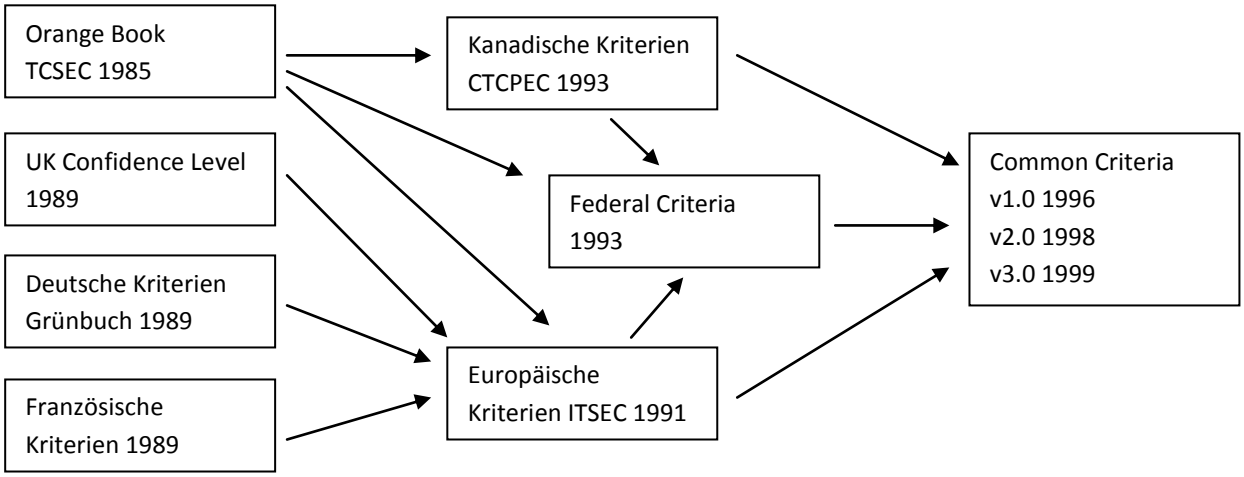

Abbildung 1: Übersicht und Abhängigkeiten der verschiedenen Kriterienkataloge

Die *Trusted Computer System Evaluation Criteria* (TCSEC) sind die ältesten Kriterien zur Bewertung der IT-Sicherheit aus dem Jahr 1985. Sie wurden in den USA entwickelt und werden auch Orange Book genannt.[2] Vier Jahre später entwickelte man in Europa ebenfalls nationale Kriterien, darunter die *UK Confidence Level* aus Großbritannien, die *deutschen IT-Kriterien* und die *französischen Kriterien*. Aus den bereits bestehenden Werken beschloss

man 1991 in Europa die europäischen Kriterien, die ITSEC, zu entwerfen.[3] Zusammen mit den ITSEC-Kriterien bildeten die zwei Jahre später entworfenen *Kanadischen Kriterien* (CTCPEC) und *Federal Criteria* (FC) die Grundlage für die im Jahr 1996 entstandenen Common Criteria (CC). Die CC sind ein internationaler Kriterienkatalog und bilden den heutigen Standard, da er fortlaufend weiterentwickelt wird.[4] Im Rahmen dieser Ausarbeitung wird ausschließlich auf die europäischen ITSEC-Kriterien und die internationalen Common Criteria eingegangen.

Zertifizierungsprozess[5]

Im Folgenden wird auf den Ablauf von IT-Sicherheitszertifizierungen und die Aufgaben der daran beteiligten Parteien in Deutschland eingegangen. In Deutschland sind drei Parteien am Zertifizierungsprozess beteiligt. Diese sind der Antragssteller/ Hersteller, die Prüfstelle und die Zertifizierungsstelle.

Eine Zertifizierung eines zu prüfenden IT-Produktes/ -Systems wird auf Antrag des Antragsstellers/ Herstellers bei der Zertifizierungsstelle durchgeführt. Danach wählt der Antragssteller/ Hersteller eine Prüfstelle aus und reicht dort sein zu prüfendes IT-Produkt/ -System zusammen mit den Evaluierungsdokumenten[6] ein.

Die Prüfstelle ist ein beliebiges vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziertes Unternehmen. Nach dem Erhalt des zu prüfenden IT-Produktes/ -Systems und der Evaluierungsdokumente wird die Prüfung durchgeführt. Der Prüfungsprozess wird dabei von einem Mitarbeiter der Zertifizierungsstelle begleitet. Nach der Beendigung der Prüfung des IT-Produktes/ -Systems wird ein Prüfungsbericht angefertigt, welcher dem Antragssteller/ Hersteller und der Zertifizierungsstelle ausgehändigt wird.

Die Zertifizierungsstelle für IT-Produkte/ -Systeme in Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik. Mit Hilfe des Prüfungsberichtes von der Prüfstelle wird ein Zertifizierungsreport vom BSI erstellt, in dem Einzelheiten zur Bewertung, Hinweise und gegebenenfalls Auflagen für den Anwender des IT-Produktes/ -Systems festgehalten wird. Die BSI-Zertifizierungsstelle übergibt dem Antragssteller/ Hersteller nach erfolgreicher Prüfung das IT-Sicherheitszertifikat und den Zertifizierungsreport. Mit Einverständnis des Antragsstellers/ Herstellers, wird der Zertifizierungsreport mit Sicherheitszertifikat auf der Internetseite des BSI[7] veröffentlicht.

Information Technology Security Evaluation Criteria (ITSEC)

Einführung

Die ITSEC sind 1991 von den Ländern Deutschland, Niederlande, Frankreich und Großbritannien in einer Arbeitsgruppe der EU-Kommission erarbeitet worden. Die Grundlage der ITSEC sind die TCSEC, die UK Confidence Level, die französischen Kriterien und die deutschen IT-Kriterien aus dem Jahr 1989.[3]

Inhalt der ITSEC

Funktionsklassen

Der ITSEC-Kriterienkatalog legt zehn verschiedene Funktionsklassen fest. Funktionsklassen umfassen eine Menge von Sicherheitsgrundfunktionen, die die Sicherheitsanforderungen einer Klasse von IT-Systemen abdeckt, und dienen zum Erreichen der Sicherheitsziele des Evaluierungsgegenstandes. Die Funktionsklassen des ITSEC leiten sich aus den deutschen IT-Kriterien ab. Es ist allerdings ebenso möglich diese Funktionen individuell zu spezifizieren, ohne auf die vordefinierten Funktionsklassen zurückzugreifen.[3, 8]

Bewertung der Qualität

Die Bewertung eines IT-Produktes/ -Systems hinsichtlich der Qualität wird in zwei verschiedene Bereiche aufgeteilt. Zum Einen in die Bewertung der korrekten Funktionsweise des Evaluierungsgegenstandes und zum Anderen in die Bewertung der Wirksamkeit der eingesetzten Sicherheitsmechanismen.[3]

Bewertung der Sicherheitsmechanismen

Zur Bewertung der Stärke der Sicherheitsmechanismen existieren die drei verschiedenen Stufen *niedrig*, *mittel* und *hoch.* Die Stufe *niedrig* sagt aus, dass der Sicherheitsmechanismus zur Abwehr von unabsichtlichen Verstößen gegen die Sicherheitsanforderungen geeignet ist. Ein Mechanismus der Stufe *mittel* bietet einen Schutz gegen absichtliche Verstöße, kann jedoch mit mittlerem Aufwand oder mit Einsatz von aufwändigen Hilfsmitteln von einer Person mit normalen Kenntnissen überwunden werden. Als *hoch* wird ein Sicherheitsmechanismus eingeschätzt, wenn dieser beim derzeitigen Stand der Technik nur mit sehr großem Aufwand und sehr aufwändigen Hilfsmitteln zu überwinden ist.[9]

Bewertung der korrekten Funktionsweise[10]

Zur Bewertung der korrekten Funktionsweise eines Evaluierungsgegenstandes wurden sieben Evaluationsstufen eingeführt. Dies sind die Stufen E0 - E6, welche die Vertrauenswürdigkeit der korrekten Funktionalität eines evaluierten IT-Produkts/ -Systems widerspiegelt. In der folgenden Abbildung sieht man die verschiedenen Evaluationsstufen und die Anforderungen jeder einzelnen Stufe.

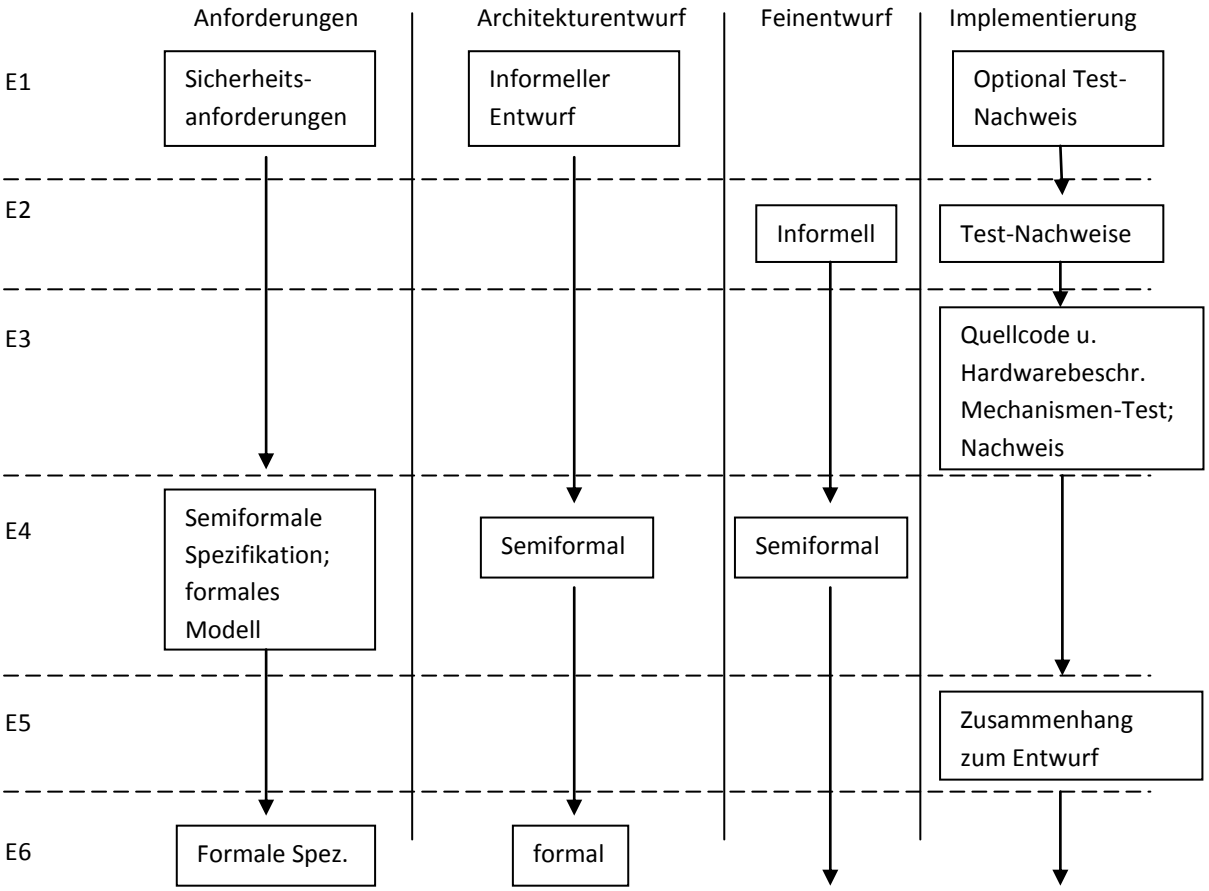

Abbildung 2: Evaluationsstufen der ITSEC-Kriterien

Die Evaluationsstufe E0 wird hier nicht mit aufgeführt, weil sie einen unzureichenden Grad des Vertrauens ausdrückt. Für die Evaluationsstufe E1 benötigt man eine Formulierung der Sicherheitsanforderungen für den Evaluationsgegenstand. In den Sicherheitsanforderungen stehen die Bedrohungen eines IT-Produkts/ -Systems mit den dazugehörigen Sicherheitsstrategien zur Beseitigung der Bedrohung. Neben den optional durchzuführenden funktionalen Tests, welche eine Testdokumentation mit Testzielen, -verfahren und –ergebnissen beinhaltet, ist eine informelle Beschreibung des Architekturentwurfs, bezogen auf die Funktionalität der einzusetzenden Sicherheitsmechanismen erforderlich.

Die Stufe E2 erfordert zusätzlich zur Stufe E1 eine informelle Beschreibung des Feinentwurfs des Evaluierungsgegenstandes. Dies ist eine Beschreibung aller sicherheitsspezifischen und -relevanten Funktionen. Außerdem ist eine Testdokumentation mit Bewertung der Testergebnisse jetzt Pflicht.

Die E3-Einstufung hat zusätzliche Anforderungen an die Implementierung. Hierbei wird eine Beschreibung, die den Zusammenhang und die Übereinstimmung zwischen Quellcode und den Hardware-Konstruktionszeichnungen und den informell beschriebenen Feinentwurf wiedergibt, gefordert.

Zur erfolgreichen Evaluation eines IT-Produktes/ -Systems in der Stufe E4 benötigt man ein formales Model mit Beschreibung der Sicherheitseigenschaften des Evaluierungsgegenstandes. Außerdem wird nun eine semiformale Beschreibung des Architekturentwurfs und des Feinentwurfs gefordert. Semiformale Hilfsmittel sind Spezifikationssprachen wie SDL oder grafische Darstellungen wie Entity-Relationship-Diagramme oder Datenflussdiagramme.

Die Evaluationsstufe E5 hat nun das Ziel von beschreibenden zu erklärenden Dokumenten zu gelangen. Dabei spielt also nicht nur die Frage wie man etwas umgesetzt hat eine Rolle, sondern auch warum man es so umgesetzt hat. Hierbei wird zusätzlich noch eine Erklärung zwischen dem Zusammenhang des Quellcodes und des Feinentwurfs gefordert.

Die letzte und höchste Stufe E6 fordert nun eine formale Spezifikation der Sicherheitsanforderungen und des Architekturentwurfs. Formale Hilfsmittel sind Spezifikationssprachen wie SPECTRUM.

Die Bewertung der Qualität des Evaluierungsgegenstandes besteht aus der Zusammensetzung der Bewertung der korrekten Funktionsweise und der Bewertung der Wirksamkeit der eingesetzten Sicherheitsmechanismen. Dieses Tupel sieht zum Beispiel folgendermaßen aus: (E3, hoch).

Einige IT-Produkte/ -Systeme müssen aufgrund gesetzlicher Vorgabe eine bestimmte Zertifizierungsstufe erreichen. Das deutsche Signaturgesetz besagt zum Beispiel, dass IT-Produkte/ -Systeme, welche Komponenten zur Erzeugung von Signaturschlüsseln enthalten, eine Zertifizierungsstufe von (E4, hoch) besitzen müssen.[11]

Fazit

Die ITSEC-Kriterien stellen einen europaweiten Standard zur Zertifizierung von IT-Produkten/ -Systemen dar. Sie sind die europäische Alternative zu den CC. Das SOGIS-MRA[12], ein

europäisches Abkommen zur gegenseitigen Anerkennung der ITSEC-Zertifizierungen, wurde erstmals am 03. März 1998 veröffentlicht. Die gegenseitige Anerkennung von Zertifikaten ist bis zu einer Stufe von (E3, niedrig) festgelegt. Hierdurch wird eine Mehrfachzertifizierung von IT-Produkten/ -Systemen innerhalb von Europa vermieden, was einen verstärkten Wettbewerb auf dem europäischen Markt zur Folge hat.[13, 31]

Eine Weiterentwicklung gegenüber den TCSEC-Kriterien ist die Trennung der Bewertung der Qualität in die Bewertung der korrekten Funktionsweise und die Bewertung der Sicherheitsmechanismen. Die deutschen IT-Kriterien hatten diese Trennung zwei Jahre zuvor ebenfalls schon berücksichtigt, allerdings kommt die Bewertung der Sicherheitsmechanismen in der Qualitätsstufe nicht zum Ausdruck.[14]

Nachteilig sind die in Verbindung mit der Evaluation entstehenden hohen Kosten. Das Ergebnis besitzt, im Vergleich zum hohen Aufwand, eine zu geringe Aussagekraft. Ein weiterer Nachteil ist, dass die Zertifikate der nach ITSEC evaluierten IT-Produkte/ -Systeme weltweit nicht anerkannt werden und somit ein Einsteigen auf dem weltweiten Markt mit einem ITSEC-Zertifikat praktisch nicht möglich ist.[15]

Common Criteria for Information Technology Security Evaluation (CC)

Einführung

Mit den CC wurde ein internationaler Standard entwickelt, mit dem man die Bewertung der IT-Sicherheit nahezu aller IT-Produkte/ -Systeme ermöglicht. Sie sind eine Weiterentwicklung und Harmonisierung der europäischen ITSEC, der TCSEC, der Federal Criteria (FC) der USA, sowie der kanadischen Kriterien (CTCPEC). Sie wurden im Dezember 1999 durch die internationale Standardisierungsorganisation (ISO) als internationale Norm ISO/IEC 15408 veröffentlicht und werden kontinuierlich weiterentwickelt.[16]

Die CC sind in drei verschiedene Teile gegliedert. Der erste Teil ist *Einführung und allgemeines Modell (Introduction and General Model)*, der zweite Teil *Funktionale Sicherheitsanforderungen (Security Functional Requirements)* und der dritte Teil *Anforderungen an die Vertrauenswürdigkeit (Security Assurance Requirements)*.[17]

Inhalt der CC

Einführung und allgemeines Modell[18]

Im ersten Teil der CC ist aufgeführt, welche Dokumente für eine Evaluation vorzulegen sind. Ebenso ist es von Vorteil ein Schutzprofil (protection profile (PP)) zu erstellen (siehe

Abschnitt Schutzprofil), in dem die Sicherheitsanforderungen des Evaluierungsgegenstandes (Target of Evaluation (TOE)) aufgelistet sind. Aus den Sicherheitsanforderungen werden anschließend Sicherheitsvorgaben[19] entwickelt. Ohne ein Schutzprofil werden die Sicherheitsvorgaben direkt formuliert. Eine Evaluierung eines IT-Produktes/ -Systems nach den CC erfolgt dabei in zwei Schritten. Als erstes erfolgt die Validierung des Schutzprofils bzw. der Sicherheitsvorgaben. Der zweite Schritt ist die Überprüfung, ob der Evaluierungsgegenstand die funktionalen Sicherheitsanforderungen und die Anforderungen an die Vertrauenswürdigkeit erfüllt.[20]

Funktionale Sicherheitsanforderungen[21]

Der zweite Teil besteht aus den funktionalen Sicherheitsanforderungen der CC, welche eine Beschreibung der Kriterien und Anforderungen an Sicherheitsgrundfunktionen sind und somit den Zweck der Funktionsklassen bei den ITSEC-Kriterien erfüllen. Mit diesen Sicherheitsanforderungen kann man das IT-Produkt/ -System auf standardisierte Weise beschreiben.

Die Sicherheitsanforderungen sind wie folgt strukturiert:

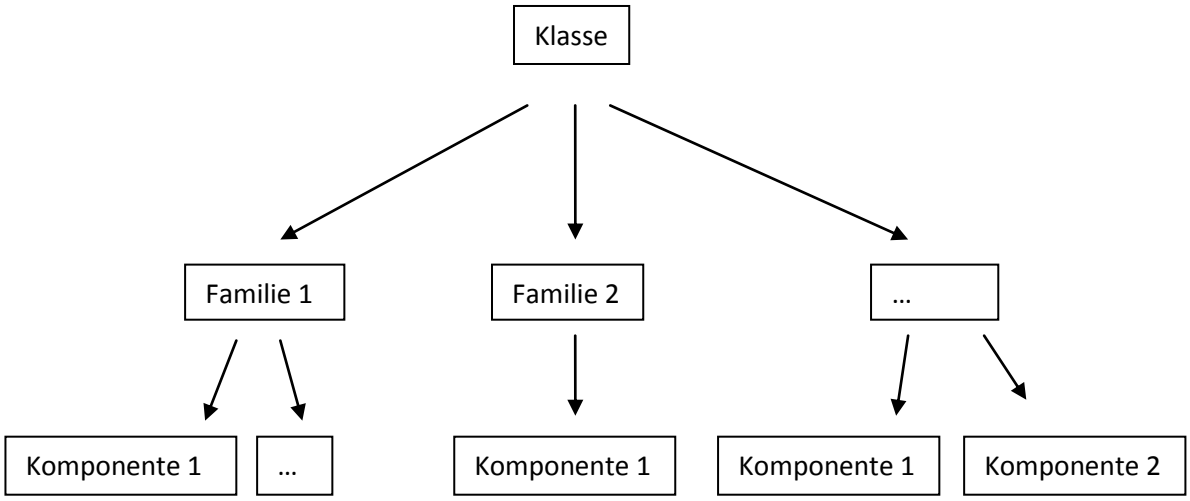

Abbildung 3: Struktur der funktionalen Sicherheitsanforderungen der CC

Es gibt verschiedene Funktionsklassen. Eine Funktionsklasse ist hier als Klasse (Classes) bezeichnet. Innerhalb einer Funktionsklasse gibt es eine oder mehrere Familien (Families). Die Familien wiederrum sind in mindestens einer Komponente (Component) unterteilt, in

der die einzelne funktionale Sicherheitsanforderung beschrieben ist. In der folgenden Abbildung 4 wird eine sehr grobe Beschreibung der einzelnen Funktionsklassen gegeben.

Klasse	Aufgabe/ Funktion
FAU	Die Klasse FAU steht für die Sicherheitsprotokollierung (Security Audit). Hierzu gehört das Erkennen, Aufzeichnen, Speichern, Analysieren von Informationen im Zusammenhang mit sicherheitsrelevanten Aktivitäten.
FCO	Die Klasse FCO befasst sich mit der Kommunikation (Communication) und beinhaltet zwei Familien, die sich mit der Identitätssicherstellung der am Datenaustausch beteiligten Seiten befassen.
FCS	Für Sicherheitsanforderungen zur kryptografischen Unterstützung (Cryptographic Support) gibt es die Klasse FCS, welche in die zwei Familien FCS_CKM und FCS_COP gegliedert ist. FCS_CKM steht für kryptografisches Schlüsselmanagement (Cryptographic key management) und FCS_COP für kryptografischen Betrieb (Cryptographic operation).
FDP	Die Klasse FDP enthält Sicherheitsanforderungen zum Schutz der Benutzerdaten (User Data Protection) in einem Evaluierungsgegenstand während des Imports, Exports und der Speicherung.
FIA	Die Klasse FIA beschäftigt sich mit Sicherheitsanforderungen für die Identifikation und Authentifizierung zur Einrichtung und Verifizierung angegebener Benutzeridentitäten (Identification and authentication).
FMT	Die Klasse FMT befasst sich mit dem Sicherheitsmanagement (Security management) und dient zur Spezifikation des Managements des Evaluierungsgegenstandes.
FPR	Um einen Schutz des Benutzers gegen

	Enthüllung und Missbrauch seiner Identität (Privacy) bereitzustellen, gibt es die Sicherheitsanforderungen der Klasse FPR.
FPT	Die Klasse FTP dient zum Schutz der Sicherheitsfunktionen des Evaluierungsgegenstandes (Protection of the TOE security function (TSF)).
FRU	Die drei Familien der Klasse FRU stellen Sicherheitsanforderungen zur Unterstützung der Verfügbarkeit geforderter Betriebsmittel (Resource Utilisation), wie zum Beispiel Rechenfähigkeiten und Speicherfähigkeiten bereit.
FTA	Die Klasse FTA enthält Anforderungen zur Kontrolle der Einrichtung einer Benutzersitzung (TOE Access).
FTP	FTP und die Familien dieser Klasse enthalten Sicherheitsanforderungen an einen vertrauenswürdigen Kommunikationspfad zwischen den Benutzern und den Sicherheitsfunktionen (Trusted Path/ Channels).

Abbildung 4: Übersicht über die CC-Funktionsklassen

Anforderungen an die Vertrauenswürdigkeit

Der dritte und letzte Teil der CC enthält Kriterien, um das Schutzprofil und die Sicherheitsvorgaben zu evaluieren. Falls Änderungen nach der Evaluation vorgenommen werden, gibt es ein Konzept (Assurance Maintenance[34]), welches beschreibt, unter welchen Voraussetzungen keine Re-Zertifizierung stattfinden muss.[21] Durch die Evaluierung wird geprüft, ob die vom Hersteller angegebene Sicherheitsfunktionalität wirksam ist. Mit dem erfolgreichen Abschluss einer Evaluierung kann der Anwender dann ein gewisses Maß an Vertrauen in die Sicherheit des IT-Produkts/ -Systems setzen.[36]

Die Struktur der Sicherheitsanforderungen an die Vertrauenswürdigkeit ist wie bereits zuvor bei den funktionalen Sicherheitsanforderungen in Klassen, Familien und Komponenten gegliedert. Die Sicherheitsanforderungen an die Vertrauenswürdigkeit können, falls sie nicht auf den Evaluierungsgegenstand anwendbar sind, individuell erweitert werden.

Hier folgt nun ein Überblick über die verschiedenen Vertrauenswürdigkeitsklassen:

Klasse	Familie	Abkürzung
ADV: Entwicklung	Funktionale Spezifikation	ADV_FSP
	Darstellung der Implementierung	ADV_IMP
	Interna der EVG-Sicherheitsfunktionen	ADV_INT
	Sicherheitsmodell	ADV_SPM
	Sicherheitsarchitektur	ADV_ARC
	EVG-Entwurf	ADV_TDS
AGD: Handbücher	Benutzerhandbuch	AGD_OPE
	Vorbereitende Verfahren	AGD_PRE
ALC: Lebenzyklus-Unterstützung	Sicherheit bei der Entwicklung	ALC_DVS
	Fehlerbehebung	ALC_FLR
	Lebenszyklus-Beschreibung	ALC_LCD
	Werkzeuge und Techniken	ALC_TAT
	Funktionen des Konfigura-tionsmanagements	ALC_CMC
	Umfang des Konfigura-tionsmanagements	ALC_CMS
	Auslieferung	ALC_DEL
ATE: Testen	Testabdeckung	ATE_COV
	Testtiefe	ATE_DPT
	Funktionale Tests	ATE_FUN
	Unabhängiges Testen	ATE_IND
AVA: Schwachstellenbewertung	Schwachstellenanalyse	AVA_VLA
APE: Schutzprofil-Evaluierung	Schutzprofil-Einführung	APE_INT
	Übereinstimmung der Ansprüche	APE_CCL
	Sicherheitsproblemstellung	APE_SPD
	Sicherheitsziele	APE_OBJ
	Definition erweiterter Komponenten	APE_ECD
	Sicherheitsanforderungen	APE_REQ
ASE: Sicherheitsvorgaben-Evaluierung	Schutzprofil-Einführung	ASE_INT
	Übereinstimmung der Ansprüche	ASE_CCL
	Sicherheitsproblemstellung	ASE_SPD
	Sicherheitsziele	ASE_OBJ
	Definition erweiterter Komponenten	ASE_ECD
	Sicherheitsanforderungen	ASE_REQ
	EVG-Übersichtsspezifikation	ASE_TSS
ACO: Zusammensetzung	Begründung der Zusammensetzung	ACO_COR

	Entwicklungsbeweise Abhängigkeit voneinander abhängiger Komponenten Bestehende EVG-Tests Bestehende Schwachstellenanalyse	ACO_DEV ACO_REL ACO_CTT ACO_VUL

Abbildung 5: Auflistung der Vertrauenswürdigkeitsklassen und deren Familien

In den Komponenten dieser Vertrauenswürdigkeitsfamilien stehen nun die einzelnen Sicherheitsanforderungen, welche das Vertrauen in die korrekte Funktionalität bestätigen sollen. Die Familie *Stärke der EVG-Sicherheitsfunktion* entspricht hierbei einer Bewertung der Sicherheitsmechanismen aus den ITSEC-Kriterien und die Familie *EVG-Entwurf* entspricht dem Architektur- bzw. Feinentwurf.[23] Die Komponenten bestehen aus Ziffern, zum Beispiel kann eine Familie die Komponenten 1-4 beinhalten, und die Komplexität der Sicherheitsanforderungen an die Vertrauenswürdigkeit erhöht sich mit einer höheren Vertrauenswürdigkeitskomponente. Das heißt, aus einer höheren Vertrauens-würdigkeitsstufe folgt eine zunehmende Testtiefe und/ oder erhöhter Aufwand bei der Erstellung von Dokumenten, welche den Entwicklungsvorgang dokumentieren.

Wie bei den ITSEC-Kriterien gibt es bei den CC Evaluationsstufen (Evaluation Assurance Level (EAL)). Welche Evaluationsstufe erreicht werden soll, wird im Schutzprofil beschrieben. Eine Evaluationsstufe wird durch eine Kombination der Vertrauenswürdigkeitskomponenten festgelegt. Eine höhere Evaluationsstufe bedeutet somit mehr und/ oder höhere Vertrauenswürdigkeitskomponenten zu erfüllen. Es ist ebenfalls möglich eine Komponente innerhalb einer Vertrauenswürdigkeitsfamilie durch eine höhere Komponente auszu-tauschen oder neue Komponenten hinzuzufügen. Die hinzugefügten oder ausgetauschten Komponenten werden später zusätzlich der Evaluationsstufe beigefügt. Es gibt sieben Evaluationsstufen, EAL1 – EAL7, welche sich an den ITSEC-Stufen orientieren. Die Stufe EAL2 entspricht dabei der ITSEC-Stufe E1. EAL1 wurde eingeführt um den Einstieg in die Evaluierung einfacher zu gestalten, denn oftmals werden IT-Produkte/ -Systeme nicht sofort auf eine höhere Evaluationsstufe geprüft, sondern erst auf einer niedrigeren Stufe, um die gewünschte Evaluationsstufe schrittweise zu erreichen.[24]

Auf dem Portal der Mitglieder der Common Criteria kann man die verschiedenen Arten von bereits zertifizierten Produkten mit ihren jeweiligen Zertifizierungsreporten, Sicherheits-vorgaben und Schutzprofilen einsehen.[25] Ein wichtiger Aspekt einer Evaluierung sind die Kosten und die Dauer. Die Kosten, die hierbei anfallen können sind zum Beispiel Kosten des Testlabors, Änderungsaufwand und die damit verbundenen Kosten, um den Anforderungen

des Schutzprofils zu entsprechen, Aufbereitung der Vertrauenswürdigkeitsdokumente und Gebühren der offiziellen Zertifizierungsstelle.[26] Die Dauer kann je nach Evaluationsstufe unterschiedlich lange betragen. Für niedrige Evaluationsstufen, wie EAL2, kann die Evaluierung sechs bis neun Monate dauern. Für höhere Evaluationsstufen, also Stufen ab EAL4, kann der Vorgang ein bis zwei Jahre dauern.[27]

Um eine einheitliche Vorgehensweise bei der Evaluierung zu schaffen, wurde die Gemeinsame Evaluationsmethodologie (Common Evaluation Methodology, CEM) entwickelt. Im Gegensatz zum Kriterienkatalog, in dem steht was evaluiert werden soll, steht in der CEM wie evaluiert werden soll. Dies stellt sicher, dass die Evaluierungsergebnisse aller Zertifizierungsstellen gleichwertig zu betrachten sind und legt den Grundstein zur gegenseitigen Anerkennung der Zertifikate.[22]

Schutzprofil

Um dem Anwender die Evaluation des evaluierten IT-Produkts/ -Systems transparenter zu machen, ihn wissen zu lassen, ob die zertifizierte Sicherheitsfunktionalität seinen Bedürfnissen entspricht und die Qualität der Sicherheit seiner jeweiligen Bedrohungslage und dem Wert seiner Daten angemessen ist, wurde das Konzept des Schutzprofils eingeführt.[28]

In Schutzprofilen werden Anforderungen an die Funktionalität, durch die CC-Funktionsklasse, und an die Vertrauenswürdigkeit, durch die Evaluationsstufen, festgeschrieben, welche eine Menge von Sicherheitszielen vollständig abdeckt. Sie sind zunächst implementierungsunabhängig, können aber durch die daraus ableitbaren Sicherheitsvorgaben auf einen konkreten Evaluationsgegenstand zugeschnitten werden. Mit der Zertifizierung eines Schutzprofils wird der Nachweis erbracht, dass das Schutzprofil vollständig, konsistent und technisch stimmig ist.[29]

Abbildung 6 zeigt den strukturellen Aufbau eines Schutzprofils gemäß den CC:

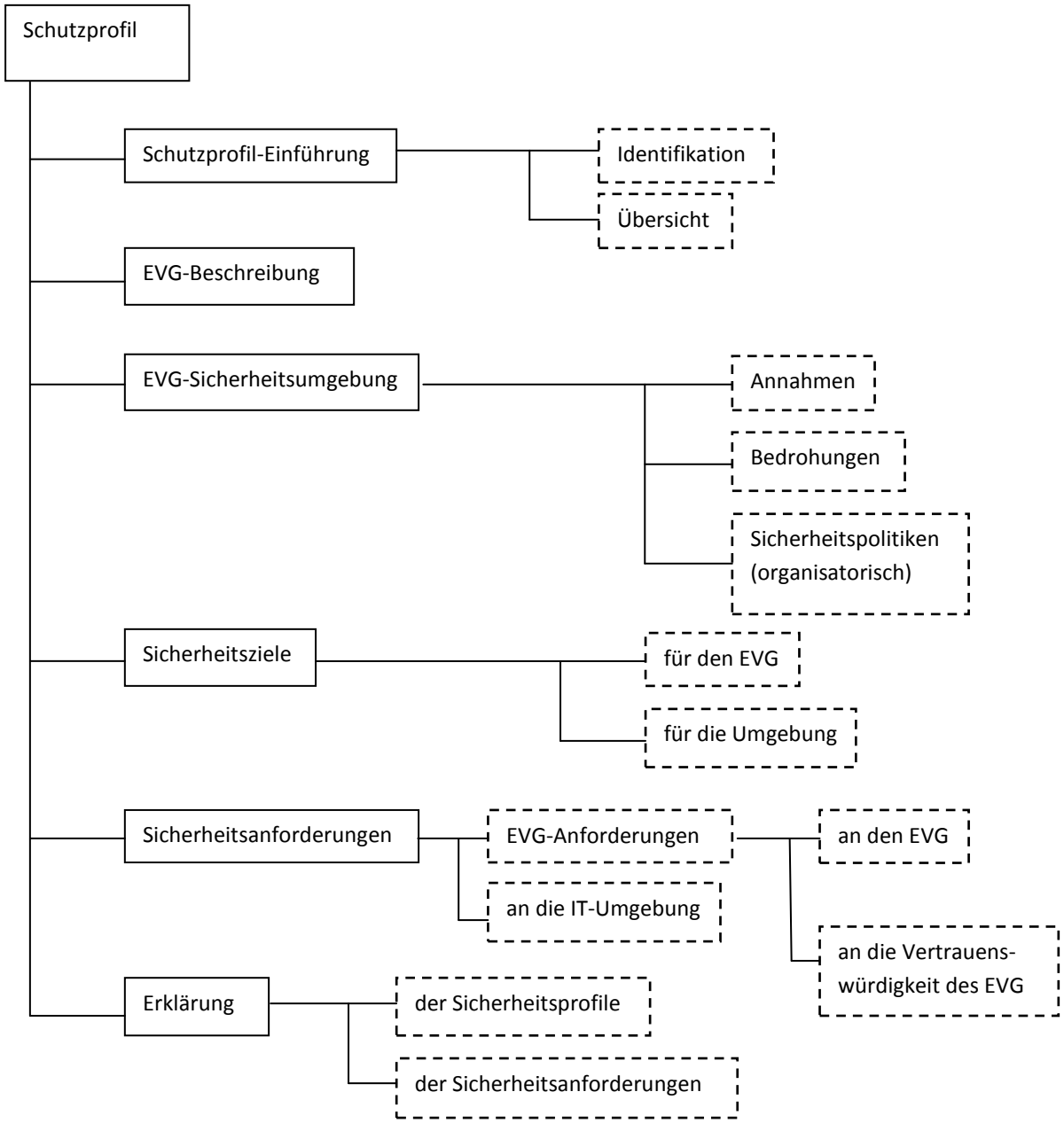

Abbildung 6: Struktureller Aufbau eines Schutzprofils

Die Einführung dient zur eindeutigen Identifizierung des Schutzprofils und soll einen allgemeinen Überblick über das Schutzprofil geben, so dass der Anwender erkennen kann, ob das Schutzprofil für ihn von Interesse ist.

Im Abschnitt *EVG-Sicherheitsumgebung* sollen im Unterpunkt *Annahmen* die Annahmen über die typische Umgebung, in der der Evaluationsgegenstand eingesetzt werden kann, getroffen werden. Unter *Bedrohungen*, sollen die Bedrohungen aufgezeigt werden, die im Bezug auf die Einsatzumgebung auf das IT-Produkt, einwirken können. Dazu zählen auch eventuell gesetzliche Vorgaben und vorgeschriebene Sicherheitsstandards. Bei den *Sicherheitspolitiken* geht es um die effektive Erfüllung der Sicherheitsziele durch das

Beschreiben von Annahmen über den sicheren Betrieb. Hierzu zählt zum Beispiel der materielle Schutz des EVGs in seiner Einsatzumgebung.

Die *Sicherheitsziele* dienen zur Angabe, wie man den Bedrohungen des EVGs entgegenwirken will. Dabei ist für jede Bedrohung mindestens ein Sicherheitsziel zu definieren.

Zur Erstellung der *Sicherheitsanforderungen* an einen EVG kann man auf die CC-Funktionsklassen zurückgreifen, da diese abgestimmte, evaluierbare und in sich konsistente Sicherheitsanforderungen enthalten. Die Anforderungen an die Vertrauenswürdigkeit sind durch die sieben EAL-Stufen vordefiniert und können ebenfalls genutzt werden. Im Abschnitt *Erklärung* muss man eine Konsistenz- und Vollständigkeitsprüfung durchführen und die Angemessenheit aller Anforderungen an den EVG erläutern.[35]

Auf der Internetseite des BSI können sind bereits zertifizierte Schutzprofile veröffentlicht und können für die Zertifizierung der IT-Produkte/ -Systeme eingesetzt werden.[30] Dies dient besonders dem Zweck der Vereinheitlichung und Standardisierung der Schutzprofile.

Fazit

Wie man sieht finden sich in den CC viele Aspekte wieder, die man bereits aus den ITSEC-Kriterien kennt. Dabei spiegeln sich die Bewertung der Sicherheitsmechanismen und die Bewertung der korrekten Funktionsweise aus den ITSEC-Kriterien in den Vertrauenswürdigkeitsklassen der CC wider. Die Funktionsklassen werden durch die funktionalen Sicherheitsanforderungen der CC und dem Schutzprofil ersetzt. Im Gegensatz zu den ITSEC-Funktionsklassen, welche sich an den zehn Funktionsklassen der deutschen IT-Kriterien orientieren, besitzen die CC ca. 150 verschiedene Funktionalitätskomponenten und damit eine wesentlich detailliertere Beschreibung der Sicherheitsanforderungen des Evaluierungsgegenstandes. Durch die Einführung eines zertifizierten, veröffentlichten Schutzprofils werden nun die Anforderungen an einen EVG weltweit einheitlich beschrieben. Ein weiterer Vorteil ist, dass man nun anhand des Schutzprofils das Ergebnis der Evaluation vollständig nachvollziehen kann.[31]

In späteren Versionen des SOGIS-MRA[12], ein Abkommen zur bisher europaweiten Anerkennung von ITSEC-Zertifikaten, wurde eine gegenseitige Anerkennung des CC-Zertifikates auf europäischer Ebene hinzugefügt. Die gegenseitige Anerkennung der Zertifizierungen reicht hier bis zu der Evaluierungsstufe EAL4. Die hierbei anerkannten Zertifizierungsstellen sind die nationalen Stellen aus Deutschland, Frankreich, Großbritannien, Niederlande und Spanien. Die Anerkennung von höheren Stufen ist für

bestimmte technische Bereiche unter besonderen Rahmenbedingungen, welche hier nicht weiter erörtert werden, möglich.[13, 32]

Im Mai 2000 wurde ein internationales Abkommen, CCRA-Abkommen[33], zur gegenseitigen Anerkennung der CC-Zertifikate und -Schutzprofilen veröffentlicht. Die gegenseitige Anerkennung reicht hier bis zur Evaluationsstufe EAL4.[32] Durch dieses Abkommen sind der Wettbewerb und das Agieren auf dem internationalen Markt möglich geworden.

Als nachteilig sind bei den CC allerdings der hohe Kosten- und Zeitaufwand der Evaluierung. Denn aufgrund der schnell fortschreitenden Technologie in der heutigen Zeit kann es vorkommen, dass ein IT-Produkt bis zu seiner Zertifizierung bereits veraltet ist.

Anmerkungen

1. Vertraulichkeit ist der Schutz vor unbefugter Kenntnisnahme von Informationen. Integrität ist der Schutz vor unbefugter Veränderung von Informationen. Verfügbarkeit ist der Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln. Die Kriterienkataloge sind ebenfalls auf andere Aspekte der IT-Sicherheit anwendbar.
    a. Vgl.: Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Part 1: Introduction and general Model, Seite 10
    b. Vgl.: Information Technology Security Evaluation Criteria Version 1.2, Seite 19
2. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 211
3. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 217
4. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 220-221
5. Vgl.: BSI-Broschüre über zertifizierte IT-Sicherheit, Art.-Nr. BSI-Bro10/331, Seite 14-15
6. Evaluierungsdokumente dokumentieren die Herstellung/ Entwicklung eines IT-Produkts/ -Systems. Hierzu gehören zum Beispiel der Quellcode, Architekturentwürfe und Feinentwürfe, Testfälle, Beschreibung der Sicherheitsanforderungen
7. Liste mit zertifizierten Produkten vom BSI: www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/ZertifizierteProdukte/zertifizierteprodukte_node.html, 17.03.2013
8. Vgl.: Information Technology Security Evaluation Criteria Version 1.2, Seite 28-30
9. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 215 und 218

10. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 218-219
11. Vgl.: § 17 Signaturgesetz
12. SOGIS-MRA: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/International/sogis_V3_pdf.pdf?__blob=publicationFile, 17.03.2013
13. Vgl.: BSI-Broschüre über zertifizierte IT-Sicherheit, Art.-Nr. BSI-Bro10/331, Seite 17
14. Bei den deutschen IT-Kriterien gibt es nur die Angabe der Qualitätsstufe Q0 – Q7, in der die Bewertung der Sicherheitsmechanismen eingeschlossen ist.
    a. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 216-217
15. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 220
16. Vgl.: www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/itsicherheitszert.html
17. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 222-224
18. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 222
19. In den Sicherheitsvorgaben (security target (ST)) sind zusätzlich zu den Informationen im Schutzprofil, weitere Informationen speziell bezogen auf den Evaluierungsgegenstand und dessen Einsatzumgebung.
    a. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 222
    b. Vgl.: BSI, IT-Sicherheitszertifizierung, www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/itsicherheitszert.html
20. Vgl.: Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 , Part 3: Security assurance components, Seite 23
21. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 223
22. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 224

23. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 235-236
24. Vgl.:
    a. Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 222
    b. Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 , Part 3: Security assurance components, Seite 30-31
25. Vgl.: Common Criteria Portal, Certified Products, http://www.commoncriteriaportal.org/products/, 17.03.2013
26. Vgl.: Corsec, Common Criteria FAQ, http://www.corsec.com/common-criteria-services/common-criteria-faq/#a11
27. Vgl.: Corsec, Common Criteria FAQ, http://www.corsec.com/common-criteria-services/common-criteria-faq/#a10
28. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 221-222
29. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 227
30. Liste zertifizierter Schutzprofile: www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/SchutzprofileProtectionProfiles/SchutzprofileProtectionProfiles_Aktuell/schutzprofile_pps_aktuell_node.html, 17.03.2013
31. Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 235
32. Vgl.: BSI, Europäische Anerkennung von ITSEC/ CC-Zertifikaten, www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/InternatAnerkennung/SOGIS_Anerkennung.html
33. CCRA-Abkommen: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/International/cc_mra_pdf.pdf?__blob=publicationFile, 12.03.2013
34. Weiter Informationen zu dem Konzept: http://www.scmagazine.com/significance-of-common-criteria-assurance-maintenance-ama/article/31385/, 18.03.2013
35. Vgl.: Vgl.: Eckert, C.: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, Seite 227-228
36. Vgl.: Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Part 1: Introduction and general Model, Seite 10

Literaturverzeichnis

Literaturquellen

I. Eckert, C., 2009: [IT-Sicherheit]: Konzepte - Verfahren – Protokolle, Kapitel 5 Bewertungskriterien, Oldenbourg Verlag, München, 6. Auflage, 2009

II. BSI-Broschüre über zertifizierte IT-Sicherheit, Art.-Nr. BSI-Bro10/331

III. Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 , September 2012

IV. Information Technology Security Evaluation Criteria Version 1.2, Juni 1991

Internetquellen

V. BSI, Europäische Anerkennung von ITSEC-/ CC-Zertifikaten, www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/InternatAnerkennung/SOGIS_Anerkennung.html, 17.03.2013

VI. BSI, Anerkennung von CC– Zertifikaten im Rahmen des CCRA, www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/InternatAnerkennung/CCRA_Anerkennung.html, 12.03.2013

VII. BSI, IT-Sicherheitszertifizierung, www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/itsicherheitszert.html, 17.03.2013

VIII. BSI, Zertifizierung, www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/zertifizierung.html, 17.03.2013

IX. BSI, IT- Sicherheitskriterien und Evaluierung nach ITSEC, www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/ITSicherheitskriterien/ITSEC/itsec_eval.html, 17.03.2013

X. Corsec, Common Criteria FAQ, http://www.corsec.com/common-criteria-services/common-criteria-faq/, 17.03.2013

Bildquellen

XI. Abbildung 1: Eckert, C., 2009: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, 2009, Seite 221

XII. Abbildung 2: Eckert, C., 2009: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, 2009, Seite 218

XIII. Abbildung 3: Eigene Darstellung aus der Beschreibung der Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 , Part 2: Security Functional Components, September 2012, Seite 173-175

XIV. Abbildung 4:

- Eckert, C., 2009: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, 2009, Seite 225-227 aus der Beschreibung der CC-Funktionsklassen
- Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 , Part 2: Security Functional Components, September 2012

XV. Abbildung 5:

- Struktur aus: Eckert, C., 2009: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, 2009, Seite 231
- Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 , Part 3: Security assurance components

XVI. Abbildung 6: Eckert, C., 2009: [IT-Sicherheit]: Konzepte - Verfahren - Protokolle, Oldenbourg Verlag, München, 6. Auflage, 2009, Seite 229