FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Sicherheitsstandards und die Common Criteria, didaktisch aufbereitet mit Moodle

MAGISTERARBEIT

zur Erlangung des akademischen Grades

Magister der Sozial- und Wirtschaftswissenschaften

im Rahmen des Studiums

Informatikmangement

eingereicht von

Valon Ismaili, Bakk. Techn.
Matrikelnummer 9927064

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer: ao. Univ.-Prof.i.R.Dr.Erich Neuwirth

Wien, 05.05.2014

(Unterschrift Verfasser/in) (Unterschrift Betreuer/in)

Erklärung zur Verfassung der Arbeit

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten, Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 05.05.2014

(Valon Ismaili)

Danksagung

An dieser Stelle möchte ich mich bei all denjenigen bedanken, die mich während der Anfertigung dieser Magisterarbeit unterstützt und motiviert haben.

Besonders danke ich meinem Betreuer Professor Herrn Neuwirth für die Unterstützung, Betreuung und die konstruktiven Vorschlägen.

Meiner Familie danke ich ganz herzlich für die unendliche Unterstützung und Motivation.

Kurzfassung

Die Arbeit vermittelt wesentliche Aspekte der Common Criteria in einer Form, die für den Schulunterricht an einer HTL verwendet werden soll. Die Einführung beginnt mit einer umfassenden Erklärung des geschichtlichen Kontext der Common Criteria und erklärt zuvorgehende Standards wie die DoD 5200.28-M, TCSEC und ITSEC. Danach wird das Sicherheitsmodell und die Terminologie erläutert, darunter Kernbegriffe wie der Evaluationsgegenstand (EVG). Mit diesem Wissen ausgestattet werdem dem Leser die zwei wesentlichen Ausdrucksformen zur Formulierung von Sicherheit vorgestellt: Sicherheitsvorgaben und Schutzprofile, wobei auch auf ihre Varianten mit geringer Vertrauenswürdigkeit eingegangen wird, die besonders bei einfacheren Projekten relevant sein können. Abschließend werden die Kataloge der Common Criteria erklärt, in denen Funktions- und Vertrauenswürdigkeitskomponenten für den Wiedergebrauch definiert werden. Abgerundet wird die Arbeit mit einem Moodle-Kurs, der wesentliche Fragen der einzelnen Kapitel formuliert interaktiv und automatisiert beurteilt beantworten lässt, und sich damit an die formulierte Zielgruppe von HTL-Schülern richtet, welche durch diese Arbeit ihr Verständnis von Sicherheitsstandards und -modellen schärfen sollen.

Abstract

This thesis discusses the main aspects of the Common Criteria and communicates them in a form fit for students at secondary schools like the Austrian HTL (Höhere Technische Lehranstalt), an engineering-focused high school for students of age 14 - 19. The paper starts by introduction the historical context of the Common Criteria, describing preceeding and influential standards like the DoD 5200.28-M, the TCSEC and the ITSEC. After that, it goes on to explain the security model and terminology of the Common Criteria, particularly the core concept of the " Evaluationsgegenstand " (target of evaluation). Having equipped the reader with this knowledge, next the main concepts of of "Sicherheitsvorgaben" and "Schutzprofile" (security targets and security profiles) are introduced, also in their shorter version of "lesser trusted" targets or profiles which are particularly useful for simpler security in projects. Finally, the Common Criteria catalogs are introduced which contain functional and assurance components for reuse by implementors of the CC. The paper is then finalized with the addition of an interactive Moodle course which picks up the essential knowledge introduced in this thesis and lets the user measure their learned knowledge in an interactive multiple-choice exam which, aiming at students, helps raise their awarness of security models and standards and gives them essential knowledge on how they work and are applied in practice.

Inhaltsverzeichnis

1 Inhalt und Aufbau

1.1 Die Common Criteria

Die *Common Criteria for Information Technology Security Evaluation* (1), kurz *Common Criteria* oder *CC* genannt, ist ein vergleichsweise junger internationaler Standard der IT-Sicherheit (2) (3) (4), der seit einigen Jahren als ISO-Standard 15408 weiter entwickelt wird (5) (6) (7). Diese Arbeit erzählt die Geschichte wichtiger IT-Standards und ihrer Sicherheitskonzepte, geht schließlich genauer auf die CC ein, und stellt anschließend ergänzend einen interaktiven Moodle-Kurs (8) für den Einsatz an einer HTL zur Verfügung.

1.2 Die Abschnitte

Die Arbeit unterteilt sich in 3 Abschnitte:

1. Geschichte der IT-Standards.
2. Beschreibung der Common Criteria.
3. Interaktiver Kurs für den Einsatz im HTL-Unterricht.

(1) erklärt den Kontext, aus die CC entstanden ist, (2) fasst wesentliche in (1) kennen gelernte Sicherheitskonzepte zusammen und zeigt, wie sie in der CC umgesetzt werden, und wie die CC aufgebaut ist und angewendet wird. Basierend aus dem theoretischen Wissen aus (2) wird in (3) ein interaktiver Moodle-Kurs für den Einsatz an einer HTL ausgearbeitet.

Konkret haben die einzelnen Punkte folgenden Aufbau:

1.2.1 Geschichte der IT-Standards

Um die CC zu verstehen, hilft Vorwissen über ältere Standards. Die Arbeit greift dabei folgende Standards auf und erklärt jeweils ihren Beitrag zur Entwicklung von Sicherheitsstandards:

1. DoD 5200.28-M: Erster militärischer Sicherheitsstandard für die IT, Grundlage für den einflussreichen TCSEC-Standard.
2. TCSEC (Orange Book): Lange im Einsatz, das Konzept von Kriterienkatalogen wurde bis zu den CC übernommen.

3. Deutsche ITSK (Grünbuch): Beurteilt zusätzlich die Qualität von Sicherheitsmaßnahmen.
4. ITSEC: Erster Länder-übergreifender europäischer Standard. Führt Evaluationsstufen ein, welche ausdrücken, wie genau Vertrauenswürdigkeit überprüft werden muss.
5. CTCPEC: Kanadischer Standard, welcher neue Kriterienkataloge für moderne Systeme einführt, die Weiterentwicklung wurde zu Gunsten der CC aufgegeben.

Im Rahmen der Erklärung der Geschichte dieser Standards wird der Leser mit wesentlichen Konzepten von Sicherheitsstandards vertraut, welche Einfluss auf die CC hatten und von ihr verwendet werden.

1.2.2 Beschreibung der Common Criteria

Die CC teilt sich auf 3 Teile auf:

1. Modell und Konzepte (2)
2. Funktionsklassen (mit Katalog) (3)
3. Vertrauenswürdigkeitsstufen (mit Katalog) (4)

Passend zu diesem Aufbau erklärt dieser Abschnitt zuerst knapp die Entstehung der CC, danach wesentliche Konzepte der IT-Sicherheit, wie Bedrohungen, Risiken und Sicherheitsmaßnahmen, das Modell, in dem sie zusammen hängen, und wie die CC dieses Modell verwendet. Darüber hinaus werden konkrete CC-Konzepte erklärt, darunter Anforderungen an die Sicherheitsfunktion sowie Anforderungen an die Vertrauenswürdigkeit, dazu Schutzprofile, Sicherheitsvorgaben, Pakete von Vorgaben und Profilen, sowie vereinfachte Vorgaben und Profile.

Anschließend wird die Struktur der CC-Kataloge aus Teil 2 und 3 näher besprochen, als Einführung wird auf die Funktionsklassen und Klassen der Vertrauenswürdigkeit und ihre Bedeutung und Einsatzmöglichkeiten eingegangen. Danach wird die Unterteilung in Klassen, Familien und Elemente erklärt, wie die einzelnen Elemente definiert werden und wie ihre Abhängigkeiten zwischen Elementen der Kataloge umgesetzt werden, und was sie bedeuten.

1.2.3 Interaktiver Kurs für den Einsatz im HTL-Unterricht

Basierend aus den Informationen aus den ersten zwei Abschnitten wird im letzten Teil der Arbeit ein interaktiver Moodle-Kurs für den Einsatz an einer HTL ausgearbeitet.

Im Abschnitt 3 wird das Wissen aus ersten zwei Abschnitten in einem interaktiven Moodle-Kurs an HTL-Schülern vermittelt. Moodle ist für die Zielgruppe eine logische Wahl: Abgesehen davon, dass es weit verbreitet und in einigen Wiener HTLs im Einsatz ist, ist es durch seine Interaktivität für junge Menschen ansprechend, und ein Musterbeispiel für den pädagogisch wertvollen Einsatz neuer Medien im Unterricht.

Der Kurs vermittelt durch Zusammenfassungen und Illustrationen wesentliche Zusammenhänge, die in Folge in Fragenkatalogen zu den einzelnen Abschnitten überprüft werden können. Zusätzlich wird Material für die Lehrer bereit gestellt, welches beim Einbau in den Unterricht helfen soll.

Das Ziel dieser Unterlagen ist die Förderung der Auseinandersetzung mit dem Thema Sicherheit in der IT, die Schaffung eines Bewusstseins für die Notwendigkeit von IT-Sicherheit, sowie die Erläuterung, wie formalisierte Sicherheit in Form der CC präzise Formulierung und Kontrolle von IT-Sicherheit garantiert und somit den Einsatz von IT-Sicherheitsstandards fördert.

Auch wenn die Arbeit selbst detailliert auf die CC eingeht, ist der Kurs im Vergleich reduziert, da im Unterricht die Auseinandersetzung mit den Konzepten der IT-Sicherheit und CC eher im Vordergrund steht, als die Einsatz-orientierte Umsetzung von CC-Schutzprofilen und Sicherheitsvorgaben.

1.3 Ziel und Abgrenzung

Die Leser, vor allem Lehrer an HTLs, sollen mit dieser Arbeit umfassend über IT-Sicherheitsstandards und speziell die CC informiert werden, und mit dem mitgelieferten Kurs in der Lage sein, IT-Sicherheit und ihre große Bedeutung über theoretische Modelle hinaus ansprechend und interaktiv an Schüler vermitteln zu können.

Die Arbeit versucht jedoch nicht, die CC als Grundlage für die Implementierung von CC-basierten Schutzprofilen und Sicherheitsvorgaben zu ersetzen, der Standard ist als endgültige Referenz hierfür unersetzlich.

2 Die Common Criteria: Geschichte

2.1 Einleitung

Die Entstehung der CC ist das Ende einer Entwicklung, die auf den Erfahrungen mit älteren Standards der IT-Sicherheit basiert, die in den letzten 30 Jahren verwendet worden sind. Von den verschiedenen Standards, die als Einfluss auf die CC genannt werden ((9 S. 7), (10 S. 211)), waren besonders die hier in weiterer Folge besprochenen maßgebend.

2.2 DoD 5200.28-M

Obwohl der TCSEC-Standard oft als Grundlage der CC genannt wird, wurde der Grundstein für die CC schon 10 Jahre zuvor, 1973, mit dem Standard *DoD 5200.28-M* (11) (*Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems*) gelegt. DoD 5200.28-M beschreibt den Zweck von Sicherheitstests und Evaluation vereinfacht wie folgt (9 S. 7):

1. Entwicklung und Erwerb von Methoden, Techniken und Standards für die Analyse, Tests und Evaluation der Sicherheitseigenschaften von Datenverarbeitungssystemen.

2. Unterstützung der Analyse, Tests und Evaluation von Sicherheitseigenschaften von Datenverarbeitungssystemen, indem Kriterien entworfen werden, mit denen eine Zertifizierungsstelle die Effektivität von Sicherheitsmaßnahmen für ein Datenverarbeitungssystem beurteilen kann.

3. Eliminiert Wiederholungen, minimiere den Aufwand, erhöhe die Effektivität und Wirtschaftlichkeit von Sicherheitsoperationen, und bietet eine Grundlage für die Abnahme und gemeinsame Verwendung von Sicherheitstests, Evaluationswerkzeugen und -ausrüstung.

Diese Ziele hatten starken Einfluss auf die ähnlich formulierten Ziele der CC, die im Kapitel 2.7.1 ab Seite 19 näher beschrieben werden.

2.3 Trusted Computer System Evaluation Criteria (TCSEC)

Die *Trusted Computer System Evaluation Criteria* (12) (kurz *TCSEC*) wurden Anfang 1980 entwickelt und unter dem Namen *Orange Book*[1]. Auch wenn die TCSEC-Kriterien heute für die Evaluierungspraxis keine Rolle mehr spielen, sind viele Konzepte und Ansätze aus Kriterienkatalogen, die heute noch im Einsatz sind, auf die TCSEC und die im Folgenden vorgestellten IT- bzw. ITSEC-Kriterien zurück zu führen (10 S. 201 - 204). Aus heutiger Sicht ist der wichtigste Beitrag der TCSEC die Einführung einer Klassifizierung, bei der Software-Produkte abhängig von ihren Sicherheitseigenschaften vorgegebenen Klassen zugeteilt werden. Tabelle 1 illustriert diese Klassen.

Kategorie	Klasse
D – minimaler Schutz	
C - benutzerbestimmbarer Schutz	C1 - benutzerspezifische Unterteilung der Daten
B - systembestimmter Schutz	B1 - Zugriffskontrolle mit einem abgestuften Zugriffsmodell für Entitäten
	B2 - ein dokumentiertes Sicherheitsmodell existiert
	B3 - Überwachung aller sicherheitsrelevanter Aktionen, ein funktionierendes Notfallkonzept und die vollständige Realisierung eines Referenzmonitors erfolgt
A - verifizierter Schutz	A1 - verifizierter Schutz
	A1 und darüber

Tabelle 1: Klassifizierung der Sicherheit nach TCSEC

Entwickelt wurden die TCSEC für die IT-Sicherheitsanforderungen des amerikanischen Verteidigungsministeriums. Dabei wurde der Standard stark auf die dort eingesetzten zentralen Betriebssysteme ausgerichtet, bei denen auch eine genaue Überwachung und Protokollierung der Benutzeraktionen gefordert war (13 S. 13 - 15). Sicherheitsbedürfnisse von kommerziellen oder damals kaum vorhandenen Privatnutzern wurden in diesem vorerst nicht beachtet – was mit der zunehmenden Computerisierung des Privatsektors ein Problem werden sollte.

[1] Diese informelle Bezeichnung bezieht sich auf den orangen Umschlag des Buches, in dem der Standard veröffentlicht worden ist. bekannt.

Ein weiterer Schwachpunkt der TCSEC ist die fehlende Trennung zwischen der Sicherheitsfunktionalität und ihrer Qualität. Die Kriterien bewerten nur, welche Funktionalität erbracht wird, können aber nicht beurteilen, *wie wirksam* die eingesetzten Maßnahmen sind (10 S. 203, 204).

Im Laufe seiner langen Lebenszeit wurde der TCSEC-Standard um mehrere Kataloge erweitert, welche Sicherheitsbedürfnisse für neue Felder der IT abdecken sollten. Trotzdem war die Erweiterung der Kataloge allein nicht ausreichend, um den geänderten Anforderungen der Anwender des Standards gerecht zu werden, die nun vor allem im Privatsektor zu finden waren (10 S. 203, 204).

Noch Anfang der 1990er Jahre plante die USA die TCSEC durch eine Überarbeitung an die neuen Erfordernisse der vermehrt nicht-militärischen Benutzer anzupassen, gab diese Bestrebungen jedoch zugunsten der Entwicklung der CC auf.

2.4 Deutsche IT-Sicherheitskriterien

Als Reaktion auf die Schwachpunkte der TCSEC veröffentlichte der Vorgänger des heutigen deutschen *Bundesamts für Sicherheit in der Informationstechnik* (kurz *BSI*) 1989/1990 die deutschen *IT-Sicherheitskriterien* (kurz *ITSK*), die – in Anlehnung an die informelle Bezeichnung Orange Book der TCSEC – auch als *Grünbuch* bekannt wurden.

Der Standard beurteilt Sicherheitsfunktionalität nach der Systemfunktionalität und der Qualität der eingesetzten Mechanismen – wobei die Beurteilung der Qualität eine Neuerung gegenüber den TCSEC darstellte.

Die Funktionalitätsklassen der IT-Sicherheitskriterien basieren teilweise auf jenen der TCSEC-Kriterien, die ITSK definierten aber auch neue Klassen, mit denen neue Sicherheitsanforderungen abgedeckt wurden, die über die TCSEC hinaus gingen.

Die Bewertung der Sicherheitsmechanismen erfolgt hier mit den Stufen ungeeignet, schwach, mittel, stark und sehr stark. Ein ungeeigneter Mechanismus ist nicht wirksam, ein schwacher wehrt unabsichtliche Sicherheitsverstöße ab, die Qualität steigt mit den Stufen

weiter an bis zur Stufe sehr stark, bei der der Mechanismus auch gegen absichtliche Sicherheitsverstöße schützt (10).

Der größte Beitrag der IT-Sicherheitskriterien ist die Einführung der Qualitätsstufen, welche später im europäischen Standard ITSEC aufgegriffen worden sind (10 S. 205 - 207).

2.5 Information Technology Security Evaluation Criteria (ITSEC)

Die *Information Technology Security Evaluation Criteria* (13) (kurz *ITSEC*) wurden 1991 als europäischer Sicherheitsstandard durch die Länder Großbritannien, Frankreich, Niederlande und Deutschland verabschiedet.

Die ITSEC übernahm das mittlerweile etablierte Konzept der Funktionsklassen vorhergehender Standards. Neu war die Beurteilung der Qualität, welche im Vergleich zu den deutschen IT-Sicherheitskriterien noch weiter aufgeteilt wurden, und zwar in die Bewertung der korrekten *Funktionsweise* des Evaluationsgegenstandes und der *Wirksamkeit* der eingesetzten Mechanismen.

Die Wirksamkeit wird durch eine Skala zur Bewertung der Stärke festgelegt, welche sich auf die Stufen *niedrig*, *mittel* und *hoch* unterteilt.

Die ITSEC-Kriterien definieren sieben Evaluationsstufen *E0* bis *E6*, wobei jede dieser Stufen den Grad an Vertrauen ausdrückt, der in die Korrektheit der Funktionalität des Evaluationsgegenstandes gesetzt wird. Die Evaluationsstufen sind hierarchisch strukturiert.

Tabelle 2 stellt diese Hierarchie dar.

Evaluationsstufe	Beschreibung
E0	Diese Stufe repräsentiert unzureichende Vertrauenswürdigkeit.
E1	Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muss nachgewiesen werden, dass der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.

E2	Zusätzlich zu den Anforderungen für die Stufe E1 muß hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muß bewertet werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.
E3	Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode bzw. die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muss bewertet werden.
E4	Zusätzlich zu den Anforderungen für die Stufe E3 muss ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.
E5	Zusätzlich zu den Anforderungen für die Stufe E4 muss ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode bzw. den Hardware- Konstruktionszeichnungen bestehen.
E6	Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer formalen Notation vorliegen, die konsistent mit dem zugrunde liegenden formalen Sicherheitsmodell ist.

Tabelle 2: Die Evaluierungsstufen der ITSEC

Die Bewertung der Qualität eines evaluierten Systems besteht aus einem Paar, bestehend aus einer Evaluationsstufe, also einer Bewertung der Korrektheit der Funktionalität, und aus einer Einstufung der Wirksamkeit der verwendeten Mechanismen.

So besagt beispielsweise die Zertifizierungsstufe "*E2, mittel*", dass mit zufrieden stellenden Mitteln die Korrektheit der Systemfunktionalität dargelegt und die Stärke der dafür eingesetzten Realisierungsmechanismen mit mittel bewertet wurde.

Der Zusammenhang zwischen den Qualitätsstufen der ITSK und den Evaluationspaaren der ITSEC ist in Tabelle 3 dargestellt.

	unzureichend	gering	zufriedenstellend	gut bis sehr gut	ausgezeichnet
ITSK	Q0	Q1	Q2	Q3 – Q5	Q6, Q7
ITSEC	E0	E1, niedrig	E2, mittel	E3 – E5, hoch	E6, hoch

Tabelle 3: Zusammenhang zwischen den Qualitätsstufen der ITSK und den Evaluationspaaren der ITSEC.

Die ITSEC stellen (wie die ITSK zuvor) Fortschritte gegenüber den TCSEC dar, konzentrieren sich aber immer noch auf hierarchische zentrale Systeme, und vernachlässigen die Benutzer ähnlich wie zuvor die TCSEC. Der Evaluationsprozess der ITSEC ist aufwändig, seine Ergebnisse haben geringe Aussagekraft. Gefahren, die sich durch die Verwendung unzuverlässiger Werkzeuge ergeben, werden nicht genügend erfasst.

Ein weiteres Problem des ITSEC-Standards war, dass er nur in Europa, aber nicht weltweit anerkannt wurde, was die Brauchbarkeit von ITSEC-Zertifikaten stark einschränkte (10 S. 207 - 209).

2.6 Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

Die *Canadian Trusted Computer Product Evaluation Criteria* (kurz *CTCPEC*) wurden im Jänner 1993 von der kanadischen Sicherheitsbehörde *Communications Security Establishment Canada* veröffentlicht (9 S. 2, 3), um Sicherheitskriterien zu schaffen, die auch auf den nicht-militärischen Bereich anwendbar waren.

Die CTCPEC waren der erste Standard, der erwartete Sicherheitsfunktion von der erwarteten Vertrauenswürdigkeit trennt (14). Die CTCPEC bauten zwar auf die TCSEC auf, berücksichtigten aber Multiprozessorsysteme, Datenbanksysteme, verteilte Systeme, Netzwerkanwendungen, usw.

Die thematische Breite der CTCPEC führte jedoch zu einer immer stärkeren Abweichung von den TCSEC, wodurch die Kompatibilität zwischen den Standards verloren ging. Dieses Problem war unter anderem ein Grund, die Entwicklung der CTCPEC einzustellen, um sich der Entwicklung eines neue, internationalen, Standards zu widmen, den Common Criteria.

2.7 Common Criteria for Information Technology Security Evaluation (CC)

2.7.1 Entstehung und Aufgabe der CC

Wie bereits in Kapitel 1 (Seite 9) erwähnt sind die *Common Criteria for Information Technology Security Evaluation* (kurz *Common Criteria* oder *CC*) ein mittlerweile ISO-zertifizierter Standard (ISO 15408: (5) (6) (7)) zur Bewertung und Zertifizierung der Datensicherheit von Computersystemen.

Die CC sind aus einer Zusammenarbeit mehrerer Länder entstanden[2]. Vor dem Entwurf der CC gab es mehrere nationale Standards der IT-Sicherheit, was den internationalen Vergleich von IT-Produkten über verschiedene eingesetzte Standards hinweg erschwerte. Die CC sollten dieses Problem beheben, indem ein internationaler Sicherheitsstandard geschaffen wurde, welcher als Grundlage zur Evaluation von Sicherheitseigenschaften von IT-Produkten verschiedene Produkte vergleichbar machen sollte, um sie damit einer größeren Gruppe von Anwendern zur Verfügung zu stellen.

Bei der Formulierung der CC war es das Ziel, einen modernen Standard der IT-Sicherheit zu schaffen, der als internationale Richtline für die Entwicklung, Evaluation und Beschaffung von IT-Produkten mit Sicherheitsfunktionalität gelten sollte.

Der Standard beschreibt einen systematischen Ansatz zur IT-Sicherheit:

Anforderungen an die Sicherheitsfunktionalität und die Vertrauenswürdigkeit eines IT-Produktes werden in einer standardisierten Sprache formuliert. Diese Sprache wird durch eine Reihe von Anforderungen in Katalogen bereit gestellt. Anforderungen lassen sich also als eine Sammlung von Einträgen dieser Kataloge ausdrücken.

[2] Beteiligt waren Australien, Neuseeland, Kanada, Frankreich, Deutschland, Japan, Niederlande, Spanien, Vereinigtes Königreich, Vereinigte Staaten von Amerika (2) (3) (4)

Ein unabhängiger Evaluationsprozess überprüft, wie weit die Anforderungen der CC von einem IT-Produkt erfüllt werden. Die Ergebnisse einer Evaluation sollen Konsumenten zeigen, ob ein IT-Produkt ihre Sicherheitsanforderungen erfüllt.

Die CC beschreibt die Formulierung der Anforderungen an die Sicherheit eines IT-Produkts, aber nicht, wie diese evaluiert werden sollen – mit dieser Aufgabe beschäftigt sich die *Common Methodology for IT Security Evaluation* (15) (kurz *CEM*).

2.7.2 Teile der CC

Die CC gliedert sich in 3 Teile:

- *Teil 1: Einleitung und allgemeines Modell* (2) bildet die Grundlage, in der die wesentlichen Begriffe und Konzepte der Common Criteria erklärt werden. Die klare Struktur und der geringe Seitenumfang soll dem Leser einen schnellen Überblick über die CC geben, um die für eine Evaluation nach den CC erforderlichen Dokumente und Prüfergebnisse rasch erstellen zu können.

- *Teil 2: Funktionale Sicherheitsanforderungen* (3) enthält einen thematisch und hierarchisch gegliederten Katalog von Sicherheitsanforderungen an die Funktionalität eines IT-Produkts, welche verwendet werden, um die Anforderungen eines IT-Produkts zu beschreiben.

- *Teil 3: Vertrauenswürdigkeitsanforderungen* (4) definiert einen Katalog von Vorlagen für Anforderungen an die Vertrauenswürdigkeit - die Prüftiefe - eines IT-Produkts. Teil 3 spezifiziert außerdem die Auswertungskriterien für Schutzprofile und Sicherheitsvorgaben und stellt sieben vordefinierte Pakete von Vertrauenswürdigkeitskomponenten vor, die Evaluationsstufen für Vertrauenswürdigkeit (*Evaluation Assurance Levels*, kurz *EALs*).

2.7.3 Die Rolle der CEM

CC-zertifizierte Produkte werden nur dann gegenseitig anerkannt, wenn es ein Vertrauen in den verwendeten Evaluationsprozess gibt. Dieses Vertrauen wird gestärkt, wenn alle

beteiligten Stellen die gleichen Kriterien und Evaluationsverfahren verwenden. Die CEM ist diese gemeinsame Evaluationsmethodik; sie beschreibt die Evaluationsmethoden, Prozeduren und Techniken für die Evaluation von Schutzprofilen, Sicherheitsvorgaben und Vertrauenswürdigkeitsstufen.

2.7.4 Common Criteria Recognition Agreement (CCRA)

Das *Common Criteria Recognition Agreement* (kurz *CCRA*) ist ein Zusammenschluss staatlicher Organisationen mehrerer Länder, deren Ziel es ist, an einer weiten Verbreitung und Unterstützung der CC zu arbeiten (1).

Die Mitglieder der CCRA stellen sicher, dass ihre nationalen Zertifizierungsstellen Evaluationen nach hohen und konsistenten Standards durchführen, wobei ausdrücklich auf eine Senkung der Kosten und Steigerung der Effizienz von Evaluationen geachtet wird. Dies soll das Vertrauen in CC-zertifizierte Produkte und Schutzprofile stärken, ihre Anwendung und Verfügbarkeit erhöhen, und nebenbei unnötige mehrfache Evaluationen vermeiden.

Das CCRA unterscheidet zwischen Mitgliedern, die Zertifikate ausstellen, und Mitgliedern, die Zertifikate konsumieren. Die ausstellenden Organisationen decken sich Großteils mit den Urhebern der CC. Österreich ist ein Zertifikate konsumierendes Mitglied, es wird durch das österreichische Bundeskanzleramt im CCRA vertreten.

3 Terminologie und Sicherheitsmodell

3.1 Einleitung

Für die Arbeit mit der CC ist zuerst eine Klärung der Begriffe und Konzepte notwendig, die von ihr verwendet werden. Dabei baut die CC auf anerkannte Begriffe und Konzepte der IT-Sicherheit auf.

3.2 Evaluationsgegenstand (EVG)

Jede Sicherheitsüberprüfung bezieht sich auf eine Entität. Diese Entität kann in den verschiedensten Formen auftreten, weshalb die CC den die evaluierbare Entität bewusst offen definiert:

Der Evaluationsgegenstand (kurz EVG) ist ein IT-Produkt, ein Teil eines IT-Produkts, oder ein Zusammenschluss mehrerer Produkte. Die einzelnen Komponenten des EVG können als Hard-, Soft- oder Firmware beschränken.

Das bedeutet, dass eine Netzwerkkarte ebenso einen EVG darstellen kann wie ein Betriebssystem in Kombination mit einer Firewall oder selbst eine Softwareprodukt mit Verpackung und Handbuch – der EVG ist in seiner Repräsentation nicht eingeschränkt. Lassen sich die für den EVG verwendeten Komponenten in irgendeiner Form verschieden installieren oder konfigurieren, dann ist auch diese Information in den EVG aufzunehmen und als unveränderlicher Teil des EVGs zu betrachten.

Aber unabhängig davon, wie der EVG definiert wird, ist zu beachten, dass eine Evaluation immer nur für jene Teile ausgeführt wird, welche als EVG definiert worden sind. Jede Änderung der Zusammenstellung oder Änderung der Konfiguration, z. B. der Austausch einzelner Komponenten durch „gleichwertige“ Soft- oder Hardware, führt zu einer Änderung der EVG und führt zum Verfall der Gültigkeit der Evaluierung.

Die CC ist bewusst flexibel genug gestaltet worden, damit sie für verschiedenste IT-Produkte und Evaluationsmethodiken angewandt werden kann. Diese Flexibilität sollte aber nicht missbraucht werden – die Art der Evaluation, die überprüften Sicherheitseigenschaften und das eingesetzte IT-Produkt sollten kohärent sein, damit die Evaluation zu relevanten Ergebnissen führt.

Eine Evaluation ist immer nur für die verwendete Methodik, die überprüften Aspekte und das eingesetzte Produkt gültig. Daher ist die Interpretation von Evaluationsergebnissen nur aussagekräftig, wenn das Produkt unter den gleichen Bedingungen eingesetzt wird, unter denen es evaluiert worden ist.

Zusammengefasst lässt sich sagen: *Ein EVG ist eine unveränderliche Zusammenstellung von IT-Komponenten, die auf eine spezifische Art installiert und konfiguriert worden sind.*

Für Evaluationsgegenstände gibt es eine große Anzahl von Beispielen, drei mögliche wären:

- Windows XP Home Edition 32 Bit Edition, ausgeliefert im Service Pack 3 in einer exakt bestimmten Version, zusammen mit einem Handbuch in der Version für Österreich.
- Ein HTC Desire HD Telefon mit installiertem Android 2.3.1.
- Der MySQL Community Server in der Version 5.5.28, unabhängig von der Software- und und Hardwareumgebung, in der er läuft.

3.3 Zielgruppen

Die CC richtet sich vor allem an drei Gruppen von Anwendern (2, Seite 34):

- Konsumenten: Haben ein Sicherheitsbedürfnis, welches durch die Evaluationen der CC erfüllt werden soll. Die Evaluation hilft, die Verwendbarkeit von IT-Produkten vergleichbar zu machen. Mit der CC kann der Konsument seine Sicherheitsbedürfnisse unabhängig von der Implementierung formulieren. Diese Anforderungen werden in der CC als Schutzprofile bezeichnet.

- Entwickler: Die CC soll Entwicklern helfen, ihr Produkt für eine Evaluation vorzubereiten und Sicherheitsvorgaben unabhängig von einer Implementierung zu formulieren. Sicherheitsvorgaben basieren auf Schutzprofilen – dadurch drücken die Entwickler aus, dass der EVG die Anforderungen des Konsumenten erfüllt.

- Gutachter: Jeder EVG muss unabhängig überprüft werden. Die CC beschreibt genau, was ein Gutachter wie zu überprüfen hat. Wie er es zu tun hat beschreibt die ergänzende Evaluationsmethodik der CC, die CEM.

Darüber hinaus gibt es noch eine Reihe anderer Zielgruppen, die allgemeines Interesse an IT-Sicherheit haben, und die CC als Referenzmaterial verwenden können:

- Sicherheitsverantwortliche: Zur Überprüfung, wie weit IT-Sicherheitsanforderungen in der Organisation vorhanden sind und korrekt umgesetzt werden.

- Interne und externe Gutachter: Können überprüfen, ob Sicherheitsmaßnahmen angemessen verwendet werden.

- Sicherheitsarchitekten: Können anhand existierender Schutzprofile überprüfen, welche Sicherheitsanforderungen an eine Kategorie von Produkt typischer Weise gestellt wird.

- Käufer von IT-Produkten: Können feststellen, ob ein erwünschtes Produkt den eigenen Vorgaben der IT-Sicherheit für eine bestimmte Umgebung entspricht und somit gekauft werden soll.

- Sponsoren einer Evaluation: Sie sind nicht direkt in die Definition und Evaluation eingebunden, fordern sie aber an und unterstützten sie.

- Zertifizierungsstellen: Verwalten und steuern die Programme für IT-Sicherheits-Evaluationen.

Für die drei Hauptzielgruppen der Konsumenten, Entwickler und Gutachter haben die drei Teile der CC eine (laut (2 S. 36)) jeweils andere Bedeutung:

- Konsumenten können, müssen aber nicht, die CC als Referenz und Richtlinie verwenden, um Schutzprofile, Sicherheitsanforderungen oder Vertrauenswürdigkeitsstufen für einen EVG zu formulieren.
- Entwickler müssen den Standard verpflichtend verwenden, um die Anforderungen von Konsumenten in die Sprache der CC zu übersetzen, oder Vorgaben von Gutachtern nachzuschlagen.
- Gutachter verwenden die CC als Referenz und Richtlinie bei der Überprüfung von Schutzprofilen und Sicherheitsprofilen auf ihre Gültigkeit.

3.4 Evaluationskontext

Um die Evaluationsergebnisse vergleichbar zu machen, sollten Evaluationen in einer definierten Umgebung stattfinden, welche Standards setzt, die Qualität der Evaluationen bewertet, und die Regeln festlegt, an die sich Gutachter halten müssen.

Die CC stellt keine Anforderungen an die rechtlichen Rahmenbedingungen; trotzdem sollte sichergestellt werden, dass verschiedene Zertifizierungsstellen unter den gleichen Bedingungen arbeiten – nur so können sie ihre Evaluationsergebnisse vergleichen und gegenseitig anerkennen (2, Seite 37).

Ein Beispiel für die Schaffung von rechtlichen Rahmenbedingungen ist das CCRA (Common Criteria Recognition Agreement). Das CCRA ist die Basis für gegenseitige Anerkennung von CC-Zertifikaten zwischen Zertifizierungsbehörde verschiedener Länder.

Ein Ansatz, um größere Vergleichbarkeit zu garantieren, ist die Verwendung der CEM; sie trägt zur Wiederholbarkeit und Objektivität von Ergebnissen bei, ist aber alleine nicht ausreichend. Viele der Kriterien in einer Evaluation benötigen die Beurteilung durch einen Experten mit Hintergrundwissen, für das Konsistenz schwer sichergestellt werden kann. Um die Konsistenz verschiedener Evaluationen zu erhöhen, können sie durch einen zusätzlichen Zertifizierungsprozess überprüft werden.

Der Zertifizierungsprozess ist eine unabhängige Inspizierung der Evaluationsergebnisse, bei der das letztendliche Zertifikat ausgestellt wird. Er ist ein Mittel, um mehr Konsistenz in der Anwendung von IT-Sicherheitskriterien zu gewährleisten. Die verwendeten Methoden für diese Auswertung und den Zertifizierungsprozess stehen in der Verantwortung der Zertifizierungsstellen und werden von der CC nicht behandelt.

3.5 Sicherheitsmodell

Dieser Abschnitt klärt die Begriffe, mit denen die CC die Elemente der IT-Sicherheit bezeichnet, sowie das Modell, über das diese Begriffe zusammen hängen. Die Konzepte und Terminologie der CC stammen aus der IT-Sicherheit; ein Grundwissen darin wird vorausgesetzt. Die Konzepte sind allgemein; es ist nicht beabsichtigt, durch ihre

Verwendung die IT-Sicherheitsprobleme zu beschränken, auf welche die CC angewendet werden kann (2, Seite 38). Die CC setzt voraus, dass der hier beschriebene Ansatz verwendet wird.

3.5.1 Vermögenswerte, Bedrohungen und Gegenmaßnahmen

Vermögenswerte sind Entitäten, welche der Besitzer als schützenswert erachtet. Die Umgebung, in der ein Vermögenswert existiert, wird als *Einsatzumgebung* bezeichnet. Dabei ist jeder Vermögenswert *Bedrohungen* ausgesetzt, die durch passende *Gegenmaßnahmen* geschützt werden müssen. Abbildung 1 verdeutlicht den Zusammenhang zwischen diesen Konzepten:

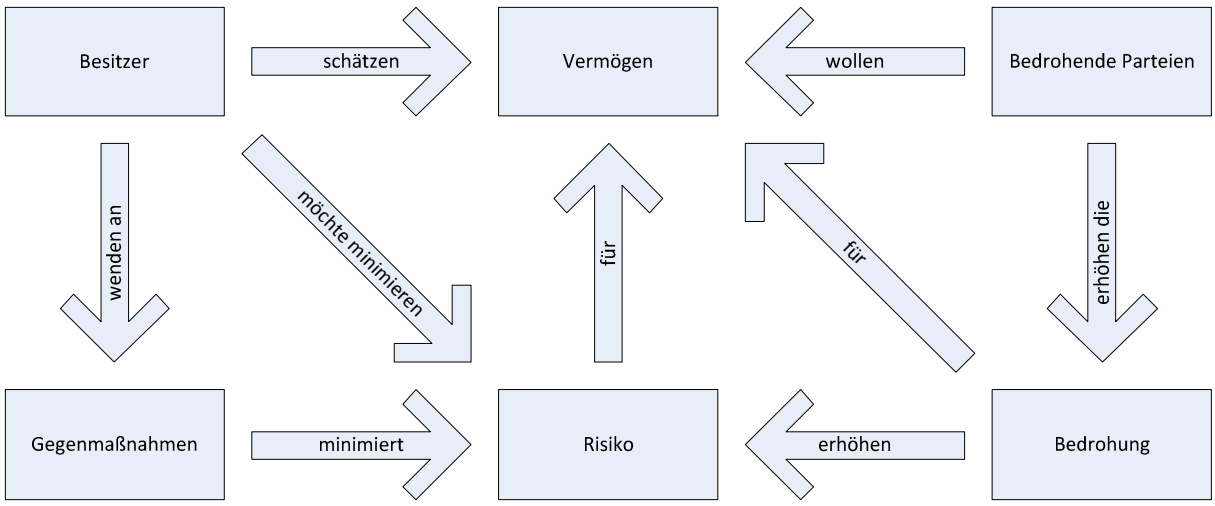


Abbildung 1: Die Bedrohungskonzepte der CC (2, Seite 39)

Konkrete Beispiele für Vermögenswerte in einer Einsatzumgebung, Bedrohungen und Gegenmaßnahmen dazu sind:

- Eine Datenbank liegt auf einem Server, ist über das Internet erreichbar, und muss zum Zugriffsschutz mit einem Passwort verschlüsselt werden.

- Eine Datei auf einem Netzwerklaufwerk darf nur von bestimmten Benutzern gesehen und ausgelesen werden, die Zugriffsrechte werden über eine Rollenbasierte Benutzerverwaltung geregelt.

- Der Computerraum einer Bank darf nur von Administratoren betreten werden, die für den Zutritt eine schwer fälschbare Chipkarte verwenden müssen.

Die Verantwortung eines Besitzers ist es, seine Vermögenswerte zu schützen – die Bedrohung kann echt oder nur angenommen sein, bedeutet aber immer einen unerwünschten Zugriff auf die Ressource, der eine Wertminderung mit sich bringt, und daher nicht im Interesse des Besitzers steht. Diese Wertminderung kann in einem Verlust der Vertrauenswürdigkeit, der Integrität oder Verfügbarkeit auftreten.

Bedrohungsverursacher sind nicht nur bösartige Benutzer, sondern auch unachtsame Personen und Prozesse. Bedrohungsverursacher erhöhen also die Risiken, denen ein Vermögenswert ausgesetzt ist, und Gegenmaßnahmen sollen diese Risiken mindern. Dabei lassen sich nicht alle Gegenmaßnahmen in der IT umsetzen, oft braucht es auch Gegenmaßnahmen außerhalb der IT – z. B. lässt sich eine Datei gegen unerlaubte Zugriffe schützen, trotzdem sollte auch der Zutritt zur Hardware selbst, auf der sie gespeichert ist, nicht für jeden möglich sein.

Der Besitzer eines Vermögenswertes besitzt also eine Verantwortung und muss gegenüber anderen Parteien erklären können, wieso der Vermögenswert Bedrohungen ausgesetzt wird, und zeigen, dass die Gegenmaßnahmen *ausreichend* und *korrekt* sind (Maßnahmen sind ausreichend, wenn sie alle Bedrohungen abdecken, und korrekt, wenn sie ihre Aufgabe erfolgreich erledigen). Gleichzeitig fehlt aber vielen Besitzern das nötige Wissen oder die Ressourcen, um zu beurteilen, ob Gegenmaßnahmen ausreichend und korrekt sind, sowie das Vertrauen, um sich ausschließlich auf das Urteil der Entwickler zu verlassen. In diesem Fall erlaubt eine Evaluation eine unabhängige Überprüfung der Angemessenheit und Korrektheit.

3.5.2 Sicherheitsvorgaben

Bei einer Evaluation wird die Angemessenheit einer Gegenmaßnahme anhand einer sogenannten Sicherheitsvorgabe überprüft. Die Sicherheitsvorgabe beschreibt den Vermögenswert, seine Bedrohungsverursacher und die passenden Gegenmaßnahmen in der Form von Sicherheitsziele. Eine Sicherheitsvorgabe demonstriert, dass diese Gegenmaßnahmen angemessen und korrekt sind.

Die Sicherheitsvorgaben für den EVG werden bei der Evaluation überprüft, die Sicherheitsvorgaben für die Einsatzumgebung aber nicht – das hat folgende Gründe:

- Die CC ist nur geeignet, um die Korrektheit von IT-Gegenmaßnahmen zu beurteilen. Daher sind Maßnahmen außerhalb der IT, wie Wachen oder Prozeduren, immer Teil der Einsatzumgebung.

- Die Beurteilung der Korrektheit von Gegenmaßnahmen kostet Zeit und Geld, was die Überprüfung aller IT-Gegenmaßnahmen unrentabel machen kann.

- Die Korrektheit mancher IT-Gegenmaßnahmen kann bereits in einer anderen Evaluation überprüft worden sein. Es ist daher unrentabel die Korrektheit nochmals zu überprüfen.

Zur detaillierten Beschreibung von Sicherheitsvorgaben für einen EVG werden funktionale Sicherheitsanforderungen verwendet. CC Teil 2 enthält einen Katalog üblicher Sicherheitsanforderungen und stellt somit das Vokabular zur Formulierung von Sicherheitsvorgaben.

Eine Sicherheitsvorgabe demonstriert, dass die funktionalen Sicherheitsanforderungen den Sicherheitsvorgaben des EVG entsprechen, die Sicherheitsziele des EVG und die Sicherheitsziele für die Einsatzumgebung die Bedrohungen abwehren und somit die funktionalen Sicherheitsanforderungen und die Sicherheitsziele für die Einsatzumgebung die Bedrohung abwehren.

Daraus folgt, dass ein korrekter EVG in einer korrekten Einsatzumgebung erwartete Bedrohungen abwehrt – Voraussetzung ist natürlich, dass EVG und Einsatzumgebung ihren Sicherheitsvorgaben entsprechen.

3.5.3 Vertrauenswürdigkeitsanforderungen

In einem EVG können aus verschiedenen Gründen Fehler entstehen: Schlechtes Design, Irrtümer, Fehler in der Entwickler, oder bewusst, durch bösartigen Code. Unabhängig von

ihrer Ursache geben Fehler dem Angreifer eine Möglichkeit, den EVG zu beschädigen oder zu missbrauchen.

Deshalb müssen Fehler vermieden werden, indem der EVG überprüft wird. Die Überprüfung kann an mehreren Stellen ansetzen: Als integrierter Teil des Entwurfsprozesses, durch einen Test des EVG, oder eine nachträgliche Überprüfung der Design-Dokumente oder der physischen Sicherheit der Einsatzumgebung.

Die Aktivitäten, die für so eine Überprüfung notwendig sind, werden mit Vertrauenswürdigkeitsanforderungen beschrieben. Damit diese Anforderungen exakt und vergleichbar sind, wird auch für diese im Teil 3 der CC ein Katalog zur Verfügung gestellt, der übliche Vertrauenswürdigkeitsanforderungen enthält.

Werden Vertrauenswürdigkeitsanforderungen erfüllt, dann gibt es ein Vertrauen in die Korrektheit. Wie hoch das Ausmaß dieses Vertrauens ist, wird von den Vertrauenswürdigkeitsanforderungen selbst bestimmt – es gibt „schwache“ und „starke“ Anforderungen. Ein vertrauenswürdiger EVG bietet dem Anwender die Gewissheit, dass der EVG weniger Schwachpunkte enthält – je strenger die Anforderungen formuliert sind, desto höher ist die Gewissheit, dass die Maßnahmen greifen.

3.5.4 Korrektheit der Einsatzumgebung

Wurde die Einsatzumgebung falsch entworfen oder umgesetzt, dann führt das zu Fehlern, die Schwachpunkte in der Sicherheit ergeben. Diese können von Angreifern ausgenutzt werden, um die Vermögenswerte zu beschädigen oder zu missbrauchen.

Das Vertrauen in die Einsatzumgebung wird in der CC nicht überprüft, statt dessen wir stets angenommen, dass die Einsatzumgebung vollständig den Sicherheitsvorgaben entspricht, die an sie gestellt werden. Trotzdem sollte der Konsument immer sicher stellen, dass die Annahmen an die Einsatzumgebung auch tatsächlich erfüllt werden. Nur so ist die korrekte Funktion des EVG garantiert.

3.5.5 Evaluation

Die CC unterscheidet zwei Arten von Evaluationen:

1. Die Evaluation eines Schutzprofils. Wie später genauer erklärt wird, ist ein Schutzprofil eine allgemeine Formulierung einer Sicherheitsanforderung und bildet die Grundlage für eine Sicherheitsvorgabe. Die Evaluation eines Schutzprofils ist somit die Evaluation der abstrakten Bausteine der Sicherheit.

2. Die Evaluation einer Sicherheitsvorgabe oder eines EVG. Eine Sicherheitsvorgabe ist eine konkrete Anforderung an die Sicherheitsfunktionalität eines EVG, ein EVG erfüllt normalerweise mehrere Sicherheitsvorgaben. Die Evaluation einer Sicherheitsvorgabe oder eines EVG ist somit die Evaluation eines konkreten Sicherheitsprodukts.

Bei der Evaluation nach (2) wird in zwei Schritten vorgegangen: Zuerst werden die Sicherheitsvorgaben evaluiert. Dabei wird die Vollständigkeit des EVGs und der Einsatzumgebung überprüft. Danach kommt es zur EVG-Evaluation, bei der die Korrektheit des EVG festgestellt wird.

Bei der Sicherheitsvorgaben-Evaluation werden die Evaluationskriterien für Sicherheitsvorgaben auf die Sicherheitsvorgabe angewendet. Diese Kriterien werden im CC Teil 3 besprochen, die genaue Methode zur Anwendung der dort beschriebenen Kriterien wird durch die eingesetzte Evaluationsmethodik bestimmt.

Eine EVG-Evaluation ist etwas komplexer: Sie benötigt den Evaluationsbeleg in Form des EVG und der Sicherheitsvorgaben, beinhaltet aber normalerweise auch Informationen aus der Entwicklungsumgebung, wie Design-Dokumente oder Testresultate der Entwickler.

Die EVG-Evaluation besteht aus der Anwendung der Vertrauenswürdigkeitsanforderungen (der Sicherheitsvorgabe) auf den Evaluationsbeleg. Welche Methode dazu angewendet wird, und wie die Vorgänge dokumentiert werden müssen wird von der verwendeten Evaluationsmethodik bestimmt.

Das Ergebnis einer erfolgreichen Evaluation verdeutlicht, ob ausreichend Vertrauen in den EVG besteht, oder nicht. Ausreichendes Vertrauen kann nur hergestellt werden, indem alle Vertrauenswürdigkeitsanforderungen erfüllt worden sind, und somit angenommen werden kann, dass der EVG den Sicherheitsanforderungen aus den Sicherheitsvorgaben entspricht.

Die EVG-Evaluation kann während oder nach der Entwicklung des EVG erfolgen.

3.5.6 Schutzprofile und Pakete

Damit Konsumenten ihre Sicherheitsanforderungen leichter formulieren können, bietet die CC Schutzprofile zur allgemeinen Definition von Sicherheitsfunktionalität sowie Pakete zur Gruppierung von Anforderungen.

Pakete

Ein Paket ist eine Menge von Sicherheitsanforderungen und gruppiert entweder Anforderungen an die Funktion oder Anforderungen an die Vertrauenswürdigkeit – eine Mischung beider ist aber nicht erlaubt (2, Seite 50).

Da es keine Kriterien gibt, nach denen ein Paket beurteilt wird, ist die einzige Anforderung an den Autor eines Pakets, dass es wiederverwendbar und sinnvoll sein soll – das heißt die verwendete Kombination von Anforderungen des Pakets soll nützlich und effektiv sein.

Die CC enthält bisher noch keine Funktionspakete, aber Vertrauenspakete in Form der Vertrauensstufen (EALs), welche in einem späteren Kapitel dieser Arbeit beschrieben sind.

Schutzprofile

Während eine Sicherheitsvorgabe einen konkreten EVG beschreibt, bleibt ein Schutzprofil abstrakt und beschreibt immer einen Typ von EVG – z. B. eine konkrete Firewall im Vergleich zu Firewalls allgemein. Schutzprofile sind somit eine ideale Vorlage für verschiedenste Sicherheitsvorgaben und Evaluationen (2, Seite 50).

Typische Urheber eines Schutzprofils sind folgende Gruppen (2, Seite 50):

- Eine Interessensgemeinschaft von Benutzern, die sich auf allgemeine Anforderungen an eine Art von EVG einigen wollen.

- Die Entwickler eines EVG, oder eine Gruppe von Entwicklern ähnlicher EVGs, die eine Mindestanforderung an diese Art von EVG formulieren wollen.

- Einer Regierung oder eines Konzerns, welche ihre Anforderungen als Teil eines Anschaffungsprozesses formulieren.

Schutzprofile erlauben für die Beschaffung von Produkten mit IT-Sicherheitsfunktionalität folgenden Prozess: Beabsichtigt eine Organisation eine bestimmte Art von IT-Sicherheits-Produkt zu erwerben, dann formuliert sie ihre Sicherheitsbedürfnisse in einem Schutzprofil, lässt dieses überprüfen und veröffentlicht es. Ein Entwickler nimmt dieses Schutzprofil, schreibt eine entsprechende Sicherheitsvorgabe, und lässt diese anschließend evaluieren. Danach erstellt der Entwickler einen EVG oder verwendet einen existierenden, und überprüft ihn anhand der Sicherheitsvorgabe.

Schutzprofile können evaluiert werden. Das Ziel einer solchen Evaluation ist zu demonstrieren, dass das Schutzprofil komplett, konsistent und technisch in Ordnung ist und als Vorlage für weitere Schutzprofile und Sicherheitsvorgaben geeignet ist.

Ein Schutzprofil kann auf ein evaluiertes Schutzprofil oder einer evaluierten Sicherheitsvorgabe aufgebaut werden. Das hat die Vorteile, dass das Risiko von Fehlern verkleinert wird und gleichzeitig der Aufwand für die Evaluation des neuen Schutzprofils sinkt, da einmal evaluierte Elemente nicht erneut evaluiert werden müssen.

Da der Entwickler so belegen kann, dass sein EVG den Sicherheitsbedürfnissen der Organisation entspricht, kann die Organisation diesen erwerben. Der gleiche Ablauf trifft auf Pakete zu.

Wie exakt Schutzprofile aufgebaut sein müssen, beschreibt das Kapitel 4.2 ab Seite 48.

Konformität

Die CC erlaubt, dass Pakete und Schutzprofile zueinander konform sein können; dies erlaubt unter anderem eine Verkettung von Schutzprofilen, bei der ein Schutzprofil immer auf seinen Vorgänger aufbaut; dies bedeutet aber auch, dass seine Vorgaben eingehalten werden müssen, um eine Evaluation erfolgreich zu bestehen. Ob die Konformität tatsächlich eingehalten wird, bestimmt eine Evaluation der Sicherheitsvorgaben.

Der sogenannte *Konformitätsanspruch* verweist auf die Quelle der Anforderungen, welche vom Schutzprofil oder der Sicherheitsvorgabe erfüllt werden. Er besteht aus einem Verweis auf verwendete Version der CC, die Art der Konformität zu den Funktionsklassen aus CC Teil 2, sowie der Sicherheitsanforderungen aus CC Teil 3.

Der Konformitätsanspruch kann die Konformität von Paketen oder Schutzprofilen entweder als konform oder erweitert beschreiben: Ist sie konform, dann werden nur Funktionsklassen aus den Katalogen der CC-Teile 2 und 3 verwendet. Ist der Konformitätsanspruch erweitert, dann werden auch Elemente verwenden, die nicht in der CC enthalten sind.

3.5.7 Evaluationsergebnisse

Eine Evaluation soll zu objektiven und wiederholbaren Ergebnissen führen (2, Seite 55), die als Beweis angeführt werden können, auch wenn es nicht möglich ist, eine absolute Skala der Objektivität zu definieren, auf der das Evaluationsergebnis repräsentiert wird. Die Existenz einer Menge von Evaluationskriterien ist eine notwendige Voraussetzung für eine Evaluation, um ihren Ergebnissen eine Bedeutung zu geben und eine technische Basis zu liefern, die es ermöglicht, dass Zertifizierungsstellen Evaluationsergebnisse gegenseitig anerkennen.

Das Evaluationsergebnis beinhaltet die Ergebnisse einer bestimmten Art von Untersuchung der Sicherheitseigenschaften eines EVG. So ein Ergebnis garantiert aber nicht, dass der EVG in jeder beliebigen Einsatzumgebung verwendet werden kann. Die Entscheidung, einen EVG für eine bestimmte Einsatzumgebung zu verwenden, ist abhängig von der Berücksichtigung vieler Sicherheitsprobleme, welche die Evaluationsergebnisse beinhalten.

Evaluationsergebnisse eines Schutzprofils

Die CC enthält die Kriterien für eine Evaluation, mit denen beurteilt werden kann, ob ein Schutzprofil vollständig, konsistent und technisch einwandfrei ist, und somit zur Entwicklung einer Sicherheitsvorgabe verwendet werden kann. Die Evaluation eines Schutzprofils muss nur sagen, ob das Schutzprofil die Evaluation bestanden hat, oder durchgefallen ist. Wenn es besteht, ist es berechtigt, in ein Verzeichnis von Schutzprofilen aufgenommen zu werden. Die Evaluationsergebnisse sollten auch einen Konformitätsanspruch enthalten.

Evaluationsergebnisse einer Sicherheitsvorgabe oder eines EVG

Die CC enthalten die Evaluationskriterien, mit denen ein Gutachter beurteilen kann, ob ausreichend Vertrauen besteht, dass der EVG den Sicherheitsanforderungen der Sicherheitsvorgabe entspricht. Die Evaluation eines EVG sollte daher als Ergebnis aussagen, ob der Evaluation bestanden worden ist, oder ob der evaluierte Gegenstand durchgefallen ist. Wenn sowohl die Evaluation der Sicherheitsvorgabe und die des EVG bestanden worden sind, dann soll das zugrundeliegende Produkt in ein Verzeichnis aufgenommen werden können. Das Evaluationsergebnis sollte auch einen Konformitätsanspruch enthalten – er wird im nächsten Abschnitt beschrieben.

Evaluationsergebnisse können für einen Zertifizierungsprozess verwendet werden; dieser Prozess ist aber kein Teil der CC.

Sobald eine Sicherheitsvorgabe und ein EVG evaluiert worden sind, können die Besitzer eines Vermögenswertes darauf vertrauen, dass des EVG, zusammen mit der Einsatzumgebung, die Bedrohungen abwehrt. Dadurch kann der Besitzer entscheiden, ob er das Risiko eingehen möchte, seinen Vermögenswert den gegebenen Bedrohungen auszusetzen.

Der Besitzer des Vermögens sollte aber gründlich überprüfen, ob die Definition des Sicherheitsproblems in den Sicherheitsvorgaben seinem tatsächlichen Problem entspricht, und die Einsatzumgebung die Vorgaben erfüllt. Falls einer dieser zwei Punkte nicht erfüllt wird, kann der EVG für die Zwecke des Besitzers ungeeignet sein.

Es kann passieren, dass Schwachstellen eines EVG erst bemerkt werden, wenn er bereits im Einsatz ist. Ein Entwickler kann dann entweder die Schwachstellen des EVG oder die Sicherheitsvorgaben anpassen – in beiden Fällen verfällt aber die Gültigkeit einer bestehenden Evaluation und macht eine neue Evaluation nötig.

4 Spezifikation von Sicherheitsvorgaben und Schutzprofilen

4.1 Spezifikation von Sicherheitsvorgaben

4.1.1 Rolle und Aufbau

Die Sicherheitsvorgabe ist Vereinbarung zwischen Gutachter und Entwickler und beschreibt exakt, was evaluiert werden soll. Außerdem ist sie eine abstrakte Beschreibung der Sicherheitseigenschaften des EVGs für potentielle Kunden. Deshalb ist es wichtig, dass die Sicherheitsvorgabe technisch korrekt, vollständig und verständlich formuliert ist.

Sie ist jedoch weder eine detaillierte noch eine vollständige Spezifikation der Sicherheitseigenschaften eines EVG. Die Sicherheitsvorgabe ist abstrakt und allgemein und enthält keine Details der Implementierung wie Informationen über Protokolle, Algorithmen oder Mechanismen. Details sind nur so weit enthalten, wie die Sicherheit davon betroffen ist – zum Beispiel, wenn die Größe oder das Gewicht des EVG eine besondere Rolle spielen.

Nach der Evaluierung spezifiziert die Sicherheitsvorgabe „was evaluiert worden ist“. In dieser Rolle dient die Sicherheitsvorgabe als eine gemeinsame Vereinbarung zwischen dem Entwickler oder Verkäufer und dem potentiellen Kunden des EVG. Die Sicherheitsvorgabe beantwortet unter anderem, ob sie den Anforderungen des Kunden entspricht, in die bestehende IT-Infrastruktur und Einsatzumgebung passt, was sie genau macht und wie vertrauenswürdig sie ist.

Eine Sicherheitsvorgabe besteht verbindlich aus folgenden Elementen:

- Einer Einleitung der Sicherheitsvorgabe, in welcher der EVG auf drei verschiedenen Abstraktionsebenen beschrieben wird.

- Einem Konformitätsanspruch, der klärt, zu welchen Schutzprofilen oder Paketen die Sicherheitsvorgabe konform ist.

- Eine Definition des Sicherheitsproblems mit einer Beschreibung der Bedrohungen, der organisatorischen Sicherheitspolitik, und den Sicherheitsvorgaben für die Einsatzumgebung des EVG.

- Sicherheitsziele die zeigen, wie das Sicherheitsproblem zwischen dem EVG und der Einsatzumgebung verteilt wird.

- Definition der erweiterten Komponenten, in der Komponenten definiert werden, die nicht in CC Teil 2 oder 3 definiert sind. Diese Komponenten beschreiben erweiterte Sicherheitsanforderungen und erweiterte Vertrauenswürdigkeitsanforderungen.

- Sicherheitsanforderungen, in denen die Sicherheitsziele des EVG in eine standardisierte Sprache übersetzt werden. Diese Sprache wird durch die Sicherheitsanforderungen ausgedrückt. Dieser Abschnitt definiert auch die Vertrauenswürdigkeitsanforderungen.

- Eine EVG-Kurzspezifikation, welche zeigt, wie die Sicherheitsanforderungen im EVG implementiert sind.

Abbildung 2 enthält alle verpflichtenden Inhalte einer Sicherheitsvorgabe. Sie kann als Vorlage verwendet werden, es sind aber auch andere Darstellungen möglich:

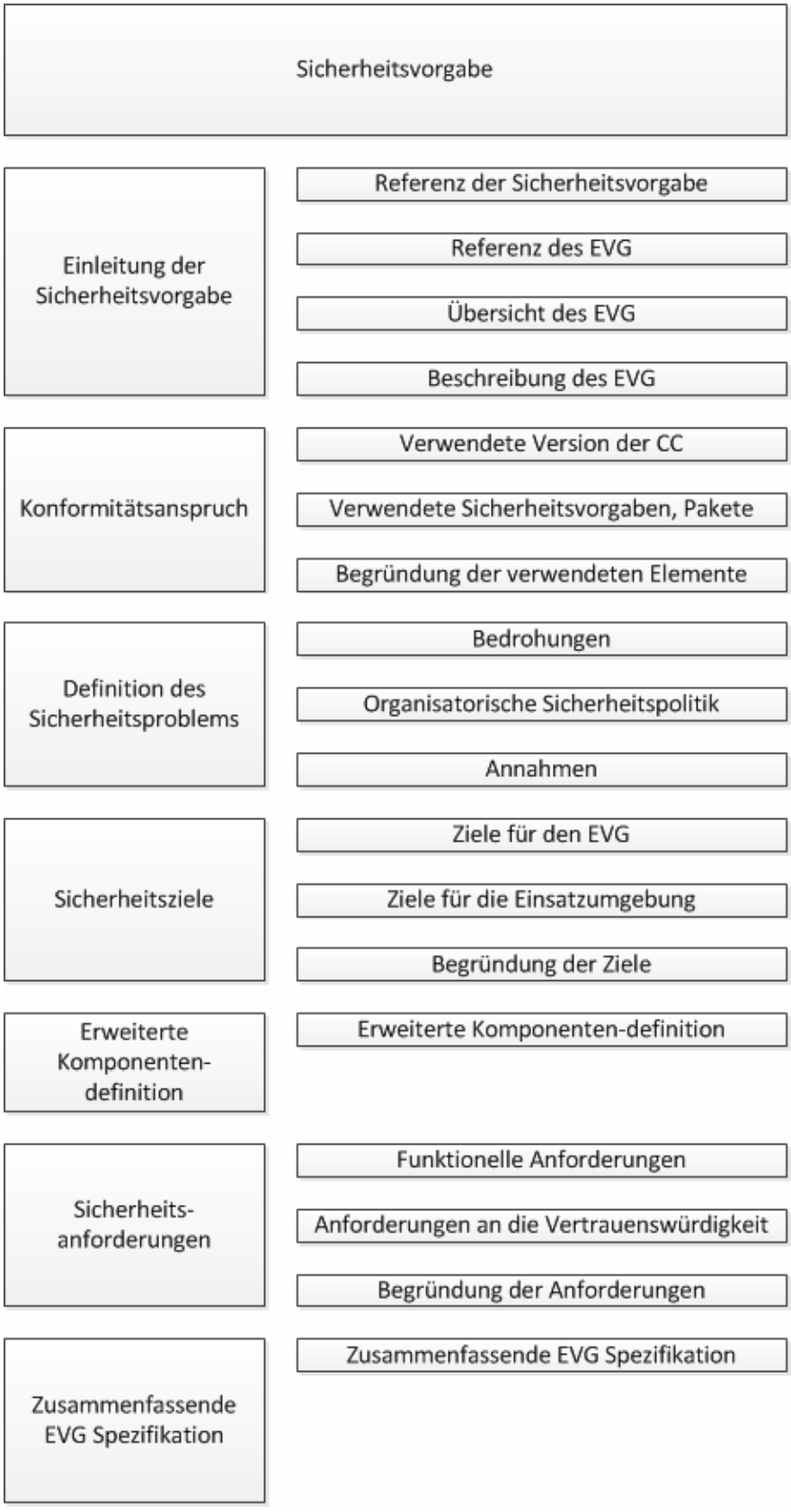


Abbildung 2: Aufbau einer Sicherheitsvorgabe (2, Seite 60)

4.1.2 Einleitung der Sicherheitsvorgabe

Die Einleitung der Sicherheitsvorgabe schildert den EVG auf drei Abstraktionsebenen über einen Referenznamen, eine Übersicht und eine Beschreibung.

Der Referenzname ist die eindeutige Bezeichnung für die Sicherheitsvorgabe und sollte stets verwendet werden, wenn auf diese Sicherheitsvorgabe Bezug genommen wird. Die Referenz besteht normalerweise aus dem Titel, der Version, den und dem Datum der Veröffentlichung.

Die EVG-Übersicht soll potentiellen Kunden bei der Entscheidung helfen, ob der EVG für sie geeignet ist. Die Übersicht ist wenige Absätze lang und beschreibt in Kürze die Art und Verwendung des EVG, seine Sicherheitseigenschaften und die benötigte Hard-, Soft- und Firmware.

Die EVG-Beschreibung schildert auf mehreren Seiten detailliert die Sicherheitseigenschaften eines EVGs. Dazu enthält sie auch eine Beschreibung der benötigten Hard-, Soft- und Firmware und der Einsatzumgebung. Gutachter und potentielle Kunden sollen ein vollständiges Bild vom EVG erhalten, unmissverständlich alle Sicherheitseigenschaften kennen lernen und wissen, welche Teile innerhalb des EVG liegen und welche außerhalb (und somit in der Einsatzumgebung).

4.1.3 Konformitätsanspruch

Der Konformitätsanspruch enthält die verwendete Version der CC und eine Liste aller Schutzprofile und Pakete, zu denen die Sicherheitsvorgabe konform ist. Außerdem wird erwähnt, ob erweiterte Sicherheitsanforderungen verwendet werden, oder nicht.

4.1.4 Definition des Sicherheitsproblems

Die Definition enthält eine Beschreibung des Sicherheitsproblems, welches gelöst werden soll. Es gibt zwar keine Vorgaben für die Formulierung der Beschreibung, jedoch ist zu beachten, dass nur eine gute Definition des Sicherheitsproblems zu einer guten Lösung führt.

Bei der Beschreibung des Sicherheitsproblems müssen nicht alle hier in Folge erwähnten Punkte enthalten sein – so ist es möglich, die organisatorische Sicherheitspolitik oder Annahmen auszulassen, wenn keine Maßnahmen in diesen Bereichen notwendig sind; es müssen aber immer entweder die Bedrohungen oder die organisatorische Sicherheitspolitik beschrieben werden. Ist der EVG physisch verteilt, dann kann es von Vorteil sein, das Sicherheitsproblem für jede Komponente separat zu besprechen.

Bedrohungen

Dieser Abschnitt beschreibt die Bedrohungen, welchen der EVG und seine Einsatzumgebung begegnen müssen. Eine Bedrohung besteht aus einer Ursache, der Art der bedrohlichen Aktion und dem betroffenen Vermögenswert.

Organisatorische Sicherheitspolitik

Falls eine Organisation den EVG zum Einsatz bringt, dann muss sie die hier beschriebenen Regeln umsetzen und befolgen – je nach Beschreibung müssen sie im EVG oder in der Einsatzumgebung umgesetzt werden.

Annahmen

Dieser Abschnitt enthält die Annahmen über die Einsatzumgebung, die erfüllt sein müssen, damit Sicherheitsfunktionalität gewährleistet werden kann. Die Annahmen können sich auf den Ort, das Personal oder die Anbindung des EVG beziehen.

Bei der Evaluation werden alle Annahmen als erfüllt betrachtet und werden nicht weiter getestet. Es können keine Annahmen über EVGs selbst gemacht werden, da die Evaluation schon Annahmen über den EVG macht, die sie dann auch überprüft.

4.1.5 Sicherheitsziele

Beschreibung

Die Sicherheitsziele beschreiben in abstrakter aber natürlicher Sprache die Lösung des Sicherheitsproblems, wobei die Beschreibung drei Rollen hat:

Die Sicherheitsziele bestehen aus kurzen und klar formulierten Aussagen, welche eine oberflächliche Lösung des Sicherheitsproblems beschreiben. Die Abstraktion ist in natürlicher Sprache formuliert und sollte für potentielle Kunden verständlich sein. Eine genauere Beschreibung der Sicherheitsziele erfolgt als Teil der Sicherheitsanforderungen.

Danach werden die Sicherheitsziele nach ihrer Zugehörigkeit zum EVG oder zur Einsatzumgebung aufgeteilt. Sicherheitsziele für die Einsatzumgebung werden meistens durch technische oder prozedurale Maßnahmen ausgedrückt, die den Betrieb des EVGs sichern sollen.

Die Sicherheitsvorgabe enthält auch eine Sicherheitszielbegründung, die erklärt, welche Sicherheitsziele welche Bedrohungen, organisatorische Sicherheitspolitik und Annahmen behandeln, und zeigt darüber hinaus, dass alle Sicherheitsziele zusammen das Sicherheitsproblem beseitigen, wobei es reicht, wenn die Bedrohung auf ein harmloses Maß reduziert wird.

Verfolgung zwischen Vorgaben und Problemdefinition

Die Verfolgung zeigt den Zusammenhang zwischen den Sicherheitsvorgaben und den dazu gehörenden Maßnahmen (gegen Bedrohungen, in der organisatorischen Sicherheitspolitik, oder in den Annahmen), wobei manchmal mehrere Sicherheitsziele nötig sein können, um eine einzige Bedrohung abzuwehren.

Die Verfolgungen müssen relevant, vollständig und korrekt sein. Alle Sicherheitsziele müssen erfüllt werden, sowie notwendig und sinnvoll sein. Sicherheitsziele können nicht zu Annahmen verfolgt werden. Abbildung 3 zeigt die erlaubten Verfolgungen.

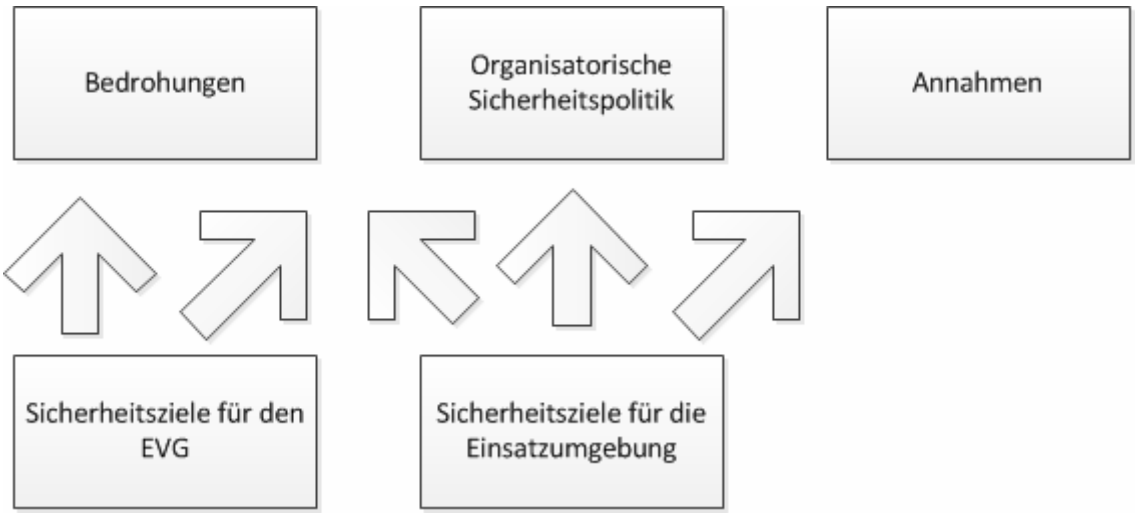


Abbildung 3: Wie Sicherheitsziele sich auf Bedrohungen, Sicherheitspolitik und Annahmen beziehen (2, Seite 70)

Rechtfertigung der Verfolgung

Die Begründung der Sicherheitsziele demonstriert auch, dass die Verfolgung effektiv ist und analysiert dafür den Effekt, der sich ergibt, wenn die relevanten Sicherheitsziele umgesetzt werden. Das Ergebnis sollte zeigen, dass alle Vorgaben tatsächlich erfüllt werden.

Bedrohungen entgegnen

Einer Bedrohung zu begegnen bedeutet nicht unbedingt, dass die Bedrohung entfernt wird; es kann auch bedeuten, dass man sie vermindert oder entschärft. Wichtig ist nur, dass sie auf ein Ausmaß reduziert wird, dass die Bedrohung unwirksam macht.

Sicherheitsziele: Fazit

Aus den Sicherheitszielen und ihrer Begründung kann man folgen, dass die Erfüllung der Sicherheitsziele das in ASE_SPD beschriebene Sicherheitsproblem löst.

4.1.6 Definition erweiterter Komponenten

Oft basieren die Sicherheitsanforderungen einer Sicherheitsvorgabe auf Komponenten aus CC Teil 2 oder CC Teil 3 – wenn das nicht der Fall ist, dann definiert man hierfür in diesem Abschnitt die sogenannten *erweiterte Komponenten*.

4.1.7 Sicherheitsanforderung

Sicherheitsanforderungen werden in zwei Gruppen unterteilt, Anforderungen an die Funktionen und Anforderungen an die Vertrauenswürdigkeit. Beide Arten werden ähnlich definiert und begründet:

Formulierung

Formuliert werden die Anforderungen mit einer standardisierten Sprache, welche den exakten Ausdruck und die Vergleichbarkeit von Anforderungen fördert. Für Anforderungen an die Funktion ist diese Sprache der Katalog des Teil 2 der CC, für die Anforderungen an die Vertrauenswürdigkeit der Katalog des Teil 3.

Sämtliche Anforderungen können über Operatoren im Detail angepasst werden. Es können auch Abhängigkeiten definiert werden, bzw. müssen Abhängigkeiten immer erfüllt sein – so lassen sich notwendige Anforderungen an die Sicherheit und das Vertrauen nur schwer übersehen.

Begründung

Die Sicherheitsvorgabe enthält eine Begründung aller funktionalen Sicherheitsanforderungen, die zeigen muss, dass die Sicherheitsziele effektiv und vollständig behandelt werden. Jede Anforderung sollte sich zu einem Sicherheitsziel verfolgen lassen, und dabei sollten alle Sicherheitsziele abgedeckt werden. Es ist möglich, dass manche Sicherheitsziele nur durch eine Kombination von Anforderungen erfüllt werden. Die Begründung muss auch demonstrieren, dass die Verfolgung zwischen Anforderungen und Zielen effektiv ist, also ihre Einhaltung die Sicherheitsziele erfüllt.

Für die Vertrauenswürdigkeitsanforderungen hat der Aufbau der Begründung keine Vorgaben und kann frei formuliert werden; die Begründung sollte aber nachvollziehbar und angemessen sein.

Gibt es keine Anforderungen, dann ist dies ebenfalls ausdrücklich anzumerken.

Sicherheitsanforderungen: Fazit

In diesem Abschnitt wird das Sicherheitsproblem als eine Menge von Bedrohungen, Maßnahmen der organisatorischen Sicherheitspolitik und Annahmen definiert. Im Abschnitt der Sicherheitsziele der Sicherheitsvorgabe wird die Lösung in Form von zwei Teillösungen präsentiert, als Sicherheitsziele für den EVG und die Einsatzumgebung. Zusätzlich zeigt die Beschreibung der Sicherheitsziele, dass das Sicherheitsproblem gelöst ist, wenn alle Sicherheitsziele erfüllt werden.

4.1.8 EVG-Übersichtsspezifikation

Die EVG-Übersichtsspezifikation soll einen potentiellen Kunden informieren, wie der EVG alle Vertrauenswürdigkeitsanforderungen erfüllt. Sie muss eine Beschreibung der allgemeinen technischen Mechanismen bieten, welche der EVG für diesen Zweck verwendet. Die Spezifikation muss detailliert genug sein, um einem potentiellen Kunden die Form und Umsetzung des EVG verständlich zu machen.

4.1.9 Bezugnahme auf andere Standards

In manchen Fällen möchte sich der Autor einer Sicherheitsvorgabe auf einen externen Standard beziehen (wie zum Beispiel auf einen kryptographischen Standard oder ein Protokoll). Dies kann auf drei Arten erfolgen:

- Über die organisatorische Sicherheitspolitik: Wenn es z. B. einen Standard gibt, wie Regierungsorganisationen das Passwort zu wählen haben, dann kann dies in den Sicherheitszielen für die organisatorischen Sicherheitspolitik der Sicherheitsvorgabe definiert werden. Dies kann wiederum zu Vorgaben für die Umgebung führen (wenn zum Beispiel die Benutzer des EVG das Passwort

entsprechend dem Standard wählen müssen), oder es führt zu Sicherheitsvorgaben des EVG und somit zu passenden funktionalen Sicherheitsanforderungen, wenn der EVG Passwörter generieren soll. In beiden Fällen muss der Entwickler in der Begründung verständlich machen, dass die Sicherheitsvorgaben des EVG und die funktionalen Sicherheitsanforderungen ausreichend sind, um die organisatorische Sicherheitspolitik zu erfüllen. Der Gutachter wird danach betrachten, ob das tatsächlich der Fall ist und die organisatorische Sicherheitspolitik von den funktionalen Sicherheitsanforderungen umgesetzt wird – wobei es auch nötig sein kann, dass der Gutachter sich zuerst näher mit dem referenzierten Standard beschäftigt.

- Als technischer Standard (z. B. ein kryptografischer Standard), der zur Verfeinerung eines funktionalen Sicherheitsanforderung verwendet wird. In diesem Fall ist die Konformität zum Standard ein Teil der Erfüllung der funktionalen Sicherheitsanforderung des EVG und wird somit auch so behandelt, als wäre der vollständige Text des Standards Teil der funktionalen Sicherheitsanforderung. Wenn nur auf einen Teil eines Standards Bezug genommen wird, dann sollte dieser Teil in der Verfeinerung der funktionalen Sicherheitsanforderung unmissverständlich erwähnt werden.

- Als technischer Standard (z. B. ein kryptografischer Standard), der in der EVG-Übersichtsspezifikation erwähnt wird. Die EVG-Übersichtsspezifikation beschreibt nur, wie die funktionalen Sicherheitsanforderungen umgesetzt werden, und wird nicht als genaue Anforderung für die Entwicklung angesehen, anders als die funktionalen Sicherheitsanforderungen. Der Gutachter muss also eine Inkonsistenz erkennen, wenn die EVG-Übersichtsspezifikation einen technischen Standard referenziert, der in den weiteren Teilen nicht mehr erwähnt wird. Es gibt jedoch keine allgemein übliche Aktivität, um die Erfüllung dieses Standards zu überprüfen.

4.1.10 Sicherheitsvorgaben mit geringer Vertrauenswürdigkeit

Wenn eine Evaluation geringe Vertrauenswürdigkeit feststellen soll, kann das Schreiben der Sicherheitsvorgaben mehr Zeit beanspruchen, als die Gutachter mit der Evaluation verbringen. Daher ist es auch möglich Sicherheitsvorgaben, die nur Vertrauenswürdigkeit nach EAL1 bieten sollen, mit stark verkürztem Inhalt zu definieren: Eine *Sicherheitsvorgabe*

mit geringer Vertrauenswürdigkeit hat keine Sicherheitsproblemdefinition, keine Sicherheitsziele und keine Begründung für diese. Was somit bleibt, sind:

- Die Referenzen auf andere EVGs und Sicherheitsvorgaben.
- Der Konformitätsanspruch.
- Die Schilderung der EVG-Übersicht, der EVG-Beschreibung und der EVG-Übersichtsspezifikation.
- Die Sicherheitsziele für die Einsatzumgebung.
- Die funktionalen Sicherheitsanforderungen und die Vertrauenswürdigkeitsanforderungen (einschließlich der Definition erweiterter Komponenten) und die Begründung der Sicherheitsanforderungen (aber nur, wenn Abhängigkeiten nicht erfüllt werden).

Eine Sicherheitsvorgabe mit geringer Vertrauenswürdigkeit kann nur zu einem Schutzprofil mit geringer Vertrauenswürdigkeit konform sein, wobei auch normale Sicherheitsvorgaben zu Schutzprofilen mit geringer Vertrauenswürdigkeit konform sein können.

Abbildung 4 illustriert die Inhalte einer gekürzten Sicherheitsvorgabe im Vergleich zur vollständigen Variante. Zum besseren Vergleich werden Inhalte, die entfallen, durchgestrichen dargestellt.

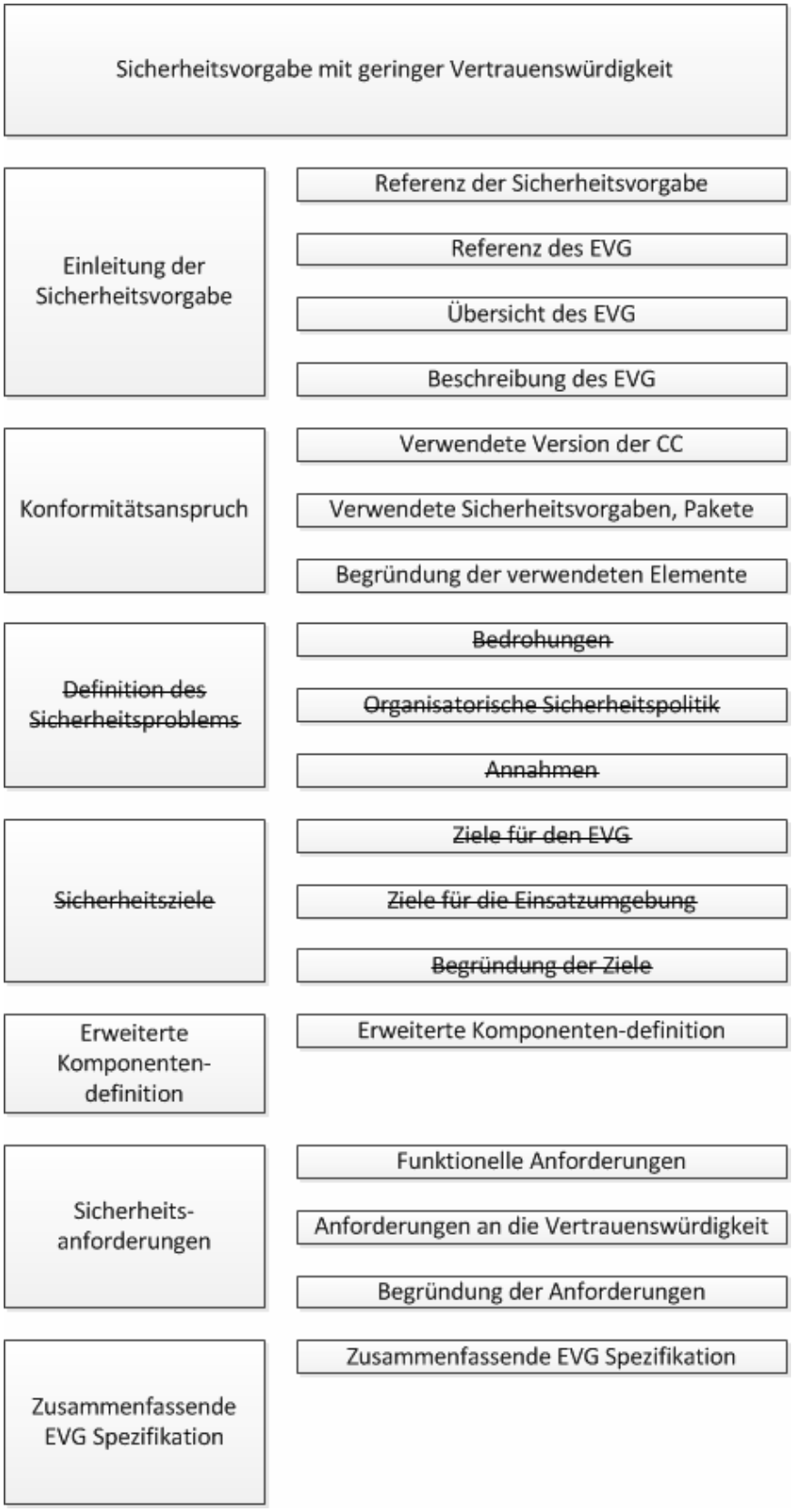


Abbildung 4: Aufbau einer gekürzten Sicherheitsvorgabe

4.2 Spezifikation von Schutzprofilen

4.2.1 Rolle und Aufbau

Schutzprofile sind abstrakte Sicherheitsvorgaben. Sie halten ihre Inhalte bewusst allgemein, um als Grundlage für Sicherheitsvorgaben verwendet zu werden. Aus dieser Beziehung ergeben sich viele Gemeinsamkeiten im Aufbau von Sicherheitsvorgaben und Schutzprofilen (2, Seite 79). Deshalb verweist dieses Kapitel wo möglich auf die existierende Beschreibung von Sicherheitsvorgaben und konzentriert sich vor allem auf die Unterschiede.

Typischerweise ist ein Schutzprofil eine Erklärung einer Benutzergemeinschaft, einer Regulierungsbehörde oder eine Gruppe von Entwicklern, in welcher eine Menge von gemeinsamen Sicherheitsbedürfnissen festgehalten wird. Ein Schutzprofil gibt dem Konsumenten einen Bezugspunkt für diese Sicherheitsbedürfnisse und erleichtert ihre zukünftige Evaluation. Typischerweise wird ein Schutzprofil für folgende Zwecke verwendet:

- Teil der Bedarfsspezifikation für einen spezifischen Konsumenten oder eine Gruppe von Konsumenten, welche ein bestimmtes IT-Produkt kaufen möchte, sofern es den Schutzprofilen entspricht.

- Teil einer Richtlinie einer Regulierungsbehörde, welche nur eine Art IT-Produkt zulässt, die dem Schutzprofil entspricht.

- Basis für eine Gruppe von IT-Entwicklern, welche sich darauf einigen, alle IT-Produkte des beschriebenen Typs nach den vereinbarten Vorgaben zu entwickeln.

Ein Schutzprofil ist jedoch weder eine detaillierte, vollständige Produktspezifikation. Sie ist eine Sicherheitsspezifikation mit hohem Abstraktionsgrad und enthält keine konkreten Details einer Implementierung.

Die einzelnen Abschnitte eines Schutzprofils und deren Inhalte sind zusammengefasst folgende:

- Die Schutzprofil-Einleitung enthält eine Schilderung des EVG-Typen.

- Der Konformitätsanspruch zeigt, zu welchen anderen Schutzprofilen oder Paketen Konformitätsansprüche bestehen.

- Die Sicherheitsproblemdefinition zeigt die Bedrohungen, organisatorische Sicherheitspolitik und Annahmen, welche vom EVG und seiner Einsatzumgebung beseitigt, umgesetzt und bestätigt werden müssen.

- Die Sicherheitsziele zeigen, dass die Lösung des Sicherheitsproblems zwischen dem EVG und der Einsatzumgebung aufgeteilt ist.

- Definition der erweiterten Komponenten, in welcher neue (erweiterte) Komponenten definiert werden können. Mit diesen erweiterten Komponenten werden erweiterte Funktionalität und Vertrauensanforderungen spezifiziert.

- Sicherheitsanforderungen, in denen die Sicherheitsziele des EVG in eine standardisierte Sprache übersetzt werden, die durch funktionale Sicherheitsanforderungen dargestellt werden. Zusätzlich definiert dieser Abschnitt Vertrauenswürdigkeitsanforderungen.

Abbildung 5 zeigt die verbindlichen Inhalte eines Schutzprofiles; sie kann auch als struktureller Umriss eines Schutzprofils verwendet werden, auch wenn ein anderer Aufbau möglich ist (z. B. können längere Erklärungen in Anhänge ausgelagert werden).

Abbildung 5: Aufbau eines Schutzprofiles. (2, Seite 85)

Ein Schutzprofil hat keine EVG-Übersichtsspezifikation.

4.2.2 Schutzprofil-Einleitung

Eine Schutzprofil-Einleitung beschreibt den EVG auf zwei Abstraktionsebenen: Durch die Schutzprofil-Referenz und die EVG-Übersicht. Die Referenz folgt dem Aufbau der Referenz von Sicherheitsvorgaben, die Übersicht hat auch hier die Rolle, einem potentiellen Anwender eine Übersicht der Sicherheitsfunktion zu geben, die in natürlicher Sprache formuliert ist.

4.2.3 EVG-Typ

Die EVG-Übersicht identifiziert die allgemeine Art von EVG (wie z. B. Firewall, Smart Card oder LAN).

4.2.4 Konformitätsansprüche

Der Konformitätsanspruch beschreibt, zu welchen anderen Schutzprofilen und Paketen Konformität besteht. Er ist identisch mit dem Abschnitt „Konformitätsansprüche“ der Sicherheitsvorgaben, unterscheidet sich aber in der Konformitätsaussage, die nun beschreibt, wie eine Sicherheitsvorgabe oder ein Schutzprofil konform zu dem Schutzprofil sein muss: strikt oder demonstrierbar.

4.2.5 Gemeinsamkeiten mit Sicherheitsvorgaben

Die Sicherheitsproblemdefinition, Sicherheitsziele, Sicherheitsanforderungen und Definition erweiterter Komponenten decken sich in ihren Inhalten mit jenen einer Sicherheitsvorgabe. Lediglich die Regeln zum Abschließen von Operationen in einem Schutzprofil sind etwas anders als jene für Sicherheitsvorgaben.

Auch Schutzprofile können sich auf fremde Standards beziehen, der Autor eines Schutzprofils sollte aber beachten, dass eine Bezugnahme auf einen Standard in einer Sicherheitsanforderung eine große Last für den Entwickler bedeuten kann – womöglich gibt es Wege außerhalb der CC, die bei der Erfüllung dieses Standards helfen können, und dem Entwickler gleichzeitig den Aufwand abnehmen.

4.2.6 Schutzprofile mit geringer Vertrauenswürdigkeit

Ein Schutzprofil mit geringer Vertrauenswürdigkeit hat dieselbe Beziehung zu einem normalen Schutzprofil, wie eine Sicherheitsvorgabe mit geringer Vertrauenswürdigkeit zu einer normalen Sicherheitsvorgabe. Das bedeutet, dass ein Schutzprofil mit geringer Vertrauenswürdigkeit aus folgenden Teilen besteht:

- Schutzprofil-Einleitung, besteht aus einer Schutzprofil-Referenz und einer EVG-Übersicht.
- Konformitätsanspruch.
- Sicherheitsziele für die Einsatzumgebung.
- Die funktionalen Sicherheitsanforderungen und die Vertrauenswürdigkeitsanforderungen (einschließlich der Definition erweiterter Komponenten) und die Begründung der Sicherheitsanforderungen (aber nur, wenn Abhängigkeiten nicht erfüllt werden).

Ein Schutzprofil mit geringer Vertrauenswürdigkeit kann nur zu anderen Schutzprofilen mit geringer Vertrauenswürdigkeit konform sein; ein normales Schutzprofil kann aber auch zu einem Schutzprofil mit geringer Vertrauenswürdigkeit konform sein.

Der gekürzte Inhalt eines Schutzprofils mit geringer Vertrauenswürdigkeit wird in Abbildung 6 gezeigt. Zum besseren Vergleich werden Inhalte, die entfallen, durchgestrichen dargestellt.

Abbildung 6: Schutzprofil mit geringer Vertrauenswürdigkeit.

4.3 Sicherheitsanforderungen

4.3.1 Einleitung

Sicherheitsanforderungen sind Teile von Paketen, Schutzprofilen und Sicherheitsvorgaben. Die CC basiert auf der Annahme, dass diese Anforderungen von den vordefinierten Funktionskomponenten aus CC Teil 2 oder den Vertrauenswürdigkeitskomponenten aus CC Teil 3 abgeleitet werden, die dann durch Operationen angepasst werden können. Die Komponenten aus den Katalogen repräsentieren die bevorzugte Art, Sicherheitsanforderungen auszudrücken, denn sie basieren auf Erfahrung und beschreiben eine bekannte und verstandene Domäne.

4.3.2 Komponenten der Kataloge

Die Komponenten der Kataloge werden in eine Hierarchie aus Klassen, Familien, Komponenten und Elementen unterteilt. Eine genaue Beschreibung dieser Hierarchie findet sich im Kapitel 5.

Komponenten können voneinander abhängig sein. Die Standard-Komponenten haben nur Abhängigkeiten innerhalb ihrer Kataloge (Funktionskomponenten untereinander und Vertrauenswürdigkeitskomponenten untereinander, aber nie Katalog-übergreifend); erweiterte Komponenten können aber sehr wohl Abhängigkeiten zu beliebigen anderen Komponenten haben. In bestimmten Fällen kann es notwendig sein, dass auf der Sicherheitsanforderung Operationen (Zuweisung, Iteration, Verfeinerung, Auswahl) ausgeführt werden müssen, um sicher zu stellen, dass die Abhängigkeit auch tatsächlich erfüllt wird.

Wir die Abhängigkeit nicht erfüllt, dann muss der Autor zeigen, dass die Abhängigkeit von einer anderen inkludierten Anforderung erfüllt wird, von der Einsatzumgebung behandelt wird, oder sonst begründen, warum sie nicht nützlich oder notwendig ist.

4.4 Operationen

Die Funktions- und Vertrauenskomponenten der CC können genau so verwendet werden, wie in der CC beschrieben, sie können aber auch durch erlaubte Operationen verändert werden. Bei der Verwendung von Operationen sollte der Autor beachten, dass die Sicherheitsanforderungen von abhängigen Anforderungen nach wie vor erfüllt werden. Die erlaubten Operationen sind folgende (2, ab Seite 46):

- *Iteration* erlaubt, dass eine Komponente mehr als einmal verwendet wird, wobei es notwendig ist, dass auf jeden Operation andere Operatoren ausgeführt werden – es ist nicht erlaubt, dieselbe Komponente in der selben Belegung öfters einzubinden.

- *Zuweisung* erlaubt die Spezifikation von Parametern.

- *Auswahl* erlaubt die Spezifikation eines oder mehrerer Elemente aus einer Liste

- *Verfeinerung* erlaubt das Hinzufügen von Details.

Iteration und Verfeinerung sind für alle Komponenten erlaubt, Zuweisung und Auswahl nur, wenn die Komponente dies ausdrücklich erlaubt.

4.4.1 Iteration

Eine Iteration kann für jede Komponente ausgeführt werden. Der Autor führt sie aus, indem er mehrere Anforderungen einbaut, welche auf der gleichen Komponente basieren. Jede Iteration einer Komponente sollte sich von ihren anderen Iterationen unterscheiden. Das wird erreicht, indem die Zuweisung, Auswahl oder Verfeinerung auf eine andere Art ausgeführt wird.

Verschiedene Iterationen müssen eindeutig gekennzeichnet werden, damit klare Begründungen und Verfolgungen zu und von diesen Anforderungen möglich sind.

4.4.2 Zuweisung

Eine Zuweisung tritt auf, wenn eine Komponente Parameter enthält, welche vom Autor gesetzt werden können. Die Parameter können eine uneingeschränkte Variable sein, oder eine Regel, welche die Variable auf eine Menge von Werten einschränkt.

Für Sicherheitsvorgaben müssen Zuweisungen stets ausgefüllt werden. Bei Profilen ist es zulässig, eine Zuweisung auch auslassen, oder ihren Bereich einzuschränken (z. B. indem man eine Auswahl vordefinierter Werte vorgibt) – wobei sowohl eine Menge von Werten wie auch eine textuelle Beschreibung möglicher Werte erlaubt sind. Der Datentyp ist stets zu beachten.

4.4.3 Auswahl

Eine Auswahl tritt auf, wenn eine Komponente ein Element enthält, für das der Autor eine Auswahl treffen muss. Enthält ein Element eines Schutzprofils eine Auswahl, dann hat der Autor folgende Möglichkeiten: Für Sicherheitsvorgaben ist die Auswahl stets durch einen oder mehrere Werte zu vervollständigen. Bei Schutzprofilen kann die Auswahl unvollständig gelassen oder weiter eingeschränkt werden, wobei dabei Werte verwendet werden sollen, welche für die Auswahl zur Verfügung gestellt werden.

4.4.4 Verfeinerung

Die Verfeinerung kann für jede Anforderung ausgeführt werden. Der Autor führt die Verfeinerung durch, indem er die Anforderungen strikter formuliert – die Anforderung darf also nicht umformuliert, nur präzisiert werden. Verstößt eine Verfeinerung gegen diese Regeln, dann wird die Anforderung als erweiterte Anforderung angesehen und sollte auch entsprechend behandelt werden.

Eine Ausnahme für diese Regel ist, dass ein Autor eine funktionale Sicherheitsanforderung verfeinern kann, um sie nur auf einen Teil aller Subjekte, Objekte, Operationen und Sicherheitsattribute oder externen Entitäten anzuwenden. Diese Ausnahme gilt aber nicht für die Verfeinerung von funktionalen Sicherheitsanforderungen aus Schutzprofilen, zu denen man konform ist.

Eine Verfeinerung muss mit der ursprünglichen Komponente verwandt sein muss. Zum Beispiel darf eine Audit Komponente nicht mit einem extra Element zur Vermeidung elektromagnetischer Strahlung erweitert werden.

Ein Sonderfall einer Verfeinerung ist eine redaktionelle Verfeinerung, bei der eine Kleinigkeit in einer Anforderung geändert wird, z. B. wenn ein Satz neu formuliert wird, um der deutschen Grammatik zu entsprechen, oder wenn er einfach dem Leser verständlicher werden soll. Diese Änderung darf die Bedeutung der Anforderung auf keine Weise ändern.

4.4.5 Erweiterte Komponenten

Die CC verlangt, dass Anforderungen auf Komponenten aus CC Teil 2 oder CC Teil 3 basieren. Sicherheitsziele sind davon ausgenommen, wenn es keine entsprechenden Komponenten gibt, oder sie nur schwer auf existierende Komponenten übersetzt werden können.

In beiden Fällen muss der Autor eine eigene erweiterte Komponente formulieren. Eine genau definierte erweiterte Komponente muss zeigen, in welcher Beziehung sie zu den erweiterten funktionalen Sicherheitsanforderungen und Vertrauenswürdigkeitsanforderungen steht, welche auf dieser Komponente basieren.

Wurde die erweiterte Komponenten korrekt definiert, dann kann der Autor Anforderungen auf diese neuen Komponente aufbauen lassen und sie anschließend auf die gleiche Art verwenden, wie er andere Anforderungen. Ab diesem Zeitpunkt gibt es keine weitere Unterscheidung zwischen vordefinierten Anforderungen aus den CC-Katalogen und erweiterten Anforderungen.

Die Definition einer erweiterten Komponente erfolgt auf die gleiche Art, wie auch die CC-Komponenten definiert worden sind: klar, unmissverständlich und evaluierbar (es soll möglich sein, systematisch zu demonstrieren, dass eine Anforderung, welche auf dieser Komponente basiert, für den EVG erfüllt ist). Erweiterte Komponenten müssen das gleiche Namensschema, die gleiche Ausdrucksweise und denselben Detailgrad wie existierende CC Komponenten verwenden.

Außerdem hat der Autor dafür zu sorgen, dass die Definition der erweiterten Komponente alle Abhängigkeiten der Komponente erwähnt.

Der Autor einer erweiterten Funktionskomponente muss in der Komponentendefinition auch alle notwendigen Evaluationsoperationen und damit verbundene Operationen angeben, ähnlich zu bestehenden CC Teil 2 Komponenten. Wird eine erweiterte Vertrauenskomponente verfasst, dann muss der Autor die passende Methodik bereit stellen, ähnlich wie die Methodik, welche von den CEM bereit gestellt wird.

Erweiterte Komponenten können in existierende Familien platziert werden, wobei der Autor verdeutlichen muss, wie sich diese Familien dadurch ändern. Wenn die Komponenten nicht in bestehende Familien passen, dann können neue Familien erstellt werden. Neue Familien müssen entsprechend der Vorgaben der CC definiert werden.

Neue Familien müssen in existierende Klassen platziert werden, wobei der Autor zeigen muss, wie sich diese Klassen dadurch ändern. Passen sie nicht in existierende Klassen, dann können sie in neue Klasse platziert werden, wobei diese Klassen entsprechend der Vorgaben der CC definiert werden müssen.

4.5 Schutzprofil-Konformität

Ein Schutzprofil soll als eine Vorlage für Sicherheitsvorgaben verwendet werden. Das bedeutet: Ein Schutzprofil beschreib eine Menge von Benutzerbedürfnissen und eine zum Schutzprofil konforme Sicherheitsvorgabe beschreibt einen EVG, welcher diese Bedürfnisse erfüllt.

Ein Schutzprofil kann als Vorlage für ein anderes Schutzprofil verwendet werden, wobei das auf die genau gleiche Art passiert, wie bei der Verwendung eines Schutzprofils als Vorlage für eine Sicherheitsvorgabe – beschrieben wird hier aber nur der zweite Fall.

Es gibt zwei Typen von Konformität (2, Seite 92):

- Strikte Konformität: Bei dieser Beziehung muss eine Sicherheitsvorgabe alle Aussagen des Schutzprofils enthalten, kann aber Aussagen hinzufügen. Strikte

Konformität soll für strenge Anforderungen verwendet werden, welche auf eine bestimmte Art befolgt werden sollen.

- Beweisbare Konformität: Das Schutzprofil und die Sicherheitsvorgabe stehen in keiner Untermenge/Obermenge-Beziehung zueinander. Das Schutzprofil und die Sicherheitsvorgabe können völlig verschiedene Aussagen enthalten, welche verschiedene Entitäten und Konzepte besprechen. Jedoch sollte die Sicherheitsvorgabe eine Begründung enthalten, wieso sie als „gleichwertig oder restriktiver“ als das Schutzprofil gesehen wird. Beweisbare Konformität erlaubt dem Autor des Schutzprofils ein übliches Sicherheitsproblem zu beschreiben, mit passenden allgemeinen Richtlinien, welche zur Lösung des Problems befolgt werden müssen, wobei berücksichtigt wird, dass es wahrscheinlich mehr als nur einen Weg gibt, um das Problem zu lösen. Beweisbare Konformität eignet sich auch für einen EVG-Typ bei dem bereits mehrere ähnliche Schutzprofile existieren (oder wahrscheinlich existieren werden), was dem Autor der Sicherheitsvorgabe erlaubt, Konformität zu allen diesen Schutzprofilen gleichzeitig zu beanspruchen, und somit Arbeit spart.

Der erlaubte Typ von Konformität wird vom Schutzprofil bestimmt. Das Schutzprofil sagt dazu in der Schutzprofil-Konformitätsaussage, welche Typen von Konformität für die Sicherheitsvorgaben erlaubt sind. Strikte Konformität ist immer einzuhalten, bei geforderter beweisbarer Konformität kann man aber auch die strikte wählen. Anders gesagt darf eine Sicherheitsvorgabe einem Schutzprofil nur auf eine beweisbare Art entsprechen, wenn das Schutzprofil dies explizit erlaubt.

Hat eine Sicherheitsvorgabe einen Konformitätsanspruch zu mehreren Schutzprofilen, dann muss es zu dem Schutzprofil konform sein, wie das Schutzprofil es jeweils verlangt, das heißt, dass eine Sicherheitsvorgabe zu verschiedenen Profilen verschiedene Konformität haben kann.

Es ist zu berücksichtigen, dass eine Sicherheitsvorgabe zu einem Schutzprofil nur vollständig konform sein kann, es gibt keine teilweise Konformität. Es ist daher die Aufgabe des Schutzprofil-Autors sicher zu stellen, dass das Schutzprofil nicht zu komplex ist und so anderen Autoren unmöglich macht zu dem Schutzprofil konform zu sein.

4.5.1 Strikte Konformität

Strikte Konformität orientiert sich an Schutzprofil-Autoren, welche einen Beweis brauchen, dass die Anforderungen aus dem Schutzprofil erfüllt werden, und dass die Sicherheitsvorgabe eine Instanz des Schutzprofiles ist, auch wenn die Sicherheitsvorgabe umfassender als das Schutzprofil sein kann. Prinzipiell beschreibt die Sicherheitsvorgabe, dass der EVG mindestens macht, was im Schutzprofil beschrieben wird, und die Einsatzumgebung höchstens alles macht, was im Schutzprofil beschrieben wird. Genauer gesagt:

- Sicherheitsproblemdefinition: Die Sicherheitsvorgabe übernimmt die Definition des Sicherheitsproblems vom Schutzprofil, kann aber noch zusätzliche Bedrohungen, organisatorische Sicherheitspolitik und Annahmen ergänzen.

- Sicherheitsziele. Die Sicherheitsvorgabe:

    - Soll alle Sicherheitsziele für den EVG entsprechend dem Schutzprofil enthalten, kann aber auch weitere Sicherheitsziele für den EVG definieren.

    - Soll alle Sicherheitsziele für die Einsatzumgebung enthalten, darf aber keine neuen spezifizieren.

    - Kann spezifizieren, dass bestimmte Ziele für die Einsatzumgebung im Schutzprofil Sicherheitsziele für den EVG in der Sicherheitsvorgabe sind. Dies wird als Neuzuweisung eines Sicherheitsziels bezeichnet.

- Sicherheitsanforderungen: Die Sicherheitsvorgabe muss alle funktionalen Sicherheitsanforderungen und Vertrauenswürdigkeitsanforderungen des Schutzprofils enthalten, kann aber zusätzliche oder stärkere funktionale Sicherheitsanforderungen oder Vertrauenswürdigkeitsanforderungen. Die Vervollständigung von Operationen in der Sicherheitsvorgabe muss konsistent mit der Vorgabe aus dem Schutzprofil sein; entweder wird die gleiche Vervollständigung verwendet, oder eine durch Verfeinerung restriktivere.

In manchen Fällen kann der Autor eines Schutzprofils wünschen, dass Sicherheitsziele für die Einsatzumgebung nicht neu zugewiesen werden sollen. In diesem Fall sollte das Schutzprofil einen entsprechenden Hinweis enthalten. Es ist auch erlaubt Bedrohungen, die organisatorische Sicherheitspolitik, Annahmen und Sicherheitsziele umzuformulieren, wenn die neue Terminologie eher jener der Konsumenten der neuen Sicherheitsvorgabe entspricht.

4.5.2 Beweisbare Konformität

Beweisbare Konformität richtet sich an Schutzprofil-Autoren, welche einen Beweis brauchen, dass eine Sicherheitsvorgabe eine passende Lösung des allgemeinen Sicherheitsproblems ist, welches im Schutzprofil beschrieben wird. Bei einer beweisbaren Konformität ist die Beziehung zwischen dem Schutzprofil und der Sicherheitsvorgabe keine klare Untermengen/Obermengen-Beziehung. Allgemein kann gesagt werden, dass die Sicherheitsvorgabe gleichwertig oder restriktiver als das Schutzprofil sein muss. Eine Sicherheitsvorgabe ist gleichwertig oder restriktiver als ein Schutzprofil, wenn:

- Alle EVGs, welche das Schutzprofil erfüllen, auch die Sicherheitsvorgabe erfüllen.

- Alle Einsatzumgebungen die Sicherheitsvorgabe erfüllen auch das Schutzprofil erfüllen. Informell ausgedrückt, soll die Sicherheitsvorgabe dem EVG die gleichen oder mehr Einschränkungen auferlegen und der Einsatzumgebung gleich viel oder weniger Einschränkungen.

Diese allgemeine Aussage kann für verschiedene Abschnitte der Sicherheitsvorgabe spezifiziert werden:

- Sicherheitsproblemdefinition: Die Konformitätsbegründung in einer Sicherheitsvorgabe soll beweisen, dass die Sicherheitsproblemdefinition in der Sicherheitsvorgabe gleichwertig oder restriktiver ist als jene des Schutzprofils. Das bedeutet, dass

    - Alle EVGs, welche der Sicherheitsproblemdefinition der Sicherheitsvorgabe entsprechen, auch jener des Schutzprofils entsprechen.

- Alle Einsatzumgebungen, welche der Sicherheitsproblemdefinition des Schutzprofils entsprechen auch jener der Sicherheitsvorgabe entsprechen.

- Sicherheitsziele: Die Konformitätsbegründung in der Sicherheitsvorgabe soll beweisen, dass die Sicherheitsziele in der Sicherheitsvorgabe gleichwertig oder restriktiver als die Sicherheitsziele im Schutzprofil sind. Das bedeutet, dass

  - Alle EVGs, welche den Sicherheitszielen für das EVG in der Sicherheitsvorgabe erfüllen, auch jene des Schutzprofils erfüllen würden.

  - Alle Einsatzumgebungen, welche den Sicherheitszielen für die Einsatzumgebung im Schutzprofil entsprechen, würden diese auch für die Sicherheitsvorgabe erfüllen.

- Funktionale Sicherheitsanforderungen: Die Konformitätsbegründung der Sicherheitsvorgabe sollte beweisen, dass die funktionalen Sicherheitsanforderungen der Sicherheitsvorgabe gleichwertig oder restriktiver sind als die funktionalen Sicherheitsanforderungen des Schutzprofils. Das bedeutet, dass alle EVGs, welche die funktionalen Sicherheitsanforderungen der Sicherheitsvorgabe erfüllen, dass alle funktionalen Sicherheitsanforderungen, welche der Sicherheitsvorgabe entsprechen, auch jenen im Schutzprofil entsprechen würden.

- Vertrauenswürdigkeitsanforderungen: Die Sicherheitsvorgabe sollte alle Vertrauenswürdigkeitsanforderungen aus dem Schutzprofil enthalten, kann aber noch zusätzliche oder übergeordnete (und daher stärkere) Vertrauenswürdigkeitsanforderungen einschließen. Die Ausführung der Operationen in der Sicherheitsvorgabe muss jener des Schutzprofils entsprechen; entweder muss die Ausführung gleich oder restriktiver sein als jene, die im Schutzprofil definiert ist (Verfeinerung wird wirksam)

5 Die Kataloge der CC

5.1 Einleitung

Gängige Anforderungen an die Sicherheitsfunktionalität und Vertrauenswürdigkeit wurden – wie schon seit früheren Standards üblich - mit der CC in einer standardisierten Form ausgedrückt und in themenverwandten Gruppen in Katalogen zusammengefasst ((3) und (4) enthalten diese Kataloge).

Diese Kataloge bilden das Vokabular, mit dem Anforderungen für eine breite Palette von Produkten formuliert werden können. Finden sich spezielle Anforderungen nicht in den Katalogen, dann kann ein Anwender eigene Anforderungen über sogenannte „Erweiterungen“ definieren.

5.2 Funktionskomponenten

5.2.1 Umsetzung von Anforderungen in Funktionen

Sicherheitsanforderungen von Schutzprofilen und Sicherheitsvorgaben werden über Funktionskomponenten ausgedrückt. Sie beschreiben das erwartete Sicherheitsverhalten des EVG und sollen dabei die vorgegebenen Sicherheitsziele erfüllen, wobei es dem Anwender möglich sein soll, diese Ziele durch eine direkte Interaktion über die Ein- und Ausgaben des EVG zu überprüfen.

Eine Sicherheitsanforderung definiert die Regeln, mit denen ein EVG den Zugriff und die Verwendung seiner Ressourcen steuert, und somit auch die Informationen und Dienste, die vom EVG gesteuert werden. Die Regeln werden in Form einer funktionalen Sicherheitspolitik ausgedrückt, welche ihren Einflussbereich anhand der involvierten Subjekte, Objekte, Ressourcen, Informationen und Operationen definiert.

Erfolgreich umgesetzte funktionale Sicherheitspolitik wird als EVG-Sicherheitsfunktion bezeichnet. Die Sicherheitsfunktion besteht aus sämtlicher Hard-, Soft- oder Firmware, auf die sich ein EVG verlässt, um Sicherheit zu gewährleisten.

Das bedeutet: Jede Sicherheitsanforderung wird mit Hilfe der funktionalen Sicherheitspolitik in eine EVG-Sicherheitsfunktion übersetzt.

5.2.2 Kommunikation, Interaktion und Ressourcen

Interne und externe Kommunikation

Ein EVG kann verteilt sein und aus mehreren Teilen bestehen. Ist das der Fall, dann kann auch eine Sicherheitsfunktion für jeden Teil des EVG andere Maßnahmen definieren.

Die Kommunikation zwischen den Teilen des EVG oder zu einem anderen vertrauenswürdigen EVG wird als interner EVG-Transfer bezeichnet. Kommuniziert der EVG mit einem nicht vertrauenswürdigen EVG, dann wird von externer Kommunikation gesprochen.

Die Menge von Schnittstellen, über welche auf von der EVG-Sicherheitsfunktion verwaltete Ressourcen zugegriffen wird, wird als EVG-Sicherheitsfunktionsschnittstelle bezeichnet. Sie definiert die Grenzen des EVG -Funktionalität, innerhalb welcher die funktionalen Sicherheitsanforderungen umgesetzt werden.

Interaktion mit dem EVG über Sitzungen

Benutzer befinden sich außerhalb des EVG und interagieren mit ihm über die EVG-Sicherheitsfunktionsschnittstelle. Benutzer können einerseits als menschliche Benutzer auftreten, die direkt (lokal) oder indirekt (über eine Remote-Verbindung) mit dem EVG-Kommunizieren, oder andererseits als externe IT-Entitäten, also fremde Hard-, Soft- oder Firmware.

Die Interaktion zwischen Anwendung und Sicherheitsfunktion wird als Sitzung bezeichnet. Die Sitzung kann über eine Reihe von Kriterien gesteuert werden, dazu gehören die Authentifizierung des Benutzers, der Zeitpunkt der Verbindung, die Art, wie auf den EVG zugegriffen wird, und die Anzahl der gleichzeitig erlaubten Sitzungen (je Benutzer oder insgesamt).

Benutzer, welche das Recht dazu haben bestimmte Operationen auf dem EVG auszuführen bezeichnet die CC als autorisierte Benutzer.

Ressourcen

Das vorrangige Ziel der EVG-Sicherheitsfunktion ist die vollständige und korrekte Umsetzung der funktionalen Sicherheitsanforderungen auf die Ressourcen und Informationen, welche der EVG zum Verarbeiten und Speichern von Informationen verwendet. Ressourcen werden an der Art von Entität unterschieden, welche sie erzeugt:

- Aktive Entitäten (auch Subjekte genannt) entstehen aus Aktionen innerhalb des EVG und lösen Operationen aus, welche auf Informationen ausgeführt werden. Subjekte arbeiten entweder im Auftrag eines oder mehreren Benutzer (als Prozess oder Dienst) oder im Auftrag des EVG selbst.

- Passive Entitäten (auch Objekte genannt) sind Container, die Informationen speichern, die mit Operationen verarbeitet werden kann. In Sonderfällen können auch Subjekte als Objekte behandelt werden (z. B. bei der Interprozesskommunikation).

Attribute von Benutzern, Sitzungen und Ressourcen

Benutzer, Subjekte, Informationen, Objekte, Sitzungen und Ressourcen, die von Regeln aus den funktionalen Sicherheitsanforderungen gesteuert werden, können Attribute enthalten. Der EVG benötigt die EVG, um sie korrekt verwenden zu können.

Manche Attribute, wie Dateinamen, dienen zur Unterscheidung von Ressourcen, andere Attribute, wie Informationen über Zugriffrechte, können direkt funktionale Sicherheitsanforderungen umsetzen. Dieser zweite Typ von Attribut wird oft als „Sicherheitsattribut“ bezeichnet.

Daten

Bei den Daten eines EVG unterscheidet man Benutzerdaten und EVG-Sicherheitsfunktionsdaten.

Die Benutzerdaten werden innerhalb des EVG gespeichert und können von Benutzer entsprechend den funktionalen Sicherheitsanforderungen verändert werden, die EVG-Sicherheitsfunktion gibt ihnen jedoch keine besondere Bedeutung – ein Beispiel dafür ist der Inhalt der Mail eines Benutzers.

Die EVG-Sicherheitsfunktionsdaten hingegen werden von der EVG-Sicherheitsfunktion benötigt, um selbst Entscheidungen zu treffen, die den funktionalen Sicherheitsanforderungen entsprechen. EVG-Sicherheitsfunktionsdaten können vom Benutzer verändert werden, sofern die funktionalen Sicherheitsvorgaben das erlauben. Beispiele für EVG-Sicherheitsfunktionsdaten sind Zugangsdaten und Einträge zu Zugriffsrechten der Benutzer.

Es gibt funktionale Sicherheitspolitik, welche für Datenschutz sorgt, dazu gehört funktionale Sicherheitspolitik für die Zugriffskontrolle und funktionale Sicherheitspolitik für den Informationsfluss. Mechanismen, welche diese funktionale Sicherheitspolitik implementieren, bewilligen oder blockieren den Zugriff oder Informationsfluss anhand der Eigenschaften des Benutzers, den verfügbaren Ressourcen, Subjekten, Objekten und Sitzungsdaten, dem Zustandsdaten der EVG-Sicherheitsfunktion und den verfügbaren Operationen.

Zwei Typen von EVG-Sicherheitsfunktionsdaten, können sich oft auf dieselben Daten beziehen: Authentifizierungsdaten und Geheimnisse.

Authentifizierungsdaten werden verwendet, um die Identität eines Benutzers zu bestätigen, der Dienste des EVG in Anspruch nehmen möchte. Die üblichste Form davon ist das Passwort, welches geheim gehalten werden muss, um effektiv zu sein. Es gibt aber auch andere Typen von Authentifizierungsdaten, welche nicht geheim gehalten werden müssen: Die biometrische Authentifizierung (über Fingerabdrücke oder die Netzhaut) verlässt sich nicht darauf, dass die Daten geheim gehalten werden, sondern nur ein Benutzer sie besitzen kann (3 S. 21).

Die CC Teil 2 verwendet den Begriff „Geheimnis“ nicht nur für Authentifizierungsdaten, sondern auch für andere Daten, welche geheim gehalten werden müssen, um die EVG-Sicherheitsfunktion umzusetzen. Ein Beispiel dafür ist die Kommunikation innerhalb eines EVG, die über einen verschlüsselten Kanal erfolgt: Der Kanal ist nur so sicher wie die Methode, mit der die verwendeten Schlüssel geschützt werden.

5.2.3 Strukturierung von Sicherheitsfunktionen

Klassen, Familien und Komponenten

Der Grundbaustein der Sicherheitsfunktionen ist die Sicherheitskomponente. Komponenten werden thematisch zusammengehörig zuerst in Familien gruppiert, um auf der obersten Ebene in Klassen zusammen gefasst zu werden. Komponenten, Familien und Klassen können untereinander abhängig sein, das heißt sich einander bedingen, um ihre Sicherheitsfunktion umsetzen zu können.

Funktionsklassen

Jede Funktionsklasse besteht aus einem Namen, einer Einleitung und einer oder mehreren Funktionsfamilien.

Der *Klassenname* identifiziert eine Funktionsklasse, wobei jede Klasse einen eindeutigen Namen hat. Die Kategorie der Klasse wird über einen kurzen Namen aus drei Zeichen bestimmt, wobei er bei der Definition der Familien dieser Klasse verwendet wird.

Die *Klasseneinleitung* beschreibt die Absicht oder den Ansatz der Familien der Klasse, um die Sicherheitsziele zu erfüllen. Sie enthält eine Abbildung, in der die Familien der Klasse und ihre Komponenten in einer Hierarchie dargestellt werden.

Funktionsfamilien

Der *Familienname* beschreibt die Familie und gibt an, welcher Kategorie sie zuzuordnen ist. Jede Funktionsfamilie hat einen eindeutigen Namen. Der Familienname kombiniert das

Kürzel des Klassennamens mit einem Kürzel für den Familiennamen. Diese Kurzform wird als Referenzname der Familie innerhalb der Komponenten verwendet.

Das *Familienverhalten* schildert, wie von der Familie beschriebene Sicherheitsziele erreicht werden können, wenn diese Familie in einem EVG verwendet wird. Außerdem beschreibt das Familienverhalten die funktionalen Anforderungen, welche alle Anforderungen der Komponenten zusammenfassen; diese Beschreibung soll den Verfassern von Schutzprofilen und Sicherheitsvorgaben helfen zu bestimmen, ob die Familie für ihre Anforderungen relevant ist.

Funktionsfamilien enthalten eine oder mehrere Komponenten, von denen jede beliebige in Schutzprofile, Sicherheitsvorgaben und Funktionspakete eingebunden werden kann. Sobald der Benutzer festgestellt hat, dass die Familie für ihn nützlich ist, soll ihm der Abschnitt *Angleichung der Komponenten* bei der Auswahl der notwendigen Komponenten helfen, indem er ihren Zweck beschreibt; Details sind in den Beschreibungen der einzelnen Komponenten zu finden.

Die Beziehung zwischen Komponenten innerhalb einer Funktionsfamilie kann hierarchisch sein. Eine Komponente ist einer anderen übergeordnet, wenn sie mehr Sicherheit bietet. Die Beschreibung der Familie soll eine Übersicht enthalten, in der diese *Komponentenhierarchie* grafisch dargestellt wird.

Der Abschnitt *Verwaltung* beschreibt die nötigen Verwaltungsmaßnahmen für eine bestimmte Komponente anhand der Komponenten der Verwaltungsklasse FMT und bietet Richtlinien für die möglichen Verwaltungsmaßnahmen, die man mit Operationen auf die Komponenten anwenden kann. Ein Autor kann die angegebenen Verwaltungskomponenten inkludieren oder andere Verwaltungsanforderungen einbinden, um die Verwaltungsmaßnahmen zu verfeinern.

Der Abschnitt *Audit* enthält prüffähige Ereignisse für den Autor, welche in Form von Komponenten der Klasse Security Audit FAU definiert werden (die Klasse selbst enthält eine detaillierte Erklärung des Security Audit). Eine Prüfanmerkung kann z. B. folgende hierarchischen Aktionen enthalten, welche über eine Zuweisungsoperation in ein Schutzprofil oder eine Sicherheitsvorgabe eingebunden werden können:

- „Minimal: Erfolgreiche Anwendung der Sicherheitsmechanismen.“

- „Grundlegend: Jede Anwendung der Sicherheitsmechanismen sowie der relevanten Informationen, die sich auf die verwendeten Sicherheitsattribute beziehen.“

- „Detailliert: Alle Konfigurationsänderungen am Mechanismus, einschließlich der Konfigurationswerte vor und nach der Änderung.“

Funktionskomponenten

Abbildung 7 illustriert die Struktur einer Funktionskomponente.

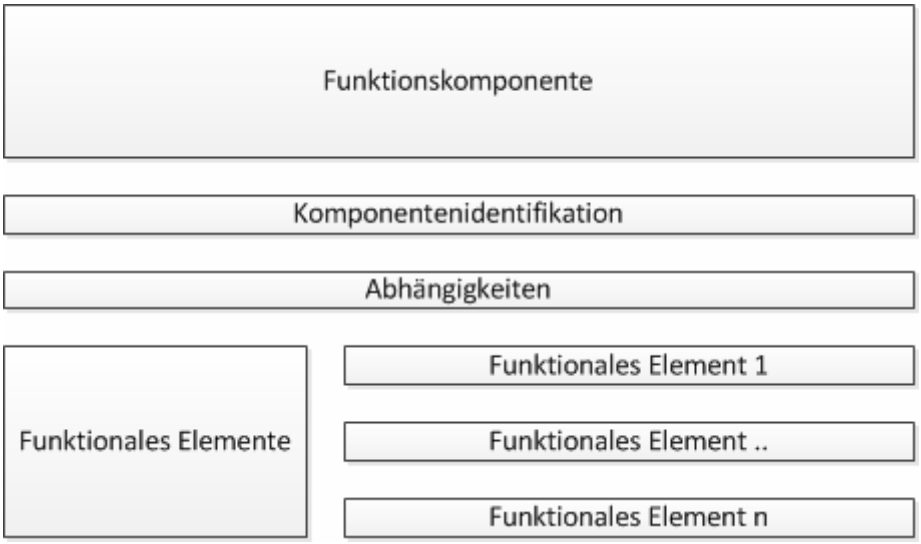


Abbildung 7: Aufbau einer Funktionskomponente

Eine Sicherheitskomponente ist die kleinste Einheit, die von einem Autor in ein Schutzprofil, eine Sicherheitsvorgabe oder in ein Paket aufgenommen werden darf.

Die *Komponentenidentifikation* enthält die Beschreibung der Komponente, die aus folgenden Teilen besteht:

- Der eindeutige Komponentenname beschreibt den Zweck der Komponente.

- Die Kurzbezeichnung dient als Referenzname und wird überall zur Identifikation der Komponente verwendet. Sie enthält die Nummer der Komponente innerhalb der Familie.

- Eine Liste untergeordneter Komponenten, statt denen die Komponente verwendet werden kann, um Abhängigkeiten der untergeordneten Komponenten zu erfüllen.

Für jede Komponente ist eine *Menge von funktionellen Elementen* gegeben. Jedes Element ist eine einzeln definierte und atomare funktionale Sicherheitsanforderung, welche nicht mehr in weitere sinnvolle Sicherheitsanforderungen zerlegt werden kann. Sie ist die kleinste funktionale Sicherheitsanforderung, welche in der CC verwendet und anerkannt wird.

Abhängigkeiten zwischen Funktionskomponenten entstehen, wenn eine Komponente für ihre korrekte Funktion die Interaktion mit oder Funktion einer anderen Komponente benötigt. Jede Funktionskomponente enthält eine vollständige Liste der Abhängigkeit von anderen Funktions- und Vertrauenswürdigkeitskomponenten. Dabei können auch den Komponenten übergeordnete Komponenten verwenden werden, um die Abhängigkeit zu erfüllen. In manchen Fällen ist es möglich, dass zur Erfüllung einer funktionellen Anforderung nur eine Abhängigkeit von mehreren angegebenen erfüllen muss. Falls es keine Abhängigkeiten gibt, wird das ebenfalls angeführt.

In bestimmten Situationen kann es vorkommen, dass die verlangten Abhängigkeiten nicht anwendbar sind. Der Autor des Schutzprofiles oder der Sicherheitsvorgabe, muss dies begründen und kann dann aber die Abhängigkeit zur Komponente aus dem Paket, dem Schutzprofil oder der Sicherheitsvorgabe entfernen.

5.2.4 Funktionsklassen des Komponentenkatalogs

CC Teil 2 enthält einen umfangreichen Katalog von Sicherheitsanforderungen, der typische Sicherheitsanforderungen abdeckt. Die Klassen sind alphabetisch sortiert, die Zuordnung einzelner Familien und Komponenten zu einer Klasse erfolgt nach keiner formellen Systematik.

Klasse FAU: Sicherheitsaudit (3, Seite 29)

Sicherheitsaudit umfasst die Erkennung, Aufnahme, Speicherung und Analyse von Information über Sicherheitsaktivitäten, z. B. Aktivitäten, welche von EVG-Sicherheitsfunktionen kontrolliert werden. Die dabei entstehenden Aufzeichnungen können überprüft werden, um zu zeigen, welche sicherheitsrelevanten Aktivitäten wann von welchem Benutzer ausgeführt worden sind.

Klasse FCO: Kommunikation (3, Seite 43)

Diese Klasse enthält zwei Familien, welche beim Datenaustausch die Echtheit der beteiligten Parteien garantiert; durch sie wird der Ursprung und Empfang einer Nachricht nachweisbar. Die Familien stellen sicher, dass die Absender und Empfänger eine Nachricht nicht abstreiten können, die Nachricht gesendet oder empfangen zu haben.

Klasse FCS: Kryptografische Unterstützung (3, Seite 48)

Bei der Umsetzung von Sicherheitsvorgaben kann Kryptografie eingesetzt werden. Diese Klasse wird verwendet, wenn der EVG kryptografische Funktionen implementiert. Die Klasse FCS besteht aus zwei Familien: Kryptografische Schlüsselverwaltung (cryptographic key management, FCS_CKM) und kryptografische Operation (cryptographic operation, FCS_COP). Die erste Familie beschäftigt sich mit der Verwaltung kryptografischer Schlüssel, die zweite Familie mit deren Anwendung.

Klasse FDP: Schutz der Benutzerdaten (3, Seite 54)

Diese Klasse enthält Familien, welche die Anforderungen für den Schutz von Benutzerdaten formulieren. Die Klasse ist auf vier Gruppen von Familien unterteilt, welche Benutzerdaten innerhalb eines EVG, während des Imports, Exports und der Speicherung verwalten, zusammen mit den damit verbundenen Sicherheitseigenschaften. Jede Familie wird zusätzlich in folgende vier Gruppen unterteilt:

- Sicherheitsfunktionspolitik zum Schutz der Benutzerdaten.

- Formen des Schutzes von Benutzerdaten.
- Offline -Speicherung, Import und Export.
- EVG-interne Kommunikation

Klasse FIA: Identifikation und Authentifizierung (3, Seite 87)

Diese Klasse definiert die Anforderungen für Funktionen zur Sicherstellung und Überprüfung der Identität eines Benutzers.

Identifikation und Authentifizierung werden benötigt um sicherzustellen, dass Benutzer mit den korrekten Sicherheitsattributen assoziiert werden, dazu gehören die Identität, Gruppen, Rollen, Sicherheits- und Integritätsstufen.

Die unmissverständliche Identifikation autorisierter Benutzer und die Korrekte Assoziation der Sicherheitsattribute mit Benutzern und Subjekten ist essentiell für die Umsetzung der beabsichtigten Sicherheitspolitik. Die Familien dieser Klasse beschäftigen sich mit Feststellung und Überprüfung der Identität eines Benutzers, überprüfen dabei deren Befugnisse zur Kontrolle des EVG, und bestimmten die korrekte Assoziation von Sicherheitsattributen für jeden autorisierten Benutzer. Andere Klassen von Anforderungen (Schutz von Benutzerdaten, Sicherheitsaudit) hängen von einer korrekten Identifikation und Authentifizierung von Benutzern ab, um korrekt und effektiv arbeiten zu können.

Klasse FMT: Sicherheitsmanagement (3, Seite 103)

Diese Klasse beschäftigt sich mit der Verwaltung verschiedener Aspekte von EVG-Sicherheitsfunktionen: Sicherheitsattribute, Daten und Funktionen der EVG-Sicherheitsfunktion. Sie erlaubt die Spezifikation verschiedener Rollen und ihrer Interaktionen. Diese Klasse hat mehrere Ziele:

- Verwaltung von EVG-Sicherheitsfunktions-Daten, z. B. Banner
- Verwaltung von Sicherheitsattributen, z. B. Zugriffskontrolllisten, Befugnis-Listen

- Verwaltung von Funktionen der EVG-Sicherheitsfunktion, z. B. Auswahl von Funktionen, Regeln und Bedingungen zur Steuerung des Verhaltens der EVG-Sicherheitsfunktion

- Definition von Sicherheitsrollen

Klasse FPR: Privatsphäre (3, Seite 118)

Diese Klasse enthält Anforderungen an die Privatsphäre; sie bieten dem Benutzer Schutz gegen die Aufdeckung und Missbrauch seiner Identität durch andere Benutzer.

Klasse FPT: Schutz der EVG-Sicherheitsfunktion (3, Seite 126)

Diese Klasse definiert Maßnahmen zur Wahrung der Integrität und Verwaltung der EVG-Sicherheitsfunktion und ihrer Daten. Obwohl diese Klasse ähnlich zur Klasse FDP (Schutz von Benutzerdaten) ist, ist ihr wesentlicher Unterschied, dass die Klasse FDP sich mit dem Schutz von Benutzerdaten beschäftigt, die Klasse FPT hingegen mit dem Schutz von Daten der EVG-Sicherheitsfunktion. Komponenten der Klasse FPT sind notwendig, um Anforderungen zu definieren, welche es unmöglich machen, die Sicherheitsfunktionspolitik des EVG zu umgehen.

Aus Sicht dieser Klasse gibt es bezüglich der EVG-Sicherheitsfunktion drei wesentliche Elemente:

- Die Implementierung der EVG-Sicherheitsfunktion, welche die Mechanismen ausführt und umsetzt, welche von den Sicherheitsfunktionsvorgaben definiert werden.

- Die Daten der EVG-Sicherheitsfunktion, welche die administrative Datenbank bildet, welche die Umsetzung der Sicherheitsfunktionsvorgaben steuert.

- Externe Entitäten, mit denen die EVG-Sicherheitsfunktion interagieren muss, um die Sicherheitsfunktionsvorgaben umzusetzen.

Klasse FRU: Betriebsmittelnutzung (3, Seite 151)

Diese Klasse unterteilt sich auf drei Familien, welche die Verfügbarkeit benötigter Ressourcen unterstützten; dazu gehören sowohl Rechenleistung wie auch der verfügbare Speicher:

- Die Familie Fehlertoleranz (fault tolerance) bietet Schutz gegen Nichtverfügbarkeit von Fähigkeiten, die vom EVG verursacht wird.

- Die Familie Dienstpriorität (priority of service) stellt sicher, dass Ressourcen zuerst den wichtigeren und Zeit-kritischeren Aufgaben zur Verfügung gestellt werden und nicht von Aufgaben mit niedriger Priorität vereinnahmt werden können.

- Die Familie Ressourcenzuteilung (resource allocation) ermöglicht die Definition von Grenzen für die Verwendung von Ressourcen, und verhindert so, dass Benutzer Ressourcen vollständig in Anspruch nehmen.

Klasse FTA: EVG-Zugriff (3, Seite 158)

Diese Klasse definiert funktionale Anforderungen für die Kontrolle der Sitzung eines Benutzers.

Klasse FTP: Vertrauenswürdiger Pfad/Kanal (3, Seite 168)

Familien in dieser Klasse bieten die Anforderungen für einen vertrauenswürdigen Kommunikationspfad zwischen Benutzern und der EVG-Sicherheitsfunktion, sowie vertrauenswürdige Kommunikationskanäle zwischen der EVG-Sicherheitsfunktion und anderen vertrauenswürdigen IT-Produkten.

Ein vertrauenswürdiger Kanal ist ein Kommunikationskanal, der von beiden Seiten einer Kommunikation erstellt werden kann, und es beiden beteiligten Parteien unmöglich macht, die Teilnahme an der Kommunikation abzustreiten.

Ein vertrauenswürdiger Pfad kann einem Benutzer die Mittel bieten, um direkt mit der EVG-Sicherheitsfunktion zu interagieren. Ein vertrauenswürdiger Pfad ist wird normalerweise für Benutzeraktionen wie Identifizierung oder Authentifizierung verwendet, kann aber auch während einer Sitzung eines Benutzers zum Einsatz kommen. Die Verwendung eines vertrauenswürdigen Pfades kann von einem Benutzer ausgelöst werden; Antworten über diesen Kanal sind garantiert vor Modifikation oder Offenlegung durch bzw. an nicht vertrauenswürdige Applikationen geschützt.

Vertrauenswürdige Pfade und Kanäle haben folgende Charakteristika:

- Der Kommunikationspfad setzt sich aus internen und externen Kommunikationskanälen zusammen (entsprechend der Komponente), welche mit einer ausgewählten Menge von Kommandos auf einer Menge von Daten der EVG-Sicherheitsfunktion arbeiten.

- Die Verwendung von Kommunikationspfaden kann vom Benutzer oder der EVG-Sicherheitsfunktion veranlasst werden.

- Der Kommunikationspfad ist in der Lage zu versichern, dass der Benutzer mit der korrekten EVG-Sicherheitsfunktion kommuniziert, und dass die EVG-Sicherheitsfunktion mit dem korrekten Benutzer kommuniziert.

5.3 Vertrauenswürdigkeitskomponenten

5.3.1 Bedeutung von Vertrauenswürdigkeit

Eines der wichtigen Prinzipien der CC ist Verständlichkeit. Die Sicherheitspolitik, die sich aus den Bedrohungen und Gegenmaßnahmen ergibt, sollen klar und eindeutig beschrieben werden, damit auch überprüft und demonstriert werden kann, dass vorgeschlagene Sicherheitsmaßnahmen tatsächlich dem beabsichtigten Zweck dienen. Die Überprüfung dieser Sicherheit ist notwendig - die CC geht dabei aus, dass Bedrohungsverursacher laufend versuchen Sicherheitslücken ausnutzen. Fehlen ausreichend vertrauenswürdige Produkte, dann führt dies zu einem beträchtlichen Risiko im Einsatz des Produkts.

Dabei kann man einer Bedrohung auf verschiedene Arten begegnen: Lässt sich die Bedrohung nicht beseitigen, dann kann man sie immer noch abschwächen, indem man Schwachstellen weniger zugänglich macht, oder dafür sorgt, dass der verursachbare Schaden möglichst gering bleibt.

Ein Grundgedanke bei der Entwicklung der CC war, dass eine größere Anstrengung bei der Evaluierung zu größerem Vertrauen führt - und dieser Prozess trotzdem effizient sein kann. Die notwendige Genauigkeit einer Evaluierung ändert sich dabei mit dem Aufgabenbereich des EVGs, dem Detail, in dem es entworfen und implementiert wird, und der Strenge der Prüfverfahren.

Die CC stellt die Vertrauenswürdigkeit aktiv durch eine Untersuchung des EVG her - die Untersuchung wird als Evaluation bezeichnet. Dabei stehen unter anderem folgende Techniken zur Verfügung:

- Analyse und Überprüfung von Prozessen und Prozeduren
- Überprüfung, ob Prozesse angewandt werden
- Analyse, ob das EVG-Design den Anforderungen entspricht
- Analyse von Funktionstest und ihrer Resultate
- Unabhängige Überprüfung der Funktionen
- Schwachstellenanalyse
- Penetrationstest

Der CC Ansatz zur Vertrauenswürdigkeit ist, dass Bedrohungen der Sicherheit und organisatorischen Sicherheitsmaßnahmen klar artikuliert, ihre Wahrscheinlichkeit gemessen und sie abgewehrt werden müssen. Die Mittel zur Vermeidung dieser Schwachstellen sind:

- Elimination: Alle Schwachstellen werden identifiziert, entfernt oder neutralisiert.

- Verringerung: Die Auswirkung der Ausnutzung einer Schwachstelle wird verringert.

- Überwachung: Stellt sicher, dass jeder Versuch, eine Schwachstelle auszunutzen, bemerkt wird, um so den Schaden einzuschränken.

Dabei können Schwachstellen durch drei Fehler entstehen:

- Fehler in den Anforderungen, wenn die formulierten Anforderungen nicht alle Schwachstellen abdecken.

- Fehler in der Entwicklung, wenn durch schlechte Standards oder falsche Design-Entscheidungen Anforderungen nicht implementiert werden oder neue Schwachstellen entstehen.

- Fehler in der Ausführung, wenn unzureichende Kontrolle über die Ausführung des EVG besteht, auch wenn das IT Produkt korrekt spezifiziert und erstellt worden ist.

Die Anforderungen an die Vertrauenswürdigkeit folgen einem hierarchischen System, wie es schon für die Funktionskomponenten vorgestellt worden ist. Auch hier besteht diese Hierarchie aus Klassen, Familien und Komponenten, wobei Familien und Komponenten noch in Teilkomponenten aufgeteilt werden. Klassen sind also auch hier abstrakte Sammlungen von Vertrauenswürdigkeitsanforderungen, die mit jeder untergeordneten Ebene weiter konkretisiert werden.

5.3.2 Strukturierung von Vertrauenswürdigkeitsfunktionen

Vertrauenswürdigkeitsklassen

Bei der Beschreibung von Vertrauensfunktionalität ist die Klasse die allgemeinste Struktur, welche nach und nach auf mehreren Ebenen immer detaillierter erklärt wird.

Formal hat jede Klasse einen *eindeutigen Namen*, welcher ihren Aufgabenbereich beschreibt. Der Name wird abgekürzt durch ein „A“ gefolgt von zwei Buchstaben, die sich auf den Klassennamen beziehen.

Außerdem hat jede Klasse eine *Einleitung*, in welcher die Zusammensetzung und der Zweck der Klasse beschrieben werden.

Jede Klasse enthält mindestens eine Unterebene, die sogenannte Familie der Vertrauenswürdigkeit.

Vertrauenswürdigkeitsfamilien

Eine Familie wird in einer Klasse mit anderen Familien gruppiert, wobei alle Familien dem gleichen Zweck dienen sollen - jenem, der in der Klassenbeschreibung angegeben worden ist.

Auch eine Familie hat einen eindeutigen Namen, der ihre Aufgabe möglichst gut beschreibt. Die Kurzversion des Namens besteht aus dem Namen der Klasse gefolgt von einem Unterstrich und drei Buchstaben, die den Namen der Familie abkürzen.

In einer *allgemeinen Beschreibung der Ziele* wird der Zweck der Familie erläutert und welche Ziele der Vertrauenswürdigkeit erfüllt werden sollen.

Falls nötig wird in einem zusätzlichen Anwendungshinweis erklärt, ob die Familie gewissen Einschränkungen unterliegt oder bei ihrer Anwendung auf bestimmte Details geachtet werden soll.

Jede Familie enthält eine oder mehrere Komponenten der Vertrauenswürdigkeit.

Vertrauenswürdigkeitskomponenten

Jede Komponente ist innerhalb einer Familie der Vertrauenswürdigkeit platziert und teilt mit ihr die Sicherheitsziele; gibt es mehrere, dann unterteilt man die Komponenten auf mehreren Stufen nach ihrer Aufgabe und Strenge, in welcher sie diese ausführen. Dabei werden die Komponenten ab 1 aufsteigend nummeriert.

Die *Beschreibung einer Komponente* enthält - wie die Strukturen zuvor - eine eindeutige Bezeichnung. Der eindeutige Name setzt sich aus dem Namen der Familie zusammen, gefolgt von einem Beistrich und der Ziffer der Komponente. Manche Komponenten können eine Zielbeschreibung enthalten, sowie Hinweise über ihre Anwendung.

Um korrekt arbeiten zu können, kann eine Komponente von mehreren anderen Komponenten abhängig sein. Gibt es solche Abhängigkeiten, dann muss eine *Liste aller Abhängigkeiten* zu fremden Komponenten angeführt werden. In Sonderfällen können Abhängigkeiten nicht erfüllt werden; der Autor hat dann aber zu begründen, wieso dies nicht der Fall ist. Ist die Komponente unabhängig, dann ist das ebenfalls ausdrücklich festzuhalten.

Jede Komponente der Vertrauenswürdigkeit besteht aus mehreren Elementen der Vertrauenswürdigkeit. Das Element der Vertrauenswürdigkeit ist die kleinste Sicherheitsanforderung. Jedes Element stellt eine Anforderung dar, die erfüllt werden muss, daher ist auch jede einzelne Anforderung als ein Element umgesetzt. Jedes Element gehört zu einem von drei Typen - D, C oder E. Der jeweilige Buchstabe wird der Elementnummer angehängt. Die Typen unterscheiden sich wie folgt:

- Aktionen vom Typ D beschreiben Tätigkeiten, die von einem Entwickler erfüllt werden sollen.

- Aktionen vom Typ C beschreiben den Inhalt und Aufbau von Belegen.

- Aktionen vom Typ E sollen von einem Gutachter ausgeführt werden. Diese Elemente setzen voraus, dass Aktionen vom Typ C bereits ausgeführt worden sind.

5.3.3 Vertrauensstufen (EALs)

Aufbau

Eine Vertrauensstufe ist eine Menge von Komponenten, die einen bestimmten Grad an Vertrauenswürdigkeit ausdrücken soll. Die existierenden Vertrauensstufen reichen von den Stufen EAL 1 bis 7 (4, ab Seite 29). Reicht bei der 1. Stufe noch ein reiner Funktionstest, um

das Vertrauen herzustellen, so muss in der Stufe 7 der gesamte Prozess ab dem Entwurf bis zur Implementierung überwacht und dokumentiert werden.

Eine Vertrauensstufe besteht aus einem eindeutigen und beschreibenden Namen einschließlich seiner Kurzform, danach werden ihre Ziele und Absichten vorgestellt. In einem optionalen Anwendungshinweis wird auf mögliche Einschränkungen oder die besondere Anwendung der Vertrauensstufe hingewiesen.

Jede Vertrauensstufe besteht aus einer Menge von Komponenten, die für sie ausgewählt worden sind, die existierenden Vertrauensstufen verwendet aber nicht alle Komponenten aus dem Katalog in Teil 3 der CC. Sie können aber zusätzlich zu den Vertrauensstufen verwendet werden, wenn sie für ein Schutzprofil oder eine Sicherheitsvorgabe verwendet werden können.

Abbildung 8 zeigt den Aufbau einer Vertrauenswürdigkeitsstufe in grafischer Form.

Ein höheres Vertrauen kann auf zwei Arten erlangt werden: Entweder, indem Vertrauenskomponenten anderer Familien eingeschlossen werden, oder indem man eine bestehende Komponente durch eine höher eingestufte Vertrauenskomponente derselben Familie ersetzt. Jede Vertrauensstufe kann durch neue Vertrauenskomponenten erweitert werden. Dabei muss mit jeder neuen Komponente eine Begründung hinzugefügt werden die beschreibt, dass und wie die neue Komponente zu einer besseren Lösung beiträgt. Es ist jedoch nicht erlaubt Vertrauenskomponenten aus einer Vertrauensstufe zu entfernen.

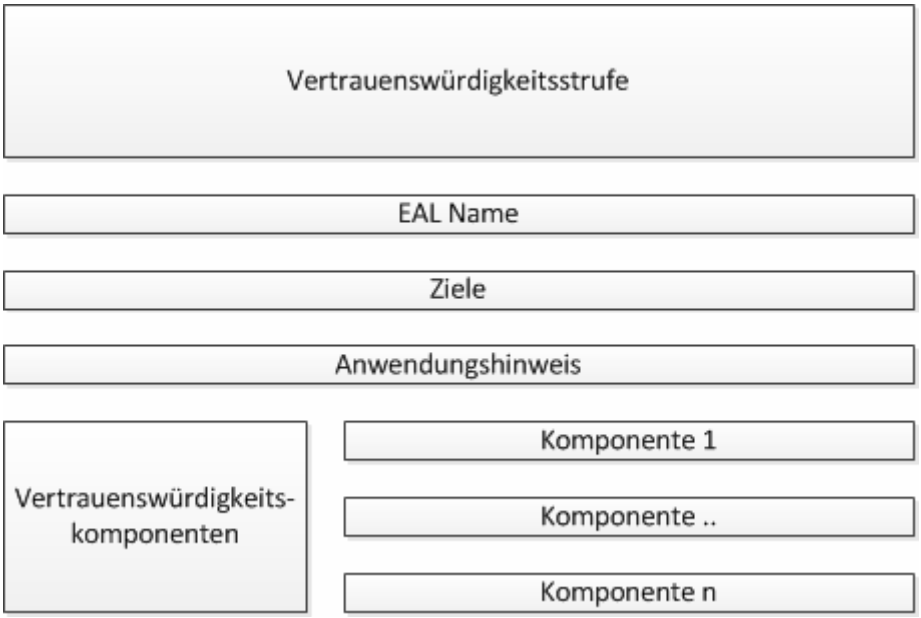


Abbildung 8: Aufbau einer Vertrauenswürdigkeitsstufe

EAL1: funktionell getestet

Die Vertrauensstufe 1 ist anwendbar, wo Vertrauen in die korrekte Arbeitsweise notwendig ist, aber nicht mit ernsthaften Bedrohungen gerechnet wird. Sie ist nützlich wenn unabhängig bestätigt werden soll, dass persönliche oder ähnliche Information ausreichend geschützt wird.

Vertrauensstufe 1 benötigt nur eine beschränkte Sicherheitsvorgabe. Die Sicherheitsanforderungen, welche das EVG erfüllen muss, müssen nur angegeben, aber nicht formell abgeleitet werden.

Vertrauensstufe 1 bietet eine Evaluation des EVG, wie er an den Kunden geliefert worden ist, einschließlich unabhängiger Tests, ob die Spezifikation erfüllt worden ist, und eine Überprüfung der bereitgestellten Hilfsdokumente. Es ist beabsichtigt, dass die Evaluation der Vertrauensstufe 1 mit der Hilfe des Entwicklers erfolgreich ausgeführt werden kann und dabei der Aufwand gering bleibt.

Eine Evaluation auf dieser Stufe sollte Belege liefern, dass der EVG konsistent mit seiner Dokumentation arbeitet.

EAL2: strukturiert getestet

Die Vertrauensstufe 2 erfordert die Mitarbeit des Entwicklers, der Design-Informationen und Testresultate liefern muss. Es sollte aber nicht mehr Mitarbeit erwartet werden, als in der Praxis üblich. Daher sollte der Test weder wesentlich mehr Zeit noch Geld in Anspruch nehmen. Die Vertrauensstufe 2 ist geeignet, wenn dem Entwickler oder Anwender eine geringe bis mittlere Vertrauenswürdigkeit unabhängig bestätigt werden soll, auch wenn die Informationen zur Entwicklung unvollständig verfügbar sind – was passiert, wenn zum Beispiel die Entwickler nur eingeschränkt verfügbar sind.

EAL3: methodisch getestet und überprüft

Die Vertrauensstufe 3 bringt einem gewissenhaften Entwickler maximales Vertrauen in sein Sicherheitsdesign, indem es schon in der Entwurfsphase überprüft wird; dabei sind keine wesentlichen Änderungen bewährter Sicherheitspraktiken notwendig.

Die Vertrauensstufe 3 ist überall einsetzbar, wo der Entwickler oder Anwender eine mittlere Stufe unabhängig bestätigter Sicherheit erwarten, und dafür eine vollständige Untersuchung des EVG und seiner Entwicklung bedürfen, ohne dass diese Untersuchung eine wesentliche Änderung der bestehenden Prozesse verlangt.

EAL4: methodisch entwickelt, getestet und überprüft

Die Vertrauensstufe 4 erlaubt dem Entwickler maximales Vertrauen in sein Sicherheitsdesign, das auf der in der Industrie üblichen Praxis basiert, die zwar genau ist, aber kein zusätzliches Expertenwissen, zusätzliche Fähigkeiten oder andere Ressourcen erfordert. Die Vertrauensstufe 4 ist die höchste Stufe, welche auch wirtschaftlich ist und sich eignet, um eine bestehende Produktlinie nachzurüsten.

EAL5: semiformal entworfen und getestet

Die Vertrauensstufe 5 erlaubt einem Entwickler maximales Vertrauen in die Sicherheitstechnik, basierend auf einer strengen und in der Industrie üblichen Praxis, welche in einem mittleren Maß Spezialwissen über Sicherheitstechniken erfordert. Ein entsprechender EVG wird schon mit der entworfen und implementiert die Vertrauensstufe 5

zu erfüllen. Es ist wahrscheinlich, dass die zusätzlichen Kosten, die für die Erlangung der Vertrauensstufe 5 investiert werden müssen, sich im Rahmen halten.

Die Vertrauensstufe 5 ist überall anwendbar wo Entwickler ein hohes Ausmaß an unabhängig bestätigtem Vertrauen in die Sicherheit brauchen, die Entwicklung geplant und mit strengen Methoden durchgeführt wird und trotzdem die Kosten für die Sicherheitstechnik in einem vernünftigen Rahmen bleiben sollen.

EAL6: semiformal verifizierter Entwurf und getestet

Die Vertrauensstufe 6 bietet dem Entwickler ein hohes Ausmaß an Vertrauen durch die Anwendung besonderer Sicherheitstechnik auf eine strenge Entwicklungsumgebung, um Vermögenswerte mit hohem Wert zu schützen. Die Vertrauensstufe 6 eignet sich für die Entwicklung von EVGs, die einem hohen Risiko ausgesetzt sind, die zusätzlichen Kosten für die Entwicklung werden mit dem hohen Wert des EVG gerechtfertigt.

EAL7: formal verifizierter Entwurf und getestet

Die Vertrauensstufe 7 ist anwendbar für die Entwicklung sicherer EVGs für Anwendungen in extrem riskanten Situationen oder wenn der äußert hohe Wert des Vermögens die hohen Kosten dieser Vertrauensstufe rechtfertigt. Die praktische Anwendung der Vertrauensstufe 7 ist derzeit auf EVGs beschränkt deren Sicherheitstechnik eine klare Aufgabe hat und ausführlich formell analysiert werden kann.

5.3.4 Zusammengesetzte Vertrauenspakete

Einleitung

Zusammengesetzte Vertrauenspakete (kurz CAPs) werden auf zusammengesetzte EVGs angewandt (wobei Komponenten bereits evaluiert sein können). Die einzelnen Komponenten werden für eine bestimmte Vertrauensstufe oder ein anderes in der Sicherheitsvorgabe definiertes Vertrauenspaket zertifiziert. (4, ab Seite 26)

Allgemein ist empfehlenswert, auch bei einem zusammengesetzten EVG zumindest die EAL1 anzuwenden, da sie leicht umsetzbar ist, und so ein grundsätzliches Vertrauen

geschaffen werden kann. Darüber hinaus bilden CAPs eine Alternative zu den EALs, und sind somit eine zweite Möglichkeit, das Vertrauen in einen zusammengesetzten EVG zu stärken.

Die zusammengesetzten Vertrauenspakete CAP A, B und C bieten in ansteigendem Maß eine höhere Vertrauensstufe, erhöhen aber entsprechend die Kosten und den Umsetzungsaufwand. Der Anwender hat so die Möglichkeit jene Stufe zu wählen, die am besten zu seinen Anforderungen und Ressourcen passt. Unabhängig von der gewählten Stufe erhöht schon allein die Verwendung von CAPs die Vertrauenswürdigkeit durch einen eindeutigen Namen, der den zusammengesetzten EVG leichter identifizierbar macht.

CAPs beinhalten nur einen Bruchteil der Familien und Komponenten des Katalogs der Vertrauenswürdigkeitskomponenten. Das liegt daran, dass sie bereits evaluierte Komponenten als Basiskomponenten verwenden können, die nicht erneut evaluiert werden müssen. CAPs berücksichtigen die Interaktion zwischen verschiedenen Komponenten und stellen auf höheren Vertrauensstufen sicher, dass auch die Schnittstellen zwischen Komponenten getestet worden sind. Da bei der Zusammenstellung der Komponenten Schwachstellen auftreten können, wird der EVG auch einer Schwachstellenanalyse unterzogen.

CAPs bestehen aus einer passenden Kombination von Vertrauenskomponenten. Jede CAP besteht aus maximal einer Komponente aus einer Vertrauensfamilie, wobei die Abhängigkeiten aller Komponenten berücksichtigt werden.

CAP A: strukturiert zusammengesetzt

CAP A bietet eine geringes Ausmaß von Vertrauenswürdigkeit für zusammengestellte EVGs und ist leicht zu implementieren (4, Seite 48). Der Entwurf erfordert keine vollständige Information der Entwicklung; der Entwickler der betroffenen Komponente muss aber Information zum Entwurf und den Testresultaten der Zertifizierung der Komponente liefern. Details über Komponenten, von denen man abhängig ist, werden nicht benötigt.

Die Umsetzung der Sicherheitsanforderungen bei CAP A werden überprüft, indem die Sicherheitsvorgaben mit den Ausgaben der Evaluation verglichen werden. Außerdem werden die Schnittstellen zwischen den EVG-Komponenten dokumentiert und der

zusammengesetzte EVG wird einer Schwachstellenanalyse unterzogen. Unabhängige Tests der Schnittstellen der Basiskomponenten können die Aussagekraft der Test stärken.

CAP B: methodisch zusammengesetzt

CAP B steigert die Sicherheit gegenüber des CAP A wesentlich, indem eine höhere Testabdeckung der Sicherheitsfunktionalität verlangt wird. CAP B bietet maximale Vertrauenswürdigkeit, ohne dafür das EVG wesentlich ändern zu müssen (4, Seite 50). Die Interaktion zwischen den EVG-Komponenten wird im Detail überprüft, die Entwickler der Basiskomponente werden auf dieser Stufe jedoch noch nicht eingebunden.

Bei der Überprüfung der Sicherheitsfunktion werden die Ausgaben der Evaluationen der einzelnen Komponenten ebenso berücksichtigt, wie die Schnittstellendefinitionen. Zusammen bilden sie die zusammengesetzten Entwicklungsinformationen, welche das Sicherheitsverhalten detailliert beschreiben.

Die Dokumentation des zusammengesetzten EVGs enthält im CAP B alle Elemente aus CAP A und nun auch belegbare Testergebnisse der Entwickler, Informationen über die Entwicklung, sowie die Begründung der Zusammensetzung und eine unabhängige Bestätigung der Resultate der Entwickler. Die Schwachstellenanalyse muss bei CAP B außerdem von einem Gutachter beglaubigt sein.

CAP C: methodisch zusammengesetzt, getestet und überprüft

CAP C gegenüber Cap B noch mal einen bedeutenden Anstieg an Vertrauenswürdigkeit und bietet so maximale Vertrauenswürdigkeit für einen zusammengesetzten EVG; die Entwickler müssen aber bereit sein, aufwändige Anpassungen im EVG vorzunehmen, um den Anforderungen für CAP C zu entsprechen. (4, Seite 52)

Wie bei CAP-B enthält CAP C eine detaillierte Analyse der EVG-Komponenten und der Schnittstellen, bindet jetzt aber auch Informationen über die Basiskomponenten in die Analyse ein – ein voller Zugriff auf die Entwicklungsinformation der Basiskomponente ist jedoch auch hier nicht nötig.

CAP-C erlaubt einem Entwickler maximale Vertrauenswürdigkeit durch eine positive Analyse der Interaktionen zwischen den Komponenten in einem zusammengesetzten EVG, die, auch wenn sie detailliert ist, nicht den vollen Zugriff auf die Entwicklungsinformationen der Basiskomponente braucht. Im Unterschied zu CAP B, das nur von Angreifern mit einem grundlegenden Angriffspotential ausgeht, erwartet sich CAP C Angreifer mit erhöhtem Angriffspotential. Entsprechend dazu enthält CAP C eine Beschreibung des EVG-Designs und eine Demonstration der Widerstandsfähigkeit gegenüber hohem Angriffspotential.

6 Interaktiver Kurs

6.1 Motivation

Ein wesentlicher Teil dieser Arbeit ist das didaktische Ziel, Sicherheitsstandards, im Speziellen die Common Criteria, Schülern der HTL näher zu bringen. Die Auseinandersetzung mit dem Standard hat zwei Ziele:

1. Das Interesse für Sicherheit soll geweckt werden. Schüler im HTL-Alter kennen Sicherheit vorrangig als Software-Eigenschaften wie Verschlüsselung von Web-Kommunikation in einem Browser oder die Anmeldung bei einer Web-Anwendung. Das Verständnis für Sicherheit als formalisiertes ganzheitliches Konzept, das Soft- und Hardware ebenso einschließt wie die Einsatzumgebung, ist allgemein weniger ausgeprägt, und soll hier geschärft werden.

2. Die Auseinandersetzung mit einem Standard soll den Nutzen von Standardisierung, den Aufbau und Inhalts von Standards vermitteln, und beim späteren Übergang in das Arbeitsleben die Arbeit mit diversen Standards, wie sie in der IT durchaus üblich ist, erleichtern.

6.2 Medium

Bei der Vermittlung der Inhalte dieser Arbeit ist es wichtig, den diskutierten Stoff Zielgruppengerecht didaktisch aufzubereiten, damit er von ihr angenommen wird. Gleichzeitig sollte sich die Lösung in den modernen Unterricht an der Schule einbauen lassen. Aus diesem Grund wird auf Papier-basiertes Lehrmaterial verzichtet, statt dessen fiel die Entscheidung, die Arbeit als Moodle-Kurs aufzubereiten.

Moodle ist ein Lernsystem, das mittlerweile an vielen Schulen, Universitäten und anderen Bildungseinrichtung zur Organisation und Durchführung von Lehrveranstaltungen und Kursen verwendet wird. Abgesehen von der reinen Darstellung von Lehrmaterial wie Texten, Bildern und Videos enthält Moodle Module zur Erstellung von Prüfungen verschiedener Ausprägung.

Ein besonderer Vorteil von Moodle ist, dass einzelne Kurse, wie auch der interaktive Kurs für diese Arbeit, als unabhängiges Modul entwickelt, gespeichert, und dann in jede Moodle-Plattform integriert werden kann. Das erleichtert die Integration in den Unterricht und die Akzeptanz unter Lehrern und Schülern, die für den täglichen Unterricht ohnehin schon eine laufende Moodle-Instanz verwenden.

6.3 Methode

Aus diesem Pool verschiedener Prüfungsarten für Moodle bietet sich die Multiple-Choice-Variante für Prüfungen besonders an, da die klare Markierung von richtigen und falschen Antworten im Gegensatz zu freiem Text eine automatisierte Bewertung zulässt.

Eine typische Multiple-Choice-Prüfung besteht dabei aus einer Menge von Fragen mit mehreren Antworten, von denen eine oder mehrere jeweils richtig oder falsch sind. Ein Schüler, der so einen Test absolviert, bekommt eine Untermenge der vorhandenen Fragen und muss diese, meist unter Zeitdruck, beantworten. Die Auswertung der Fragen erfolgt sofort, sie können dann, je nach Einstellung, wiederholt beantwortet werden.

Die Fragen der Multiple-Choice-Prüfung beziehen sich auf die einzelnen Kapitel dieser Arbeit und fragen wesentliche Aspekte ab, welche an Schüler vermittelt werden sollen. Ein besonderes Augenmerk wurde auch darauf gelegt, dass die Fragen auch als kritische Auseinandersetzung mit dem Stoff und den CC verstanden werden können, und den Leser motivieren sollen, selbst ähnliche Fragestellungen im Umgang mit Standards, und speziell mit Sicherheitsstandards und maßnahmen, anzuwenden.

6.4 Installation

Der Moodle-Kurs wird mit dieser Masterarbeit als digitaler Anhang auf CD ausgeliefert. Eine Installationsanleitung für den Kurs findet sich im Anhang A am Ende dieses Dokuments.

7 Zusammenfassung

Wir ursprünglich geplant, erklärt die Arbeit kompakt und auch auf einem für Laien zugänglichen Niveau die Common Criteria, sowie ihre Umgebung, um sie anschließend in einem interaktiven Moodle-Kurs für HTL-Schüler aufzubereiten. Die wesentlichen Meilensteine der Arbeit fassen sich wie folgt zusammen:

Die Common Criteria werden in ihrem Kontext vorgestellt. Durch die vorangestellte und detaillierte Geschichter vorhergehender Standards werden dem, zuvor mit Sicherheitsstandards möglicherweise nicht vertrauten, Leser, auf verständliche Art die Herkunft und der Bedarf für die Common Criteria erklärt.

Terminologie und Sicherheitsmodell werden ausführlich und reichlich bebildert erklärt, die umfassende Erklärung, die, im Vergleich zu in Standards üblicher Sprache, wesentlich informeller ausfällt, erleichtert dem Leser den Zugang zu den wesentlichen Grundbausteinen für das Verständnis der Common Criteria.

Durch die Erklärung der Spezifikation von Sicherheitsvorgaben und -profilen bekommt der Leser das nötige Wissen um einerseits die in Folge erklärten Komponentenkataloge zu verstehen, und andererseits selbst Sicherheitsvorgaben und Schutzprofile zu entwerfen. Als besonders nützlich sollte sich auch die Einbindung der Vorstellung der Schutzprofile und Sicherheitsvorgaben mit geringer Vertrauenswürdigkeit heraus stellen, da sie besonders bei Projekten mit weniger hoher Vertrauensstufe weniger Aufwand verursachen.

Abgerundet wird die Arbeit durch den erfolgreich umgesetzten interaktiven Moodle-Kurs, der in unterhaltsamer interaktiver Form das in dieser Arbeit besprochene Wissen in Multiple-Choice-Test vermittelt. Mit dem digitalen Kurs in der CD im Anhang dieser Arbeit sowie der mitgelieferten Installationsanleitung steht jedem Lehrer der Weg frei, den Kurs einfach in ein existierendes Moodle-System zu integrieren.

In Hinsicht auf den Einsatz des Kurses, und damit die Nützlichkeit dieser Arbeit, wäre es interessant im Rahmen einer weiteren Arbeit zu erkunden, wie gut Lehrer diesen Stoff in ihren Lehrplan einbauen können, wie die Kurse von Lehrern und Schülern aufgenommen werden, und inwiefern sie das Sicherheitsverständnis von Schülern verbessern.

Literaturverzeichnis

[1] 1. The Common Criteria Portal. [Online] http://www.commoncriteriaportal.org.

[2] 2. *Common Criteria for Information Technology Security Evaluation; Part 1: Introduction and general model; Version 3.1, Revision 3, Final.* Juli : CCMB (Common Criteria Management Board), Juli 2009. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf.

[3] 3. *Common Criteria for Information Technology Security Evaluation; Part 2: Security functional components; Version 3.1, Revision 3, Final.* s.l. : CCMB (Common Criteria Management Board), Juli 2009. http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf.

[4] 4. *Common Criteria for Information Technology Security Evaluation; Part 3: Security assurance components; Version 3.1, Revision 3, Final.* s.l. : CCMB (Common Criteria Management Board), Juli 2009. http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf.

[5] 5. *ISO/IEC 15408-1:2009 Part 1: Introduction and general model.* s.l. : ISO/IEC, 2008.

[6] 6. *ISO/IEC 15408-2:2008 Part 2: Security functional components.* s.l. : ISO/IEC, 2008.

[7] 7. *ISO/IEC 15408-3:2008 Part 3: Security assurance components.* s.l. : ISO/IEC, 2008.

[8] 8. Moodle.org: open-source community-based tools for learning. [Online]

[9] 9. **Herrmann, Debra S.** *Using the Common Criteria for IT Security Evaluation.* s.l. : Auerbach Publications, 2002. 0849314046.

[10] 10. **Eckert, Claudia.** *IT-Sicherheit: Konzepte - Verfahren - Protokolle.* überarbeitete Auflage (19. April 2006). s.l. : Oldenbourg Wissenschaftsverlag, 2006. ISBN-10: 3486578510.

[11] 11. *DoD Directive 5200.28.* s.l. : Department of Defense, März 1988. http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/d520028p.pdf.

[12] 12. *Department Of Defense Trusted Computer System Evaluation Criteria.* s.l. : Department Of Defense, Dezember 1985. http://csrc.nist.gov/publications/history/dod85.pdf.

[13] 13. *Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria.* Luxembourg : Office for Official Publications of the European Communities, Juni 1991. http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf.

[14] 14. **Merkow, Mark und Breithaupt, James.** *Information Security: Principles and Practices.* s.l. : Prentice Hall. 0131547291.

[15] 15. *Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, Final.* s.l. : CCMB (Common Criteria Management Board), Juli 2009. http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf.

[16] 16. **Witt, Bernhard Carsten.** *IT-Sicherheit kompakt und verständlich: Eine praxisorientierte Einführung.* s.l. : Vieweg+Teubner Verlag, 2006. 3834801402.

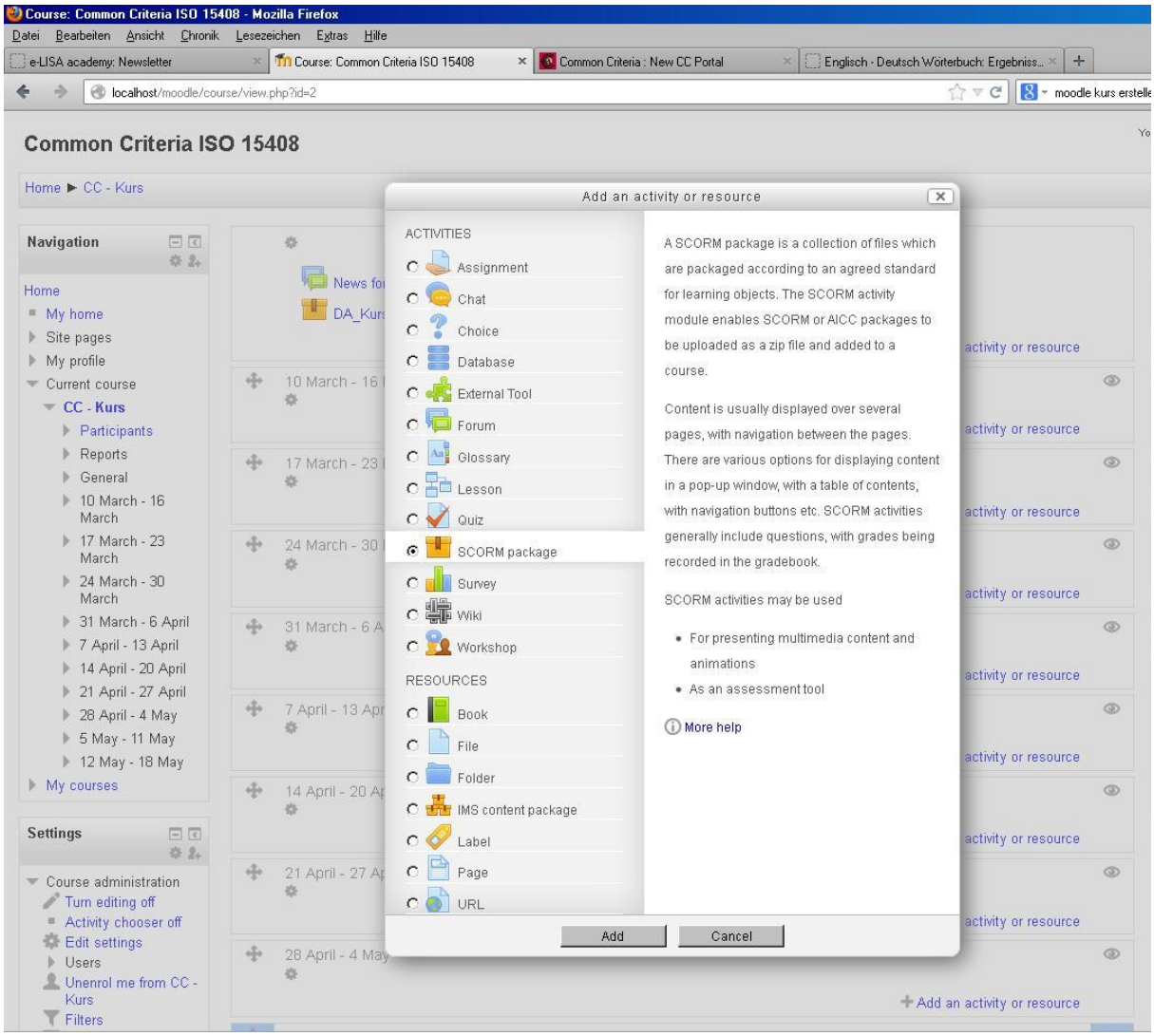
Abbildungsverzeichnis

Tabellenverzeichnis

Anhang A: Installationsanleitung Moodle-Kurs

Falls Sie Moodle installiert haben dann können Sie den Kurs in der der Masterarbeit beiliegenden CD in einem SCORM-Paket im ZIP-Format finden. Um das Paket in Ihre Moodle-Instanz zu integrieren gehen Sie wie unten beschrieben vor:

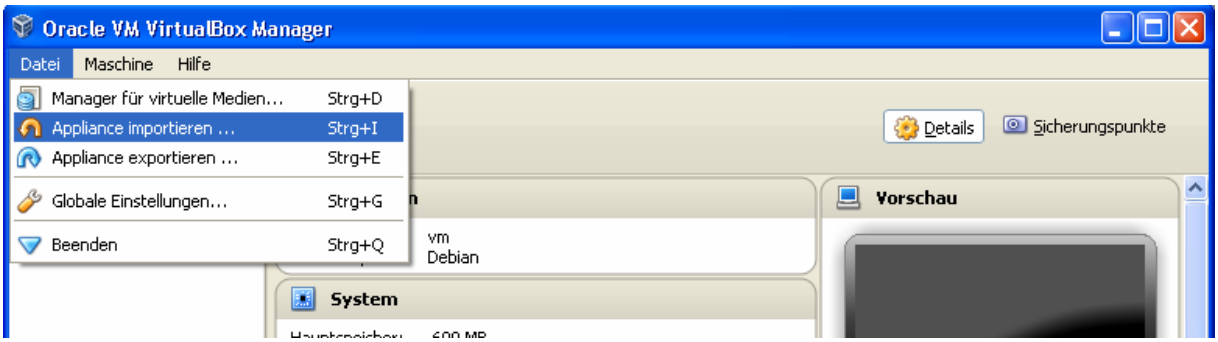
Gehen Sie in den Kursbereich, in den Sie den Kurs integrieren möchten, und gehen so vor, als ob Sie eine neue Aktivität anlegen ("add an activity or resource") wollten.



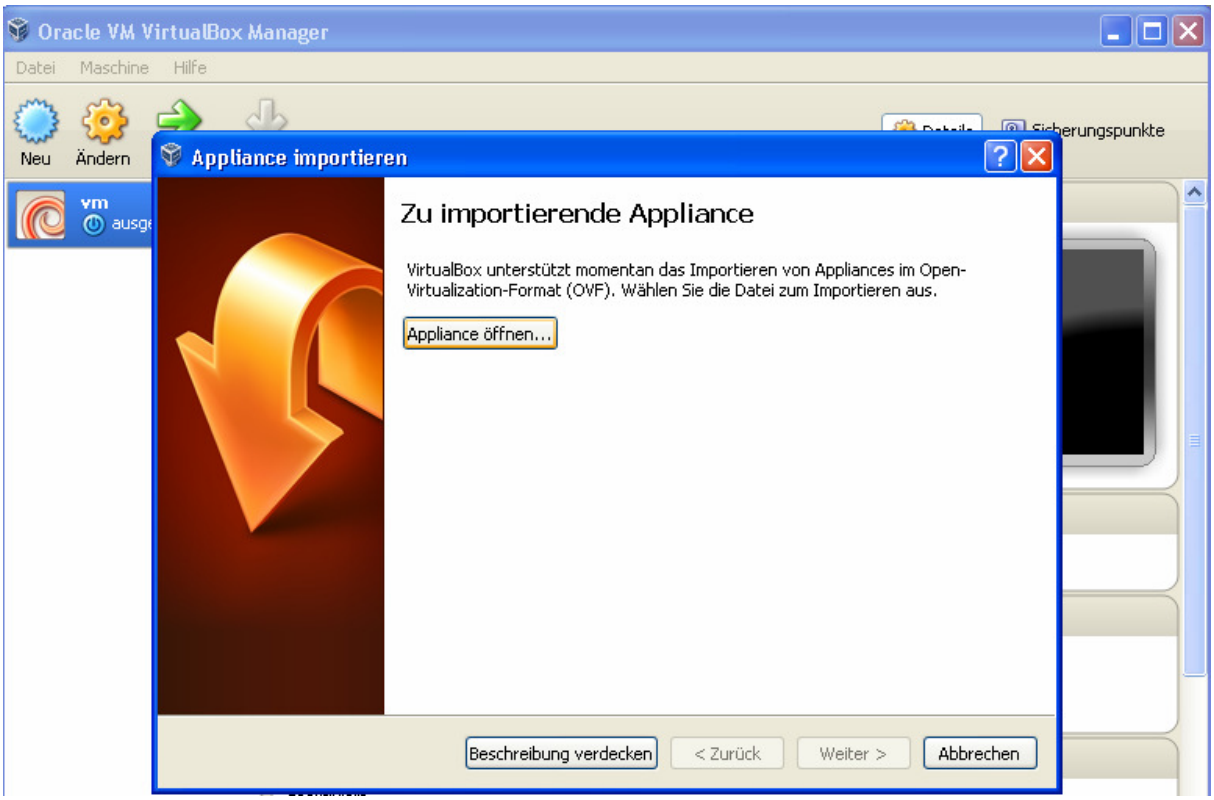
Wählen Sie nun „SCORM package“ aus dem Pop-Up-Menü aus. Laden Sie das SCORM-Paket auf Ihre Moodleplattform, geben Sie einen Namen und eine Beschreibung an und klicken Sie auf „Speichern“ („Save and return to course“).

Falls Sie noch kein Moodle installiert haben, dann können Sie die Moodle-Appliance (Datei Kurs_VM.ova) in der der Masterarbeit beiliegenden CD finden. In der Appliance ist der Kurs schon integriert. Voraussetzung hierfür ist eine VirtualBox-Installation. Um die Appliance zu importieren gehen Sie wie unten beschrieben vor.

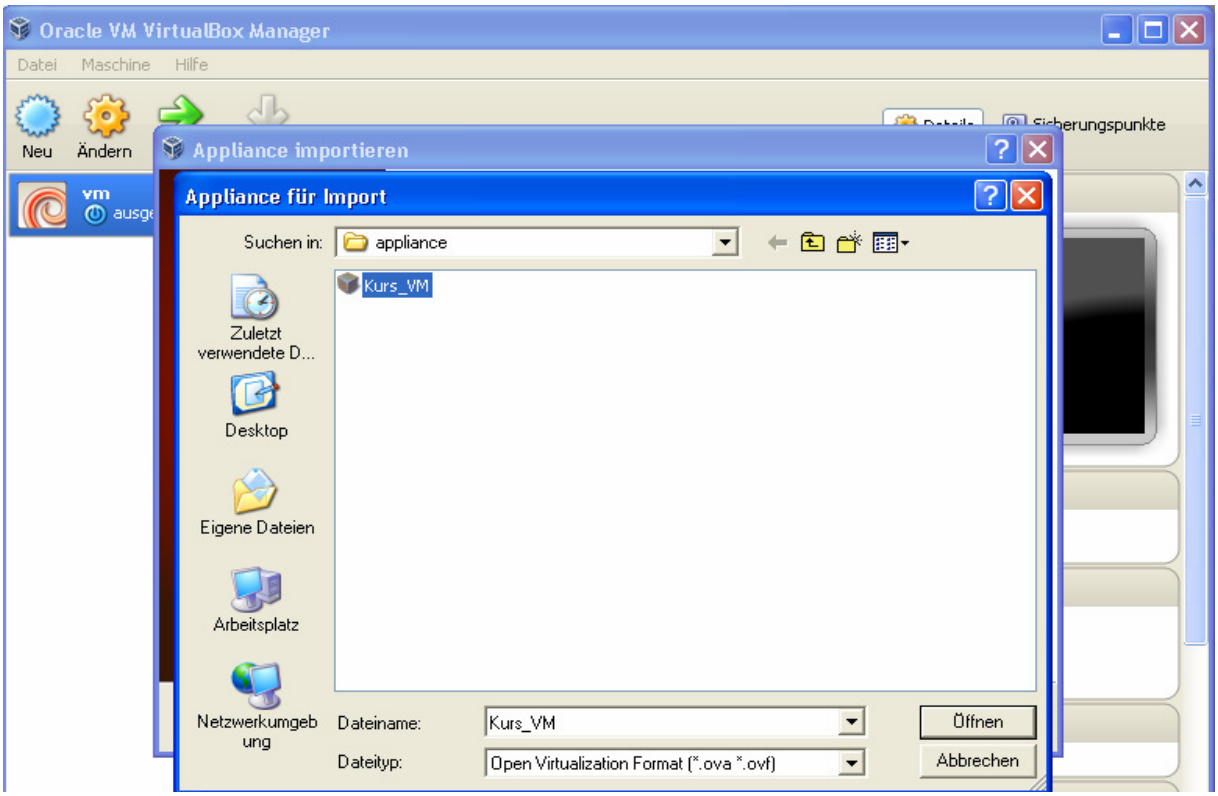
1. Schritt: Öffnen Sie VirtualBox und gehen Sie auf „Datei“ -> „Appliance importieren“.



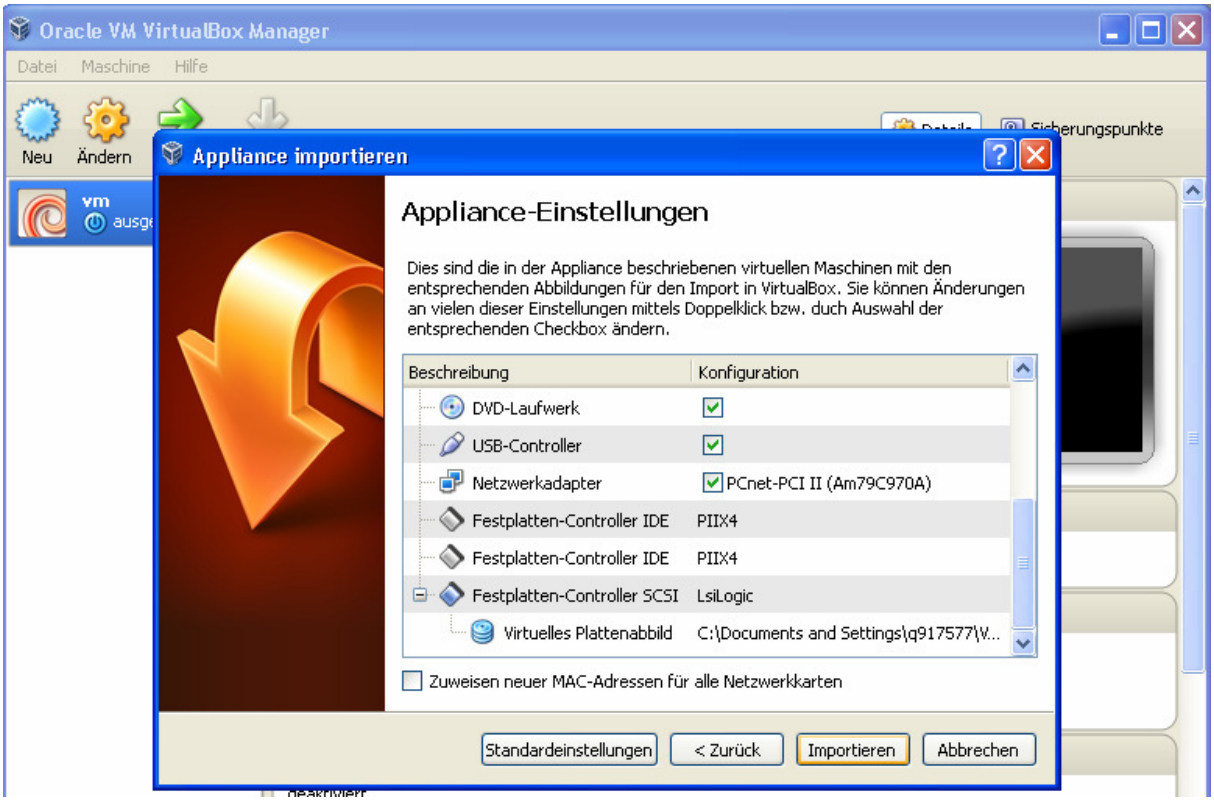
2. Schritt: Nachdem Sie auf „Appliance importieren“ geklickt haben öffnet sich ein Popup-Fenster (s. Bild unten). Klicken Sie auf „Appliance öffnen“.



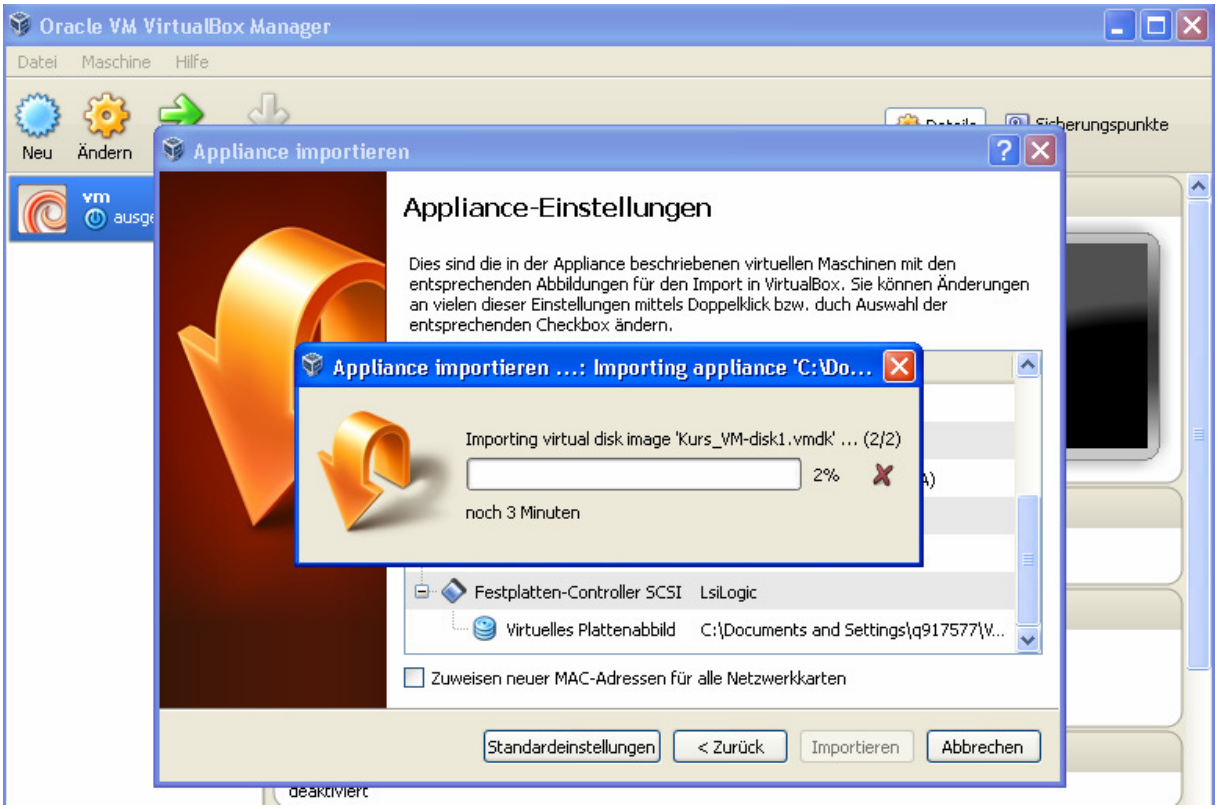
3. Schritt: Nachdem Sie auf „Appliance öffnen“ geklickt haben öffnet sich ein anderes Popup-Fenster (siehe Bild unten). Gehen Sie nun zum Verzeichnis, in dem Sie vorher die Appliance gespeichert/entpackt haben, und wählen Sie die Datei "Kurs_VM.ova" aus. Anschließend klicken Sie auf „Öffnen“. Nachdem Sie auf „Öffnen“ geklickt haben schließt sich das letzte Popup-Fenster und Sie befinden sich in Popup-Fenster, das sich im 2. Schritt geöffnet hat. Hier klicken Sie auf „Weiter“.



4. Schritt: Nachdem Sie auf „Weiter“ geklickt haben, sollten Sie das Bild unten sehen. Hier klicken Sie bitte auf „Importieren“.

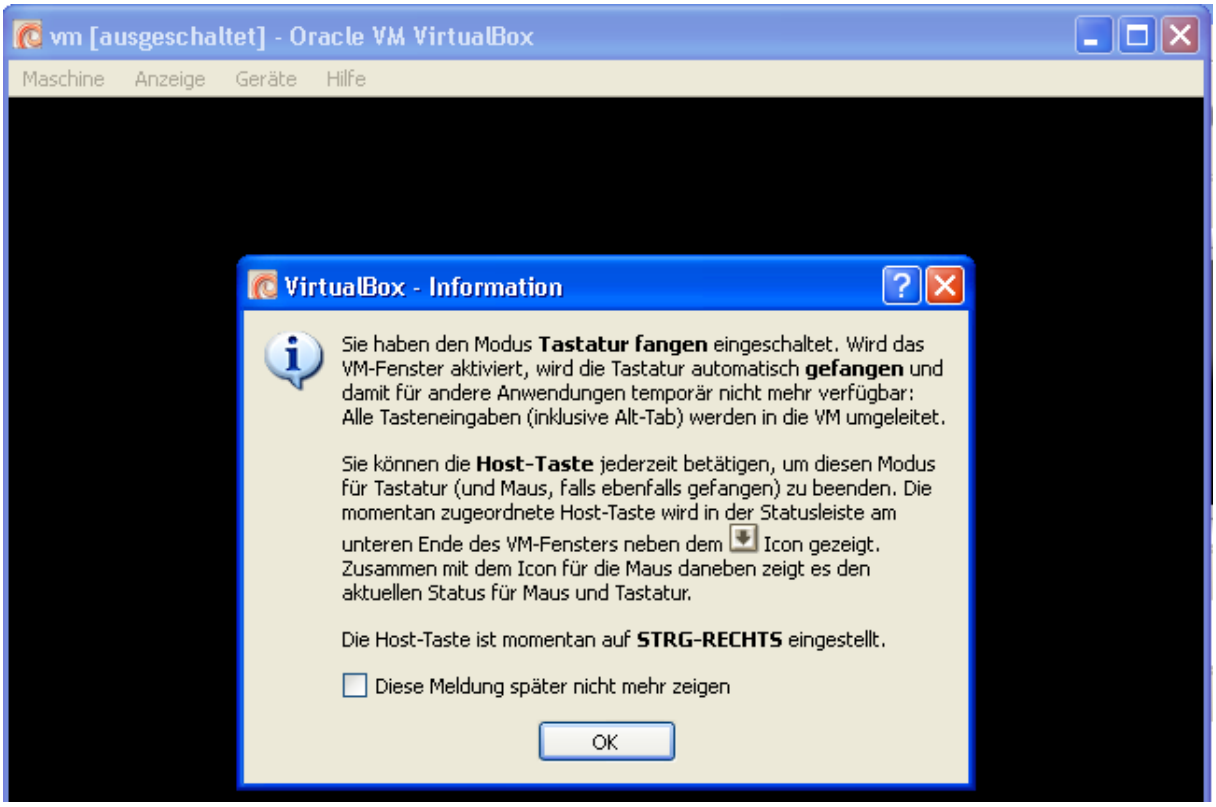


5. Schritt: Nachdem Sie auf „Importieren“ geklickt haben, sollten Sie das Bild unten sehen. Nach paar Minuten sollte die neue Maschine auf Ihre Liste der Maschinen links erscheinen.



6. Schritt: Wählen Sie die Maschine (Blau markiert) und klicken Sie auf starten.

7. Schritt: Nachdem Sie auf „Starten“ geklickt haben sollten Sie das Bild unten zu sehen bekommen. Hier klicken Sie bitte auf „OK“.



8. Schritt: Der Export-Prozess hat alle Konfigurationen der Maschine exportiert. Somit auch die Netzwerk Interface des Hosts. Das muss geändert werden. Wählen Sie hier „Netzwerkeinstellungen ändern“ (Bild: Netzwerkeinstellungen ändern) und im Popup-Fenster (Bild: Netzwerkeinstellungen übernehmen), das sich nachdem Klicken auf „Netzwerkeinstellungen ändern“ öffnet, klicken Sie auf „OK“ um die Netzwerkeinstellungen zu übernehmen.

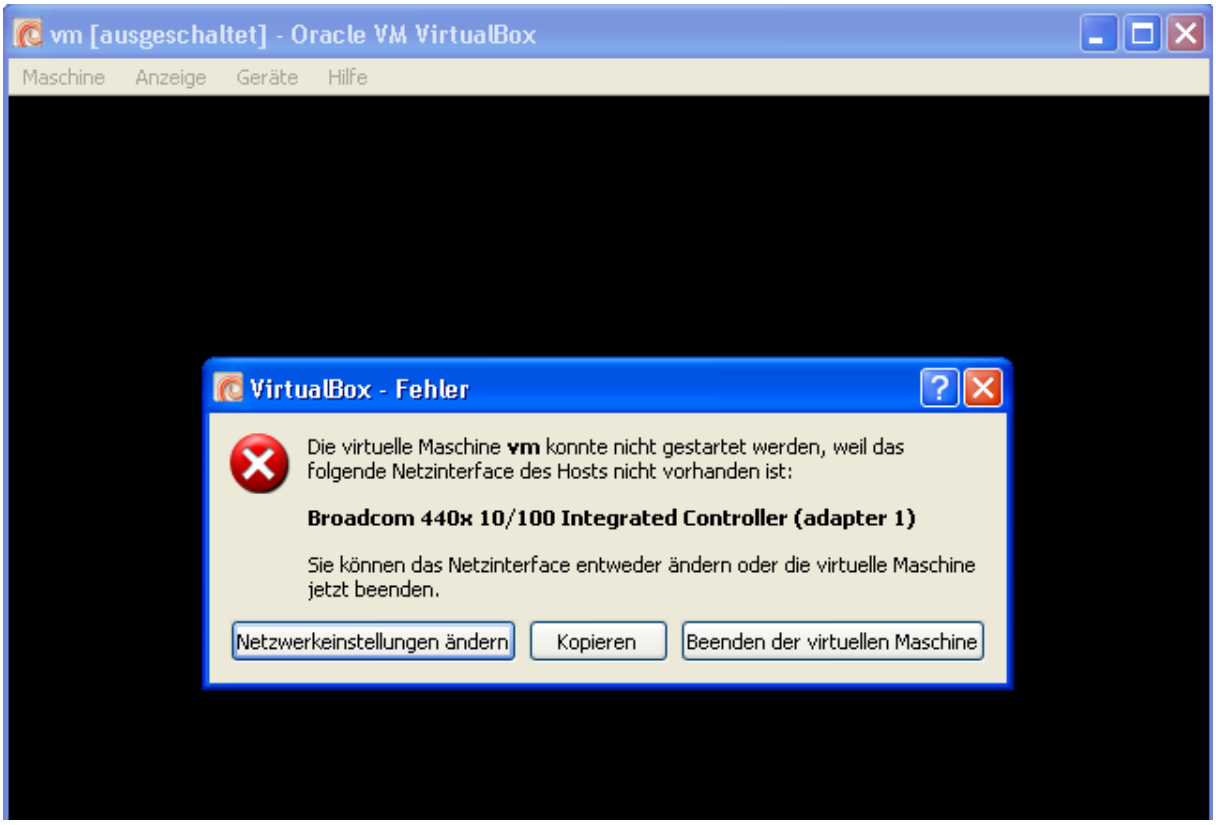


Bild: Netzwerkeinstellungen ändern

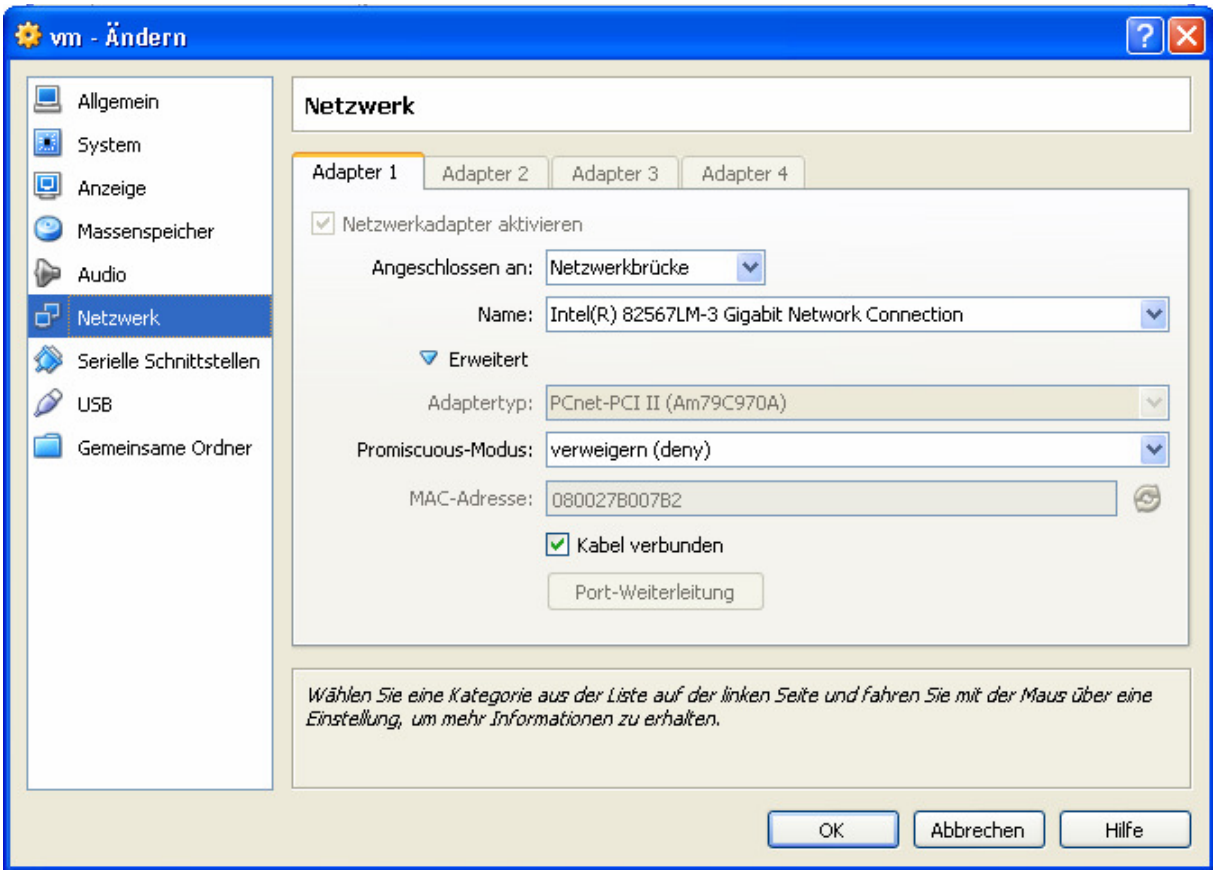


Bild: Netzwerkeinstellungen übernehmen.

9. Schritt: Danach bekommen Sie das erste Bild (VM_Booten) unten zu sehen. Warten Sie bis das zweite Bild (Network konfigurieren) erscheint und wählen Sie „< ok >“ aus (Navigationstasten: TAB, Pfeile; Auswählen: Enter). Falls in der Zwischenzeit sich ein Popup-Fenster öffnet, bei dem nur „OK“ ausgewählt werden kann, dann „OK“ klicken.

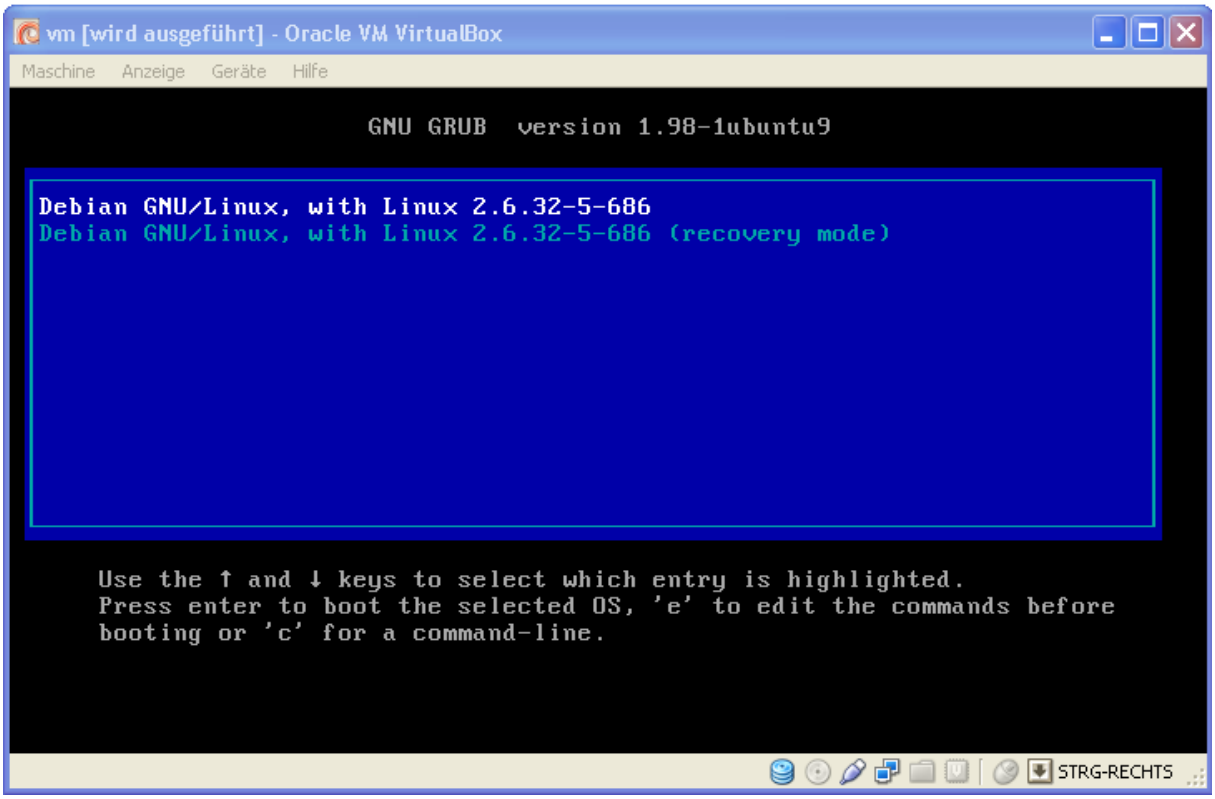


Bild: VMBooten

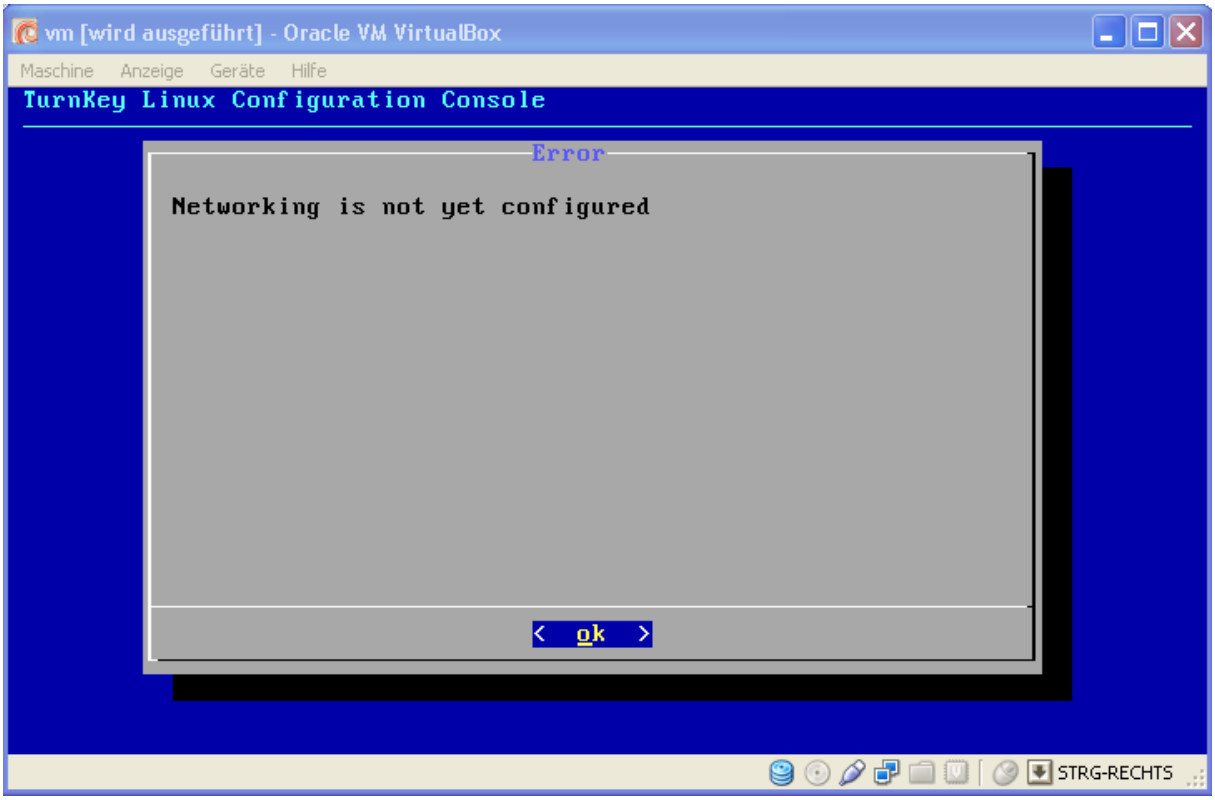
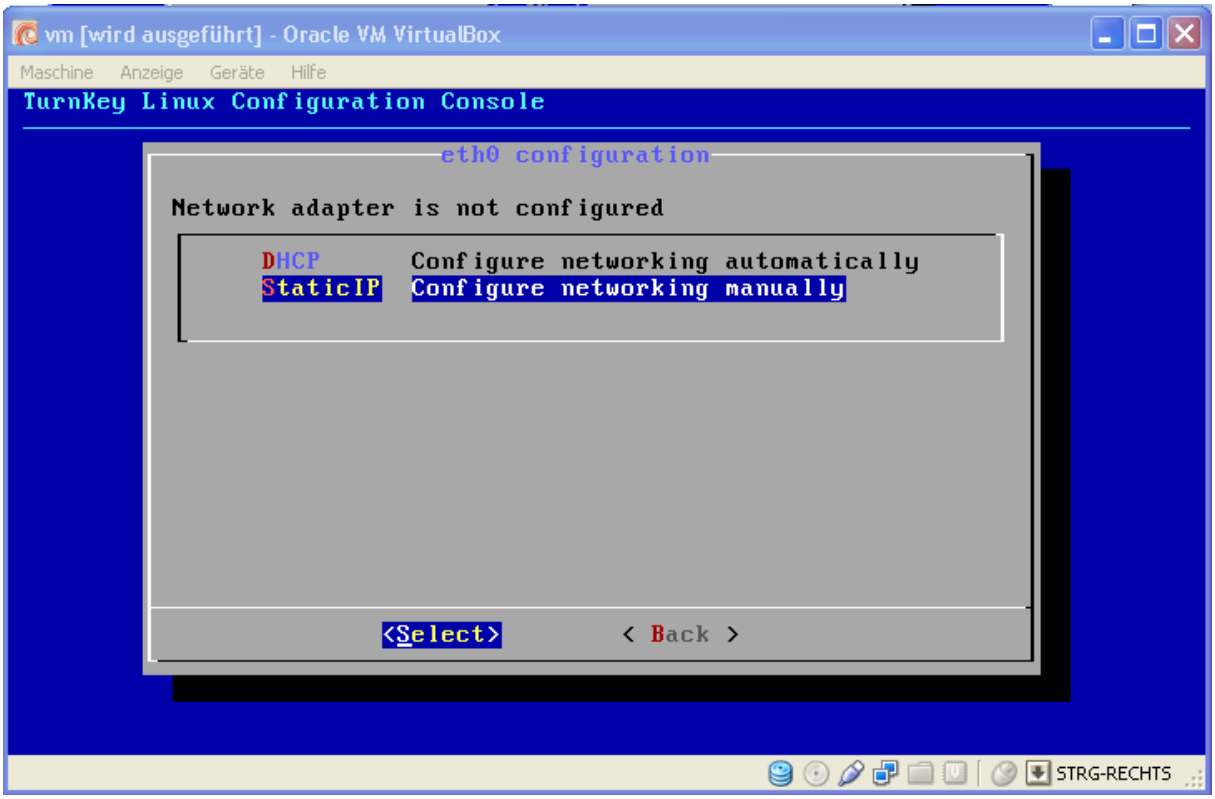


Bild: Network konfigurieren

10. Schritt: Nachdem Sie „< ok >“ ausgewählt haben sollten Sie das Bild unten sehen. Wählen Sie hier „StaticIP“ und dann „<Select>“.



11. Schritt: Nachdem Sie „<Select>“ ausgewählt haben sollten Sie das Bild (IP eintragen) unten zu sehen bekommen. Um IP Address, Netmask und Default Gateway einzutragen müssen Sie zuerst Ihre IP Addresse, Netmask und Default Gateway herausfinden. Starten Sie Eingabeaufforderung (Command Line) und tippen Sie „ipconfig“ ein (s. Bild: IP herausfinden). In meinem Fall werde ich jetzt in das Feld IP Adress „10.16.42.50“ eintragen (die rot markierten Zahlen sollen nicht mit Ihre IP-Adresse übereinstimmen);in das Feld Netmask „255.255.255.0“; in das Feld Default Getaway „10.16.42.254“ (s. Bild: IP eingetragen). Wählen Sie hier (s. Bild: IP eingetragen) bitte „< Apply >“aus.

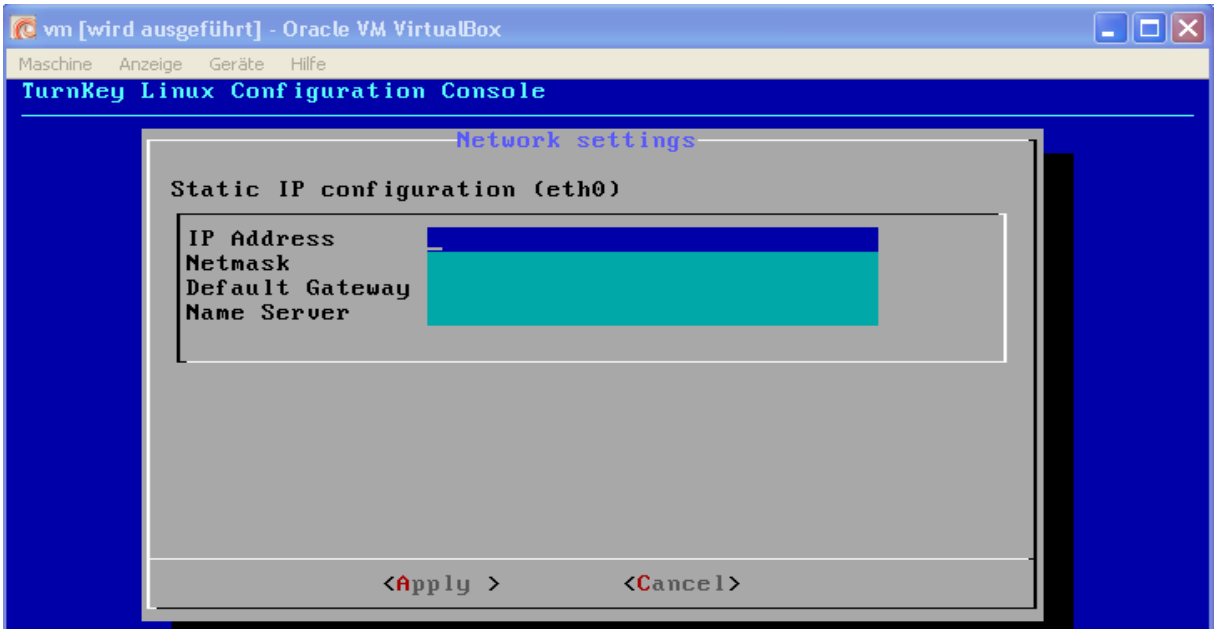


Bild: IP eintragen

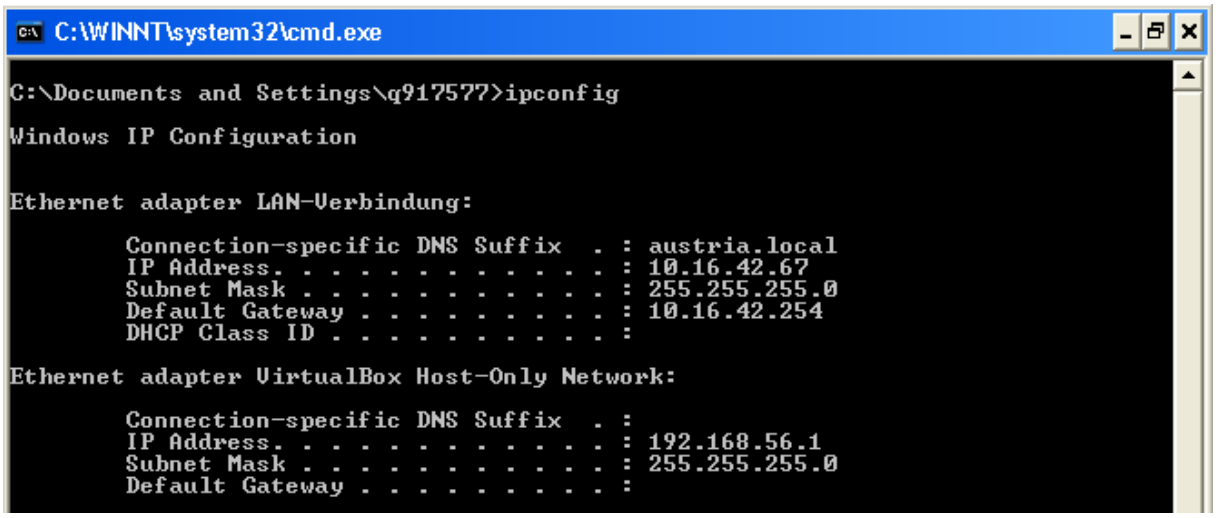


Bild: IP herausfinden

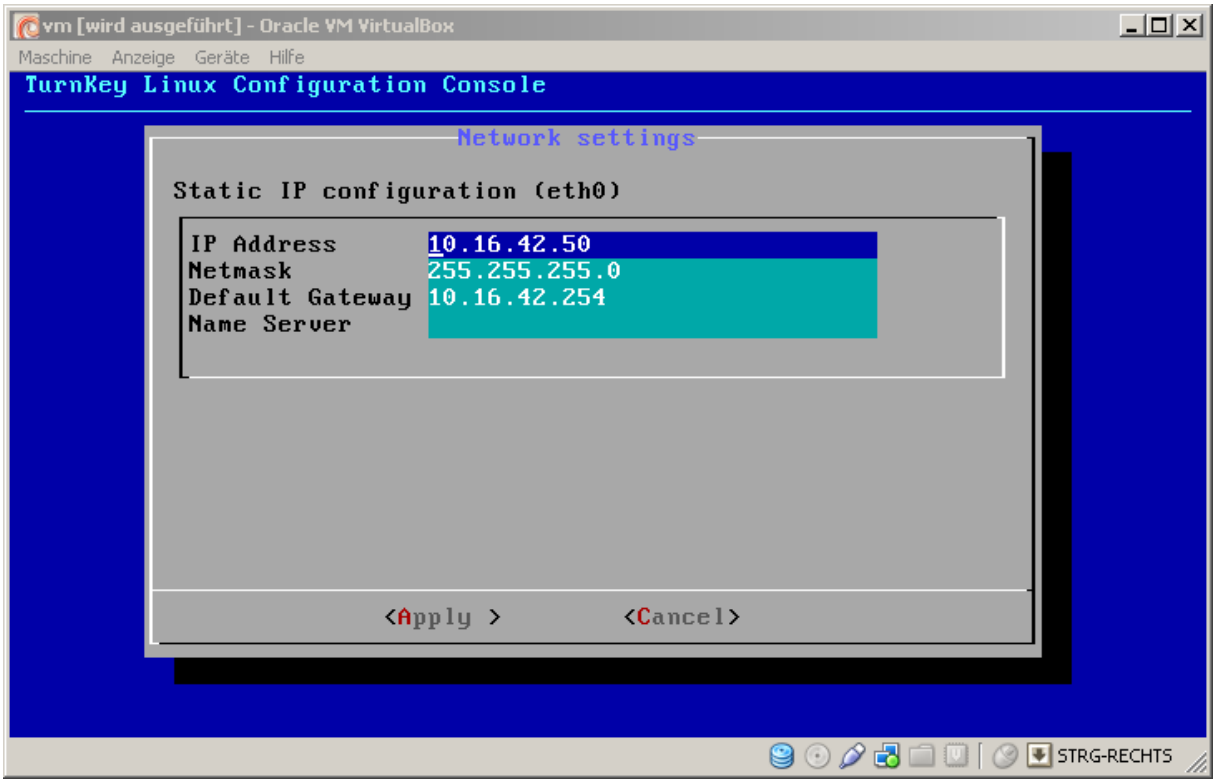
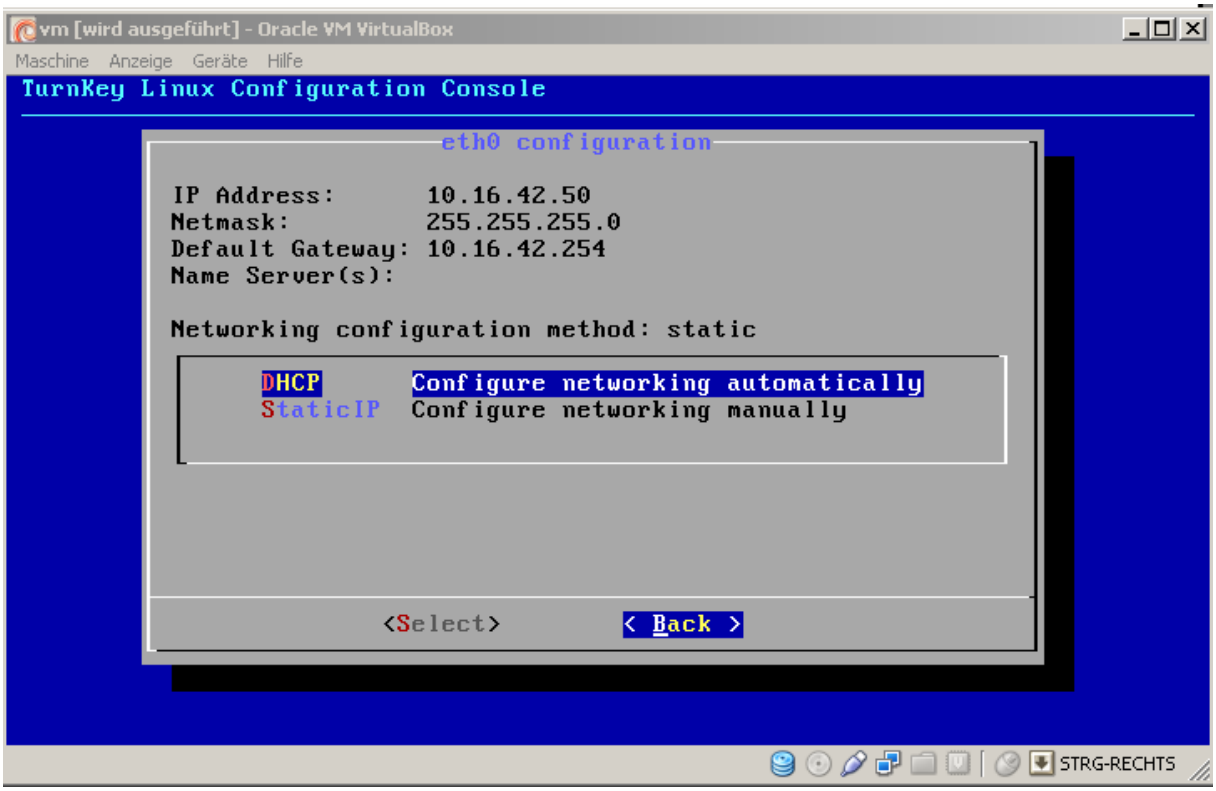
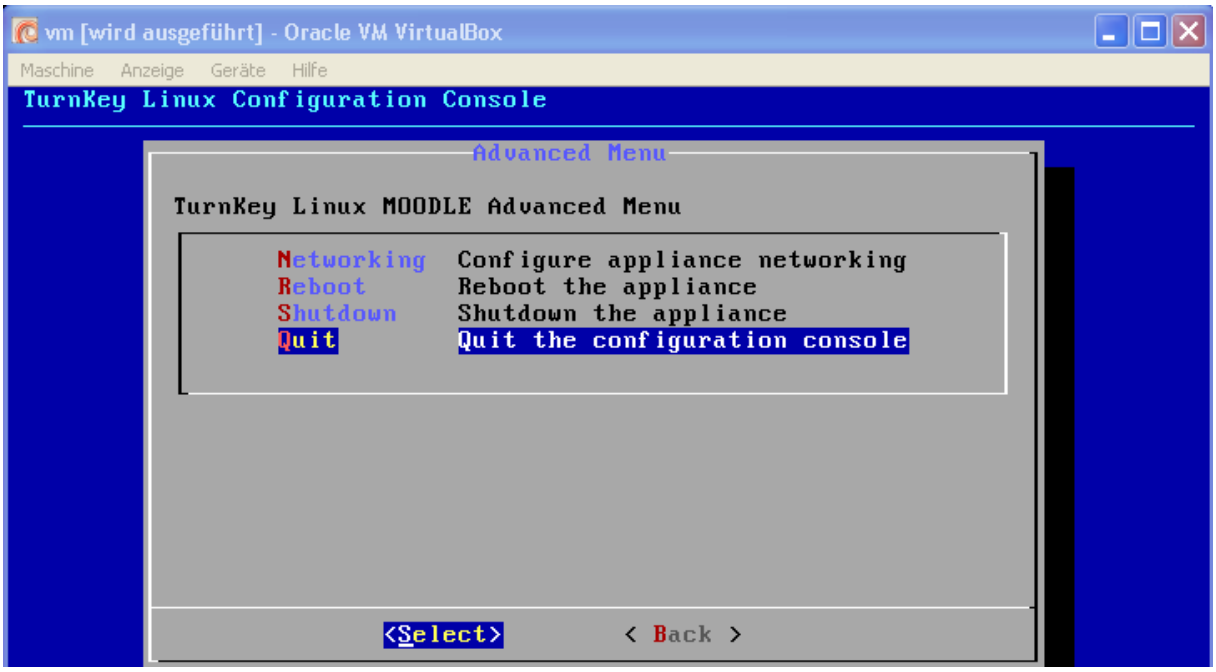


Bild: IP eingetragen

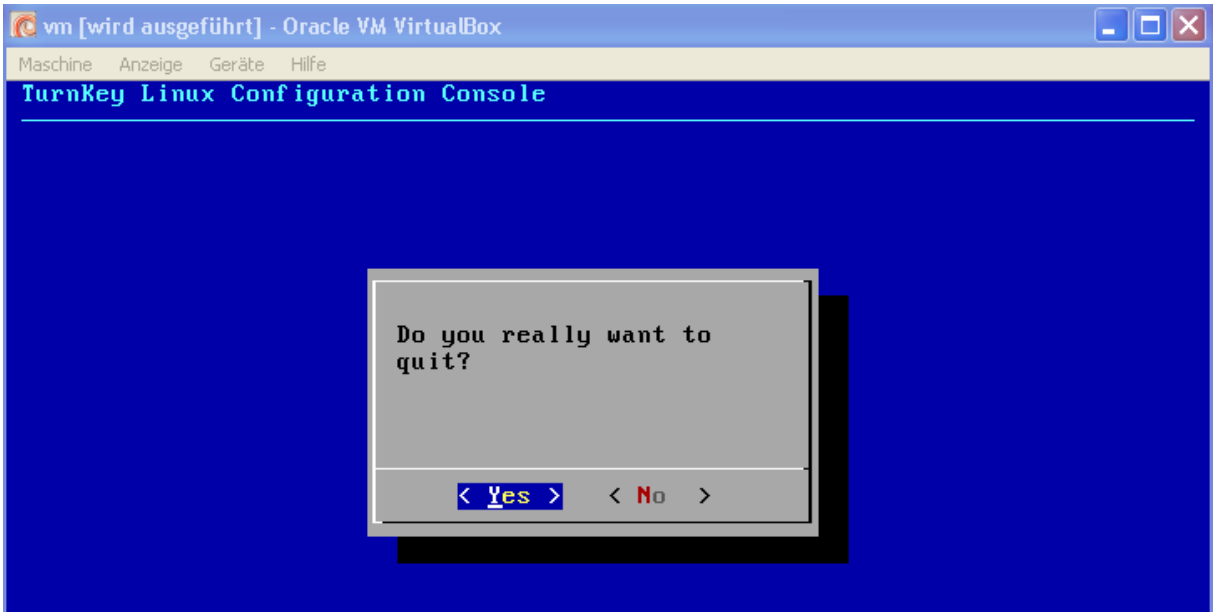
12. Schritt: Nachdem Sie „<Apply>“ ausgewählt haben sollten Sie das nächste Bild zu sehen bekommen. Wählen Sie hier bitte „<Back>“ aus.



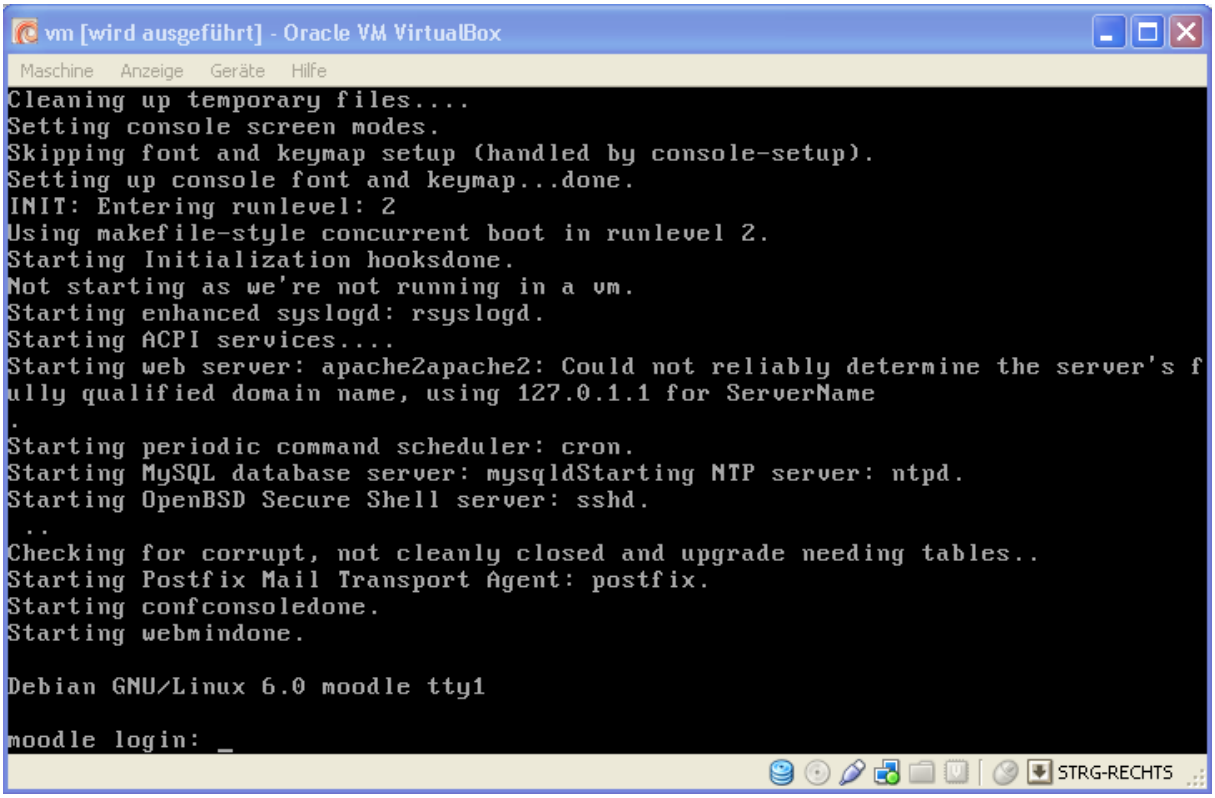
13. Schritt: Nachdem Sie „<Back>“ ausgewählt haben sollten Sie das nächste Bild sehen. Hier wählen Sie zuerst „Quit“ aus und dann bitte „<Select>“.



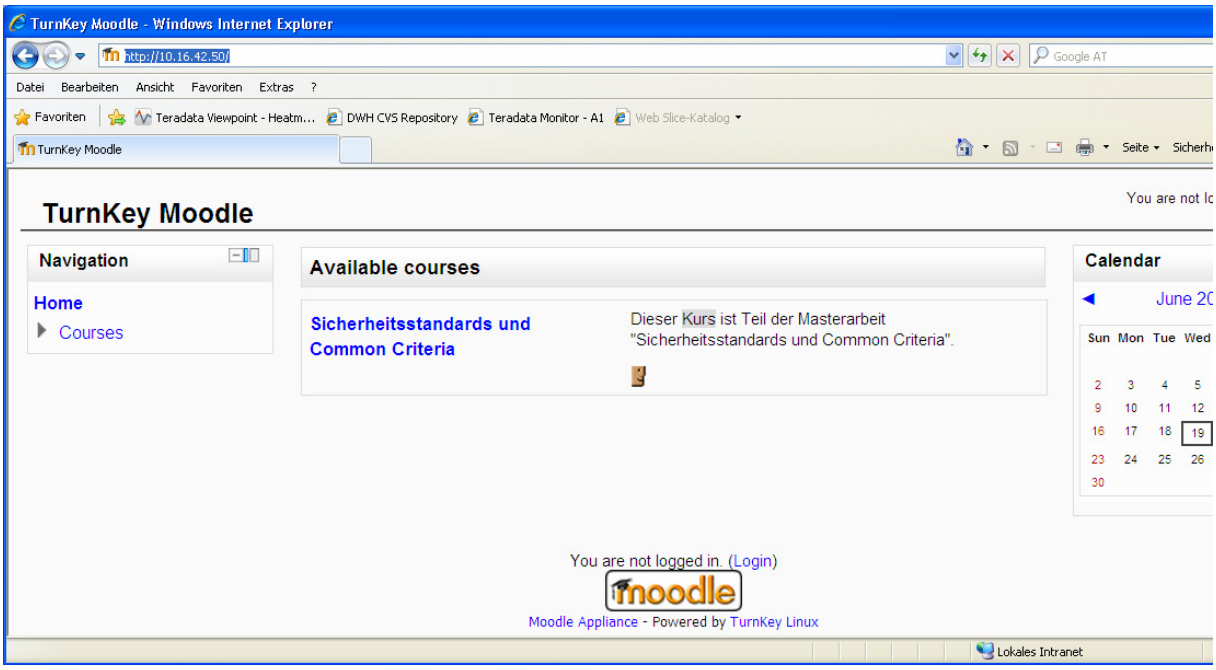
14. Schritt: Nachdem Sie „<Select>“ ausgewählt haben bestätigen Sie bitte, indem Sie „<Yes>“ auswählen, dass Sie Konfiguration verlassen wollen.



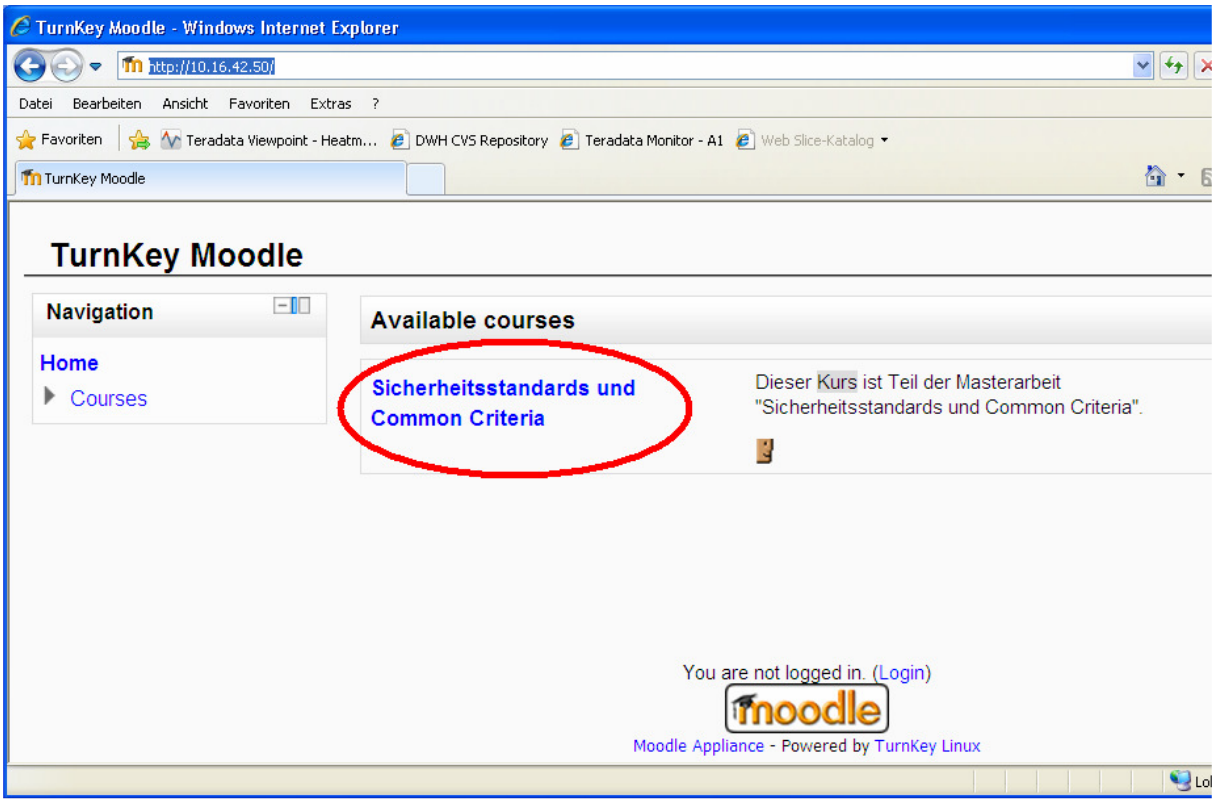
15. Schritt: Nachdem Sie das Verlassen der Konfiguration bestätigt haben sollten Sie das folgende Bild sehen. Sie werden aufgefordert, sich in Moodle einzulogen. Tippen Sie bitte hier „root“ für „moodle login“ und „admin“ für „Password“.



16. Schritt: Öffnen Sie Ihren Lieblingsbrowser und tippen Sie die IP Adresse (in meinem Fall: "http://10.16.42.50/"), die Sie bei der Konfiguration eingetragen haben (s. Bild unten).



17. Schritt: Klicken Sie auf „Sicherheitsstandards und Common Criteria“. Falls Sie eine Sicherheitszertifikat-Meldung bekommen dann ignorieren Sie die Warnung und fahren fort.



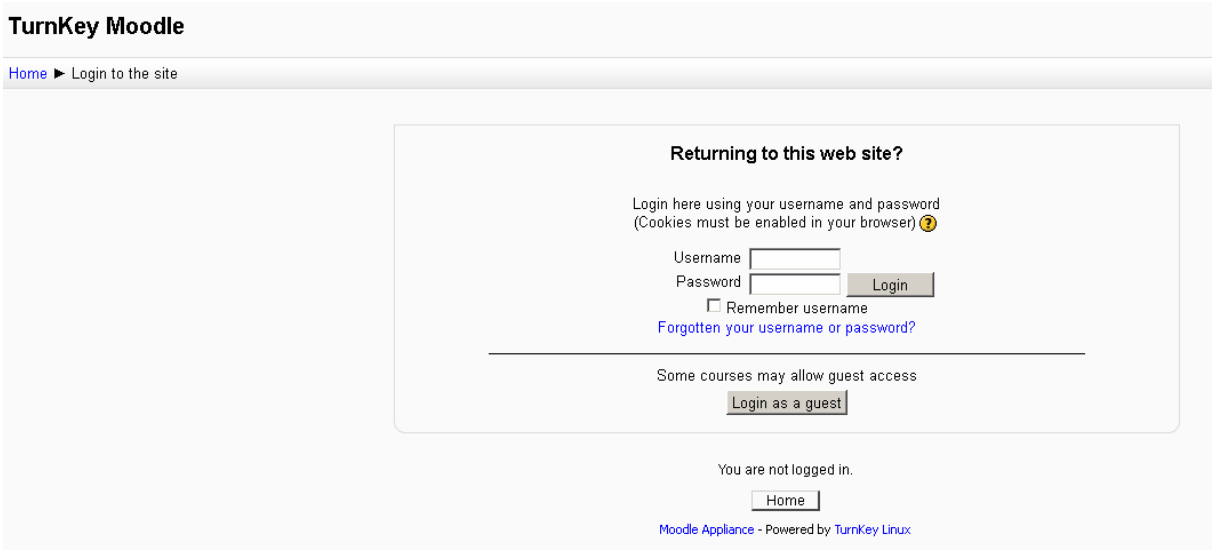
18. Schritt: Einloggen

als Gast

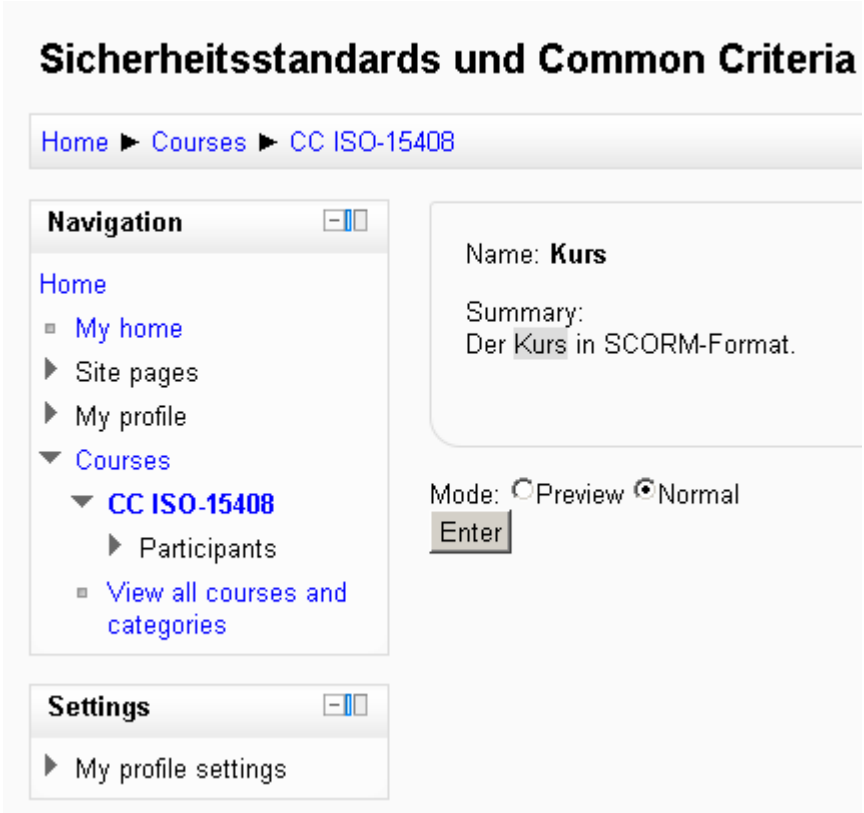
- Username: gast
- Password: CC-iso-15408

als Administrator

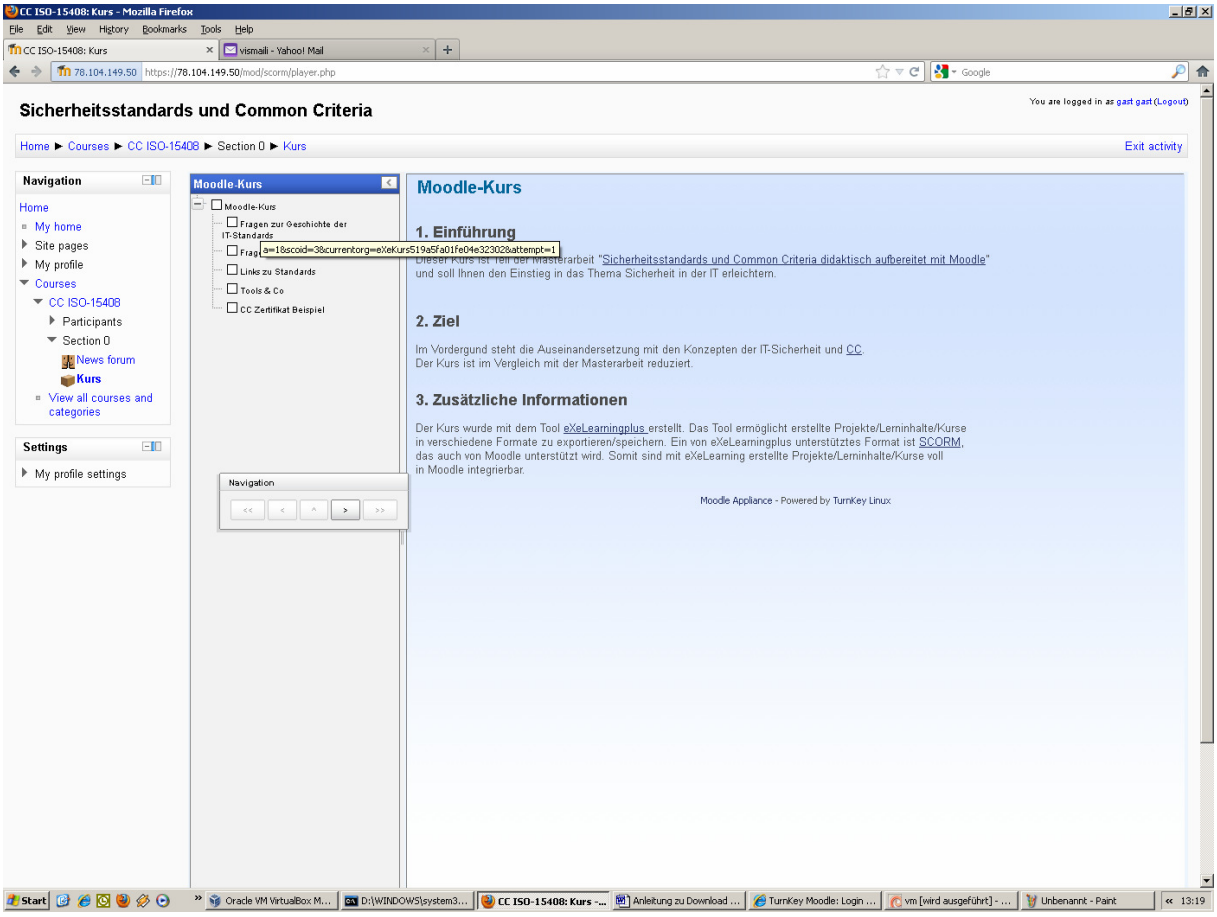
- Username: admin
- Password: admin



19. Schritt: Klicken Sie auf „Enter“.



20. Schritt: Kurs anschauen.


CC ISO-15408: Kurs - Mozilla Firefox
Sicherheitsstandards und Common Criteria
Moodle-Kurs
1. Einführung
2. Ziel
3. Zusätzliche Informationen