Common Criteria und Schutzprofile - ISO-Standard für die Prüfung und Bewertung der Sicherheit von Informationstechnik

1 Einleitung

Internationale Standards sind für die Wirtschaft von außerordentlicher Bedeutung, weil sie den globalen Markt sicherstellen. Aber auch Verbraucher profitieren von der weltweiten Normung, weil erst die Vereinheitlichung von Produkten deren Vergleichbarkeit ermöglicht. Normen im Bereich der Informationstechnik sind besonders nützlich, weil der Computermarkt seit jeher ein Weltmarkt ist.

Für die Prüfung und Bewertung der Sicherheit von Informationstechnik IT gibt es seit dem 01.12.1999 den Internationalen Standard ISO/IEC 15408 "Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria, CC)".

Die CC entstanden in intensiver Zusammenarbeit der europäischen Länder Deutschland (BSI), Frankreich (DCSSI), Großbritannien (CESG) und der Niederlande (NLNCSA) mit Vertretern aus Kanada (CSE) und den USA (NIST und NSA). Sie harmonisieren die bis dahin von den beteiligten Organisationen erstellten Kriterien, also die europäischen ITSEC, die US-amerikanischen TCSEC und die kanadischen CTCPEC (Canadian Trusted Computer Product Evaluation Criteria).

Die CC sind jedoch mehr als nur eine Zusammenfassung ihrer zugrundeliegenden Kriterien.

Sie ermöglichen die detaillierte Spezifikation von Sicherheitsanforderungen in Form von Schutzprofilen oder Sicherheitsvorgaben. Schutzprofile dokumentieren aktuelle Sicherheitsprobleme, den passenden Lösungsansatz und daraus abgeleitete Anforderungen für einen bestimmten Produkttyp. Die Sicherheitsvorgaben schneidern Schutzprofile auf ein konkretes IT-Produkt zu. Sicherheitsvorgaben sind damit die obligatorische Grundlage jeder CC-Evaluation. Eine erfolgreiche Evaluation bestätigt, dass dem IT-Sicherheitsproblem durch das evaluierte Produkt in angemessener Weise vollständig begegnet wird.

Das erklärte Ziel der CC war, die weltweite gegenseitige Anerkennung von Evaluationsergebnissen zu ermöglichen.

Das Bundesministerium des Innern hat im Einvernehmen mit dem Bundesministerium für Wirtschaft die deutsche Übersetzung der CC Version 2.1 wie zuvor die Vorgängerversionen 1.0 und 2.0 am 29.09.2000 mit der Bekanntgabe im Bundesanzeiger in Deutschland eingeführt. Hersteller/Vertreiber von IT-Produkten und Bundesbehörden können beim Bundesamt für Sicherheit in der Informationstechnik (BSI) Sicherheitszertifikate auf Grundlage der CC beantragen und diese im internationalen Wettbewerb nutzen.

Die CC gliedern sich in folgende 3 Teile:

Teil 1: Einführung und Allgemeines Modell

Teil 2: Funktionale Sicherheitsanforderungen

Teil 3: Anforderungen an die Vertrauenswürdigkeit

2 Teil 1 der CC - Einführung und Allgemeines Modell

Evaluationsansatz der Common Criteria

Die Spezifikation der Sicherheitsfunktionalität wird vom Hersteller in dem Dokument Sicherheitsvorgaben beschrieben. Die CC enthalten 7 hierarchische Prüftiefen, - die Vertrauenswürdigkeitsstufen (Evaluation Assurance Level, EAL) - die durch weitere Prüfanforderungen ergänzt werden können.

Das zentrale Ziel jeder Evaluation ist die Herstellung des notwendigen Vertrauens. Die CC ahben das Ziel, Vertrauen in die Wirksamkeit der Sicherheitsfunktionalität eines IT-Produktes zu schaffen. Der Aufbau des vom Evaluator benötigten Produkt-Know-Hows wird durch das CC-Prüfverfahren so unterstützt, dass er nicht nur die funktional korrekte Implementierung sondern auch die Nicht-Ausnutzbarkeit von Schwachstellen bestätigen kann.

Die CC sind auf alle IT-Sicherheitsprodukte und -systeme anwendbar. Es kann Hardware und Software nach den CC evaluiert werden, wobei der Schwerpunkt bei der Software liegt.

Schutzprofile (Protection Profiles PP)

Mit dem Konstrukt der Schutzprofile richten sich die CC vornehmlich an den Anwender von IT und bieten ihm die Möglichkeit, entsprechend dem Schutzbedarf seiner Daten und Anwendungen seine gewünschten Sicherheitsanforderungen zu spezifizieren. Dieses Instrument der Schutzprofile ist für den Anwender von IT von ganz besonderer Bedeutung, kann er doch damit seine gewünschte IT-Sicherheit in Form von maßgeschneiderten IT-Sicherheitskonzepten darlegen und international bekanntgeben. Hersteller von IT haben die Möglichkeit, anwendergerechte IT-Sicherheitstechnik zu implementieren.

Aber auch Hersteller von IT können für Produktklassen Schutzprofile schreiben und damit quasi eine Standardisierung der Sicherheitsleistung für einzelne Produktgruppen schaffen.

Das Schutzprofilkonstrukt ist in den CC detailliert beschrieben und durch weitere Handbücher, die im Internet unter der BSI-Homepage www.bsi.bund.de und unter der internationalen CC-Homepage www.commoncriteria.org zum Download bereitstehen, praxisnah erläutert. Die grobe Struktur lässt sich kurz wie folgt skizzieren:

Das Schutzprofilkonstrukt beinhaltet in seinem ersten Teil das eigentliche Sicherheitskonzept zur Ermittlung des Sicherheitsbedarfs. Dieser Strukturteil ist in seiner inhaltlichen Ausgestaltung völlig frei und ermöglicht dem Schreiber des Schutzprofils, die Produktklasse aus Anwendersicht und seine reale bzw. angenommene Einsatzumgebung möglichst exakt zu beschreiben. Dabei soll die Beschreibung der Produktklasse dem Leser bereits ein Verständnis für die zu schützenden Werte vermitteln, etwa durch die Einordnung der zu verarbeitenden Daten in Forschungsergebnisse, Geschäftsdaten, personenbezogene Daten, Verschlussdaten im staatlichen Bereich usw. Die Annahmen zur Einsatzumgebung berücksichtigen insbesondere die Aspekte, die bereits zur Sicherheit der zu schützenden Werte beitragen. Dazu gehören räumliche Aspekte, Einschränkungen der Nutzung oder Ausbildungsstand der Anwender. Einzuhaltende Gesetze oder Regeln sowie die von der IT abzuwehrenden Bedrohungen vervollständigen die Darstellung des Sicherheitsbedarfs und ermöglichen die Ableitung der notwendigen Sicherheitsziele.

Die Vorgehensweise nach CC erzwingt vom Schreiber des Schutzprofils bereits bei der Ermittlung der Sicherheitsziele eine Vollständigkeitsanalyse zum Nachweis, dass die Sicherheitsziele ausreichend und notwendig sind, den ermittelten Sicherheitsbedarf vollständig zu erfüllen.

Die Sicherheitsziele können sich auf unterschiedlichste Techniken auswirken. Mit Hilfe der Kataloge der CC können die Anforderungen an die Sicherheitsfunktionalität und Vertrauenswürdigkeit durch Auswahl der passenden Komponenten beschrieben werden. Bei der Auswahl der Sicherheitsanforderungen ist man nicht an die CC gebunden. Man kann sie auch frei wählen, wann immer dies sinnvoll zu begründen ist. Vom PP-Verfasser wird wie bei den Sicherheitszielen eine Analyse der Vollständigkeit und Notwendigkeit aller Anforderungen verlangt. Aber auch die Analyse der Widerspruchsfreiheit und gegenseitigen Unterstützung der Anforderungen ist in einem eigenen Erklärungsteil zu leisten.

Mittels eigener Prüfkriterien der CC werden Schutzprofile von einer akkreditierten Prüfstelle evaluiert und erhalten von der jeweiligen nationalen Zertifizierungsstelle ein international anerkanntes Zertifikat bei erfolgreich abgeschlossener Prüfung.

Die Evaluierung von Schutzprofilen gibt den Herstellern die Sicherheit, dass das Schutzprofil ein sinnvolles, vollständiges und in sich widerspruchsfreies Pflichtenheft für die IT-Sicherheit ihres Produktes darstellt. Außerdem haben sie die Gewähr, dass durch die Auswahl der CC-Komponenten die Sicherheitsanforderungen einen angemessenen Präzisionsgrad zur Umsetzung der Sicherheitsleistung haben. Die internationale Akzeptanz der Schutzprofile eröffnet dem Hersteller für sein Produkt erweiterte Marktchancen.

Zur Zeit wird die Registrierung der zertifizierten Schutzprofile noch von nationalen Stellen wie dem BSI vorgenommen. Zertifizierte und registrierte Schutzprofile werden international anerkannt. Auf den Websites der am CC-Projekt beteiligten Organisationen finden sich bereits verschiedenste Schutzprofile sowie weitere Hinweise zum allgemeinen Themenkomplex.

Durch ein ISO-Registrierungsverfahren soll die weltweite Anerkennung von Schutzprofilen gewährleistet werden. Es gibt bereits eine nationale Normungsorganisation, die bereit ist, das internationale Register zu führen. Eine für Deutschland wichtige Entscheidung ist bereits durch die Festlegung getroffen, dass auch in nichtoffiziellen Sprachen der ISO wie Deutsch erstellte Schutzprofile registriert werden können.

Sicherheitsvorgaben (Security Target ST)

Möchte ein IT-Hersteller für sein Produkt ein Sicherheitszertifikat nach CC, so muss er die Sicherheitsleistung seines Produktes mit dem als Sicherheitsvorgaben bezeichneten Dokument beschreiben. Die Struktur dieses Dokumentes setzt auf dem Schutzprofilkonstrukt auf und ist insbesondere um die Aspekte der konkreten Umsetzung erweitert.

Wenn der Hersteller auf ein Schutzprofil zurückgreifen kann, erleichtert dies ihm den Aufwand zur Erstellung seiner Sicherheitsvorgaben erheblich. Liegt für das Produkt kein passendes Schutzprofil vor, so können die Sicherheitsvorgaben direkt und auf ganz ähnliche Weise wie beim Schutzprofil formuliert werden, ohne dass vorher ein Schutzprofil erstellt werden muss.

Analog zur Vorgehensweise bei den Schutzprofilen werden mittels eigener Prüfkriterien der CC die Sicherheitsvorgaben von einer akkreditierten Prüfstelle evaluiert und die Ergebnisse in einem

Prüfbericht festgehalten. Erst nach Akzeptanz des Prüfberichtes durch die nationale Zertifizierungsstelle ist die Evaluation der Sicherheitsvorgaben erfolgreich abgeschlossen. Nun können alle Beteiligten am Evaluierungsverfahren das Vertrauen in die zur erfolgreichen Durchführung der Evaluation notwendige Qualität der Sicherheitsvorgaben haben.

Bei der Auswahl der Sicherheitsanforderungen in den Sicherheitsvorgaben ist man wie bei Schutzprofilen nicht an die CC gebunden. Man kann sie frei wählen, wann immer dies sinnvoll zu begründen ist.

3 Teil 2 der CC - Katalog funktionaler Sicherheitsanforderungen

Der Teil 2 der CC enthält einen umfangreichen Katalog bausteinartiger Funktionalitätsanforderungen in komponentenstruktur. Er erleichtert die korrekte Erstellung von Schutzprofilen und Sicherheitsvorgaben. Die Sicherheitsanforderungen sind so vorgegeben, dass deren Verwendung die Evaluierbarkeit der Sicherheitsvorgaben garantiert. Die CC sind aber offen für weitere frei definierte funktionale Sicherheitsanforderungen, falls für die geforderte Sicherheitsfunktionalität keine passenden Komponenten gefunden werden.

Eine einfache Struktur der Kataloge ermöglicht dem Leser der CC, die passenden Anforderungen leicht zu finden.

Viele Komponenten nehmen Einfluss auf die Auswahl anderer Komponenten, indem sie das Vorhandensein einer bestimmten Funktionalität verlangen. Diese sind durch Abhängigkeitslisten dargestellt und müssen bei der Auswahl der Komponenten berücksichtigt werden.

Auch wird bei Auswahl einzelner Komponenten auf interessante zu protokollierende Ereignisse hingewiesen, beispielsweise die Eingabe eines falschen Passwortes bei der Authentisierung. Die möglichen protokollierbaren Ereignisse werden in der hierarchischen Form minimale, einfache und detaillierte Protokollierung angeboten.

Außerdem werden die für eine Komponente möglichen Adminstrationsaspekte angeführt, beispielsweise die Einstellbarkeit von Passworteigenschaften. Diese Hinweise unterstützen den Schreiber von Schutzprofilen und Sicherheitsvorgaben in seinen Überlegungen, alle erforderlichen Aspekte zu berücksichtigen.

Zur individuellen Anpassung der ausgewählten Sicherheitsanforderungen werden verschiedene Operationen angeboten. Es kann z.B. produktabhängig *ausgewählt* werden, ob eine Sicherheitsfunktion gegen unbefugte Veränderungen von Daten, gegen deren unbefugte Weitergabe oder gegen beides schützen soll. Vorher müsste z.B. der Name der Funktion *zugewiesen* werden. Eine *Verfeinerung* könnte darin bestehen, eine bestimmte Art der Implementierung für diese Funktion zu fordern, z.B. dass sie hardwaremäßig vor dem Überschreiben geschützt sein muss. Als weitere Operation wird die *Iteration* definiert, die es ermöglicht, eine Komponente mehrfach auszuwählen, z.B. für verschiedene Domänen des EVG.

4 Teil 3 der CC - Sicherheitsanforderungen zur Vertrauenswürdigkeit

Die im Teil 3 der CC katalogisierten Sicherheitsanforderungen an die Vertrauenswürdigkeit ermöglichen erst die Vergleichbarkeit der Evaluierungsergebnisse. Auch der teil 3 erhebt keinen

Anspruch auf Vollständigkeit und lässt unter Berücksichtigung der Komponenteneigenschaften der CC-Kriterien die Definition weiterer Anforderungen zu.

Der wichtigsten Themen zu Anforderungen an die Vertrauenswürdigkeit werden im Folgenden kurz umrissen.

Ein wesentlicher Anteil der Evaluierungsarbeit beansprucht die Evaluierung des Entwicklungsprozesses. Mit Hilfe der Entwicklungsdokumentation baut der Evaluator seine Produktkenntnisse in der geforderten Tiefe auf und muss den Nachweis leisten, dass die vorgelegten Dokumente alle Korrektheits- und Vollständigkeitsanforderungen der CC erfüllen. Dabei wird ein vierstufiger Entwicklungsprozess angenommen - Spezifikation der Anforderungen, des Architekturentwurfs, des Feinentwurf und der Implementierung,

Die Schwachstellenbewertung ist das zentrale Ziel der Evaluation und kann erst durchgeführt werden, wenn ausreichend tiefe Kenntnis über das Produkt aufgebaut wurde. Sie enthält u.a. die Aspekte Stärke der Funktionen und Ausnutzbarkeit von Schwachstellen. Beide Aspekte können mit „niedrig“, „mittel“ oder „hoch“ bewertet werden, was als Maß für den Aufwand zur Überwindung einer Schwachstelle oder einer Sicherheitsfunktion steht. Aber auch detaillierte Anforderungen an die durchzuführenden Tests, eine Vereinfachung des Produktdesigns, qualitative Anforderungen an die Spezifikationsform der Dokumente bis hin zu Anforderungen an die Entwicklungslabors, das Auslieferungsverfahren und die Inbetriebnahme des Produktes gehören dazu.

Das sinnvolle und abgestimmte Zusammenfügen von Vertrauenswürdigkeitskomponenten ist nicht trivial und wird durch sieben hierarchisch strukturierte Pakete an unterschiedliche Prüftiefen, den Vertrauenswürdigkeitsstufen (EAL1 bis EAL7), erleichtert.

Das Hinzufügen weiterer Anforderungen zu einer EAL-Stufe ist möglich und kann besonders zum Ausdruck gebracht werden. Damit soll dem Hersteller eine Möglichkeit gegeben werden, seine besonderen Anstrengungen zur Verbesserung der Vertrauenswürdigkeit hervorzuheben.

5 Fehlerbehebung und Erhaltung der Vertrauenswürdigkeit

Im Rahmen der Evaluierung und Zertifizierung kann das Problem entstehen, dass nach der Zertifizierung eines Produkts - bedingt durch einen kurzen Produktzyklus oder aufgrund korrigierter Fehler - eine neue Version des Produkts auf den Markt kommt, für die das Zertifikat keine Gültigkeit mehr besitzt. Zur Lösung dieses Problems bieten die CC verschiedene Möglichkeiten an.

Die formale Re-Zertifizierung

Die Re-Zertifizierung gibt dem Hersteller die Möglichkeit, in einem stark verkürzten Verfahren, in dem nur die sicherheitsrelevanten Änderungen des Produkts geprüft werden, das Zertifikat für ein schon zertifiziertes Produkt auf eine neue Version übertragen zu lassen. Diese Möglichkeit wurde in Deutschland schon häufig genutzt. Im Rahmen der Einführung der CC wurden bereits Re-Zertifizierungen nach CC auf der Basis von ITSEC Zertifikaten durchgeführt. Dies zeigt im übrigen auch die Kompatibilität der beiden Kriterienwerke.

Die Familie Fehlerbehebung

Diese Familie behandelt Verfahren und Prozeduren des Entwicklers, die sicherstellen, dass entdeckte Sicherheitsfehler aufgezeichnet und korrigiert werden. Auch wenn zum Zeitpunkt der Evaluation die zukünftige Befolgung der Fehlerbehebungsprozeduren nicht festgestellt werden kann, besteht die Möglichkeit, die vom Entwickler dargelegten Prozeduren zu prüfen. Eine formale Re-Zertifizierung kann somit vermieden werden.

Die Klasse Erhaltung der Vertrauenswürdigkeit

Diese Klasse erhält Anforderungen, die sicherstellen sollen, dass der Evaluationsgegenstand seine Sicherheitsvorgaben nach Änderungen an demselben oder seiner Umgebung weiterhin einhält. Solche Änderungen schließen die Entdeckung neuer Bedrohungen oder Schwachstellen sowie die Korrektur von gefundenen Fehlern ein. Die Benutzung dieser Klasse muss jedoch mit der jeweiligen Zertifizierungsstelle näher geregelt werden.

6 Gemeinsame Evaluationsmethodologie (Common Evaluation Methodology CEM)

Das vorrangige Ziel der internationalen Harmonisierung von IT-Sicherheitskriterien ist die formale gegenseitige Anerkennung von Evaluationsergebnissen. Die Erarbeitung einer gemeinsamen Evaluationsmethodologie (Common Methodology for Information Technology Security Evaluation, CEM) stellt sicher, dass von den beteiligten Stellen die Kriterien in gleicher Weise angewendet werden. Dadurch ist es möglich, ausreichendes Vertrauen in die Evaluationsergebnisse anderer Stellen zu haben. Die zur Zeit gültige Version 1.0 des Teils 2 der CEM beschreibt die Methodology für die Evaluation von Schutzprofilen, Sicherheitsvorgaben und IT-Produkten bis zu EAL4.

Bei der Entwicklung der CEM geht es um die Schaffung eines gemeinsamen Konzepts und einer abgestimmten Methodik für die Durchführung von Evaluationen auf Basis der CC. Dabei beschreiben die Kriterien *was* evaluiert und die Methodologie *wie* evaluiert werden soll. Richten sich die Kriterien in erster Linie an den Hersteller/Antragsteller (denn sein Evaluationsgegenstand muss die Kriterien erfüllen), so ist die Methodologie primär an den Evaluator adressiert (denn sie beschreibt, wie evaluiert werden soll). Natürlich enthalten beide Werke Aspekte, die für alle Beteiligten an einer Evaluation in gleichem Maße relevant sind.

Bezugsadressen:

Die CC und CEM können von verschiedenen Servern und Mail-Boxen abgerufen werden. . Das BSI bietet Informationen zu den CC unter http://www.bsi.bund.de/cc/ .

Die umfassendsten Informationen zum gesamten Common Criteria Projekt sind in Englisch unter http://www.commoncriteria.org vorhanden. Im CC Teil 1, Anhang A sind ausführliche Adressinformationen der beteiligten Organisationen abgedruckt.