

IT - Evaluationshandbuch

Handbuch für die Prüfung der Sicherheit von Systemen der Informationstechnik (IT)

1. Fassung vom 22. Februar 1990

herausgegeben von der

ZSI - Zentralstelle für Sicherheit in der Informationstechnik

im Auftrag der Bundesregierung

Bundesanzeiger

Vorwort

Als "Meßlatte" zur Beurteilung der Sicherheit informationstechnischer Systeme hat die Zentralstelle für Sicherheit in der Informationstechnik (ZSI) unter Beteiligung von Wirtschaft und Wissenschaft die "IT-Sicherheitskriterien" im Auftrag der Bundesregierung erarbeitet und am 1. Juni 1989 veröffentlicht.

Das vorliegende "IT-Evaluationshandbuch" baut auf den "IT-Sicherheitskriterien" auf. Es wurde ebenfalls unter Beteiligung von Wirtschaft und Wissenschaft erarbeitet und beschreibt, wie informationstechnische Systeme oder selbständige Komponenten nach diesen Kriterien geprüft werden. Es soll insbesondere die Gleichbehandlung der Hersteller sowie ihrer zu prüfenden Produkte gewährleisten.

Die ZSI wird Sicherheitszertifikate erst vergeben, nachdem ihre Aufgaben wie vorgesehen gesetzlich geregelt sind. Übergangsweise wird sie sich darauf beschränken, solche Produkte zu prüfen, für die eine Bundesbehörde einen Bedarf angemeldet hat. Dessen ungeachtet wird die ZSI Kriterien, Verfahren, Werkzeuge und formale Hilfsmittel für die Prüfung und Bewertung der Sicherheit von Systemen bzw. Komponenten der Informationstechnik entwickeln.

Außer der durch Gesetz zu regelnden Vergabe von Sicherheitszertifikaten durch die ZSI sind auch einige andere Fragestellungen im "IT-Evaluationshandbuch" zur Zeit noch nicht abschließend geklärt. So gibt es derzeit noch keine einsatzfähigen und von der ZSI zugelassenen formalen Hilfsmittel, um allen in Kapitel 3 dieses Handbuchs spezifizierten Forderungen zu entsprechen. Erste Entwicklungsergebnisse lassen es jedoch als sicher erscheinen, daß diese Hilfsmittel in absehbarer Zeit vorliegen.

Der Forderung, die "IT-Sicherheitskriterien" auf Kriterienkataloge anderer Nationen abzubilden, wird besondere Bedeutung beigemessen. Die ZSI betreibt mit Nachdruck die notwendigen Aktivitäten zur Harmonisierung der Sicherheitskriterien und der gegenseitigen Anerkennung der Prüfergebnisse.

Das "IT-Evaluationshandbuch" hat deshalb in dieser 1. Fassung teilweise vorläufigen Charakter. Es wird ebenso wie die "IT-Sicherheitskriterien" nach Bedarf fortgeschrieben werden, um neue Erkenntnisse und praktische Erfahrungen aus Evaluationen einzubeziehen.

Neben den "IT-Sicherheitskriterien" und dem "IT-Evaluationshandbuch" wird ein "IT-Sicherheitshandbuch" (Handbuch für sichere Anwendung der Informationstechnik) erarbeitet. Diese drei Handbücher bilden die "Standardwerke zur IT-Sicherheit". Sie stellen umfassende Informationen zur Ermittlung des Sicherheitsbedarfs bereit und ermöglichen die Planung und Realisierung der daraus abgeleiteten Sicherheitsmaßnahmen.

Dr. Leiberich

Leiter der Zentralstelle für Sicherheit in der Informationstechnik

Zusammenfassung

Das hier vorgelegte IT-Evaluationshandbuch ist Bestandteil der Standardwerke zur IT-Sicherheit. Es enthält eine Vielzahl von Aussagen und Hinweisen, die sich mit organisatorischen Fragen im gesamten Umfeld einer Evaluation befassen.

Das IT-Evaluationshandbuch besteht aus 12 Kapiteln. Die ersten vier Kapitel orientieren sich an den IT-Sicherheitskriterien ^{<1>}, die restlichen Kapitel enthalten eigenständige Aussagen zum Umfeld und Ablauf einer Evaluation.

Kapitel 1 enthält mehrere detaillierte Beispiele, die eine Einführung geben, wie Mechanismen, die für einzelne Grundfunktionen vorgeschlagen werden, bewertet werden. Dieser Bewertungsvorgang muß für jeden Mechanismus einer Grundfunktion durchgeführt werden.

Kapitel 2 gibt Erläuterungen zu den einzelnen Funktionalitätsklassen und weist besonders darauf hin, daß die Anzahl der Funktionalitätsklassen nicht auf die in den IT-Sicherheitskriterien beschriebenen beschränkt ist.

Kapitel 3 gibt detaillierte Erläuterungen zu den einzelnen Punkten jeder Qualitätsstufe. Dieses Kapitel muß immer im Zusammenhang mit dem Kapitel Qualitätsstufen der IT-Sicherheitskriterien gelesen werden.

Kapitel 4 enthält detaillierte Ausführungen zum Inhalt und Umfang der bei einer Evaluation vorzulegenden Dokumentation am Beispiel der Qualitätsstufen Q1 - Q3.

Kapitel 5 gibt Erläuterungen zum Qualitätsaspekt "Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen". Es wird beschrieben, warum die Abgrenzungsmechanismen bei einer Evaluation mit evaluiert werden müssen. Dies wird durch Beispiele für Abgrenzungsmechanismen verdeutlicht.

Kapitel 6 beschreibt das Evaluationsumfeld. Nach der Verabschiedung des BSI-Errichtungsgesetzes werden hier rechtliche und organisatorische Rahmenbedingungen festgelegt werden.

Die jetzt folgenden Kapitel 7 bis 12 beziehen sich auf den Evaluationsvorgang.

<1> IT-Sicherheitskriterien: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)
Herausgegeben von der Zentralstelle für Sicherheit in der Informationstechnik im Auftrag der Bundesregierung.

Kapitel 7 beschreibt den Ablauf einer Evaluation. Die einzelnen Unterkapitel beschreiben einen möglichen organisatorischen Aufbau des Evaluations-Teams. Darauf folgt eine Ausarbeitung zum Reviewprozeß. Dies ist der vorgeschlagene Weg, um während der Evaluation zu tragfähigen Einzel- und Gesamtentscheidungen zu gelangen. Das nächste Unterkapitel zeigt die Vorarbeiten auf, die notwendig sind, wenn entweder ein Hersteller oder ein Anwender eine Evaluation bei einer Evaluationsstelle starten will. Es folgt ein detaillierter Vorschlag in fünf Phasen mit jeweils mehreren Stufen, der den Ablauf einer Evaluation und die dabei zu bewältigenden Aufgaben beschreibt. Daran anschließend wird eine mögliche Vorgehensweise bei einer Teilevaluation vorgestellt. Am Ende der Evaluation steht die Ausstellung des Zertifikates, welches in seinem inhaltlichen Aufbau beschrieben wird. Das Kapitel schließt mit Hinweisen auf die Konsequenzen, die sich für einen Hersteller ergeben, wenn er ein evaluiertes Produkt vertreibt.

Kapitel 8 beschreibt die Besonderheiten von begleitenden Evaluationen.

Kapitel 9 erläutert, wann eine Reevaluation notwendig wird. Dafür werden vier Regeln aufgestellt und an Beispielen ihre Anwendung und die sich für das Zertifikat ergebenden Konsequenzen aufgezeigt.

Kapitel 10 behandelt die Evaluation von IT-Systemen, die bereits evaluierte Komponenten enthalten. Hier werden die Erkenntnisse aus der ersten Evaluation eines solchen Systems noch starken Einfluß auf die Einzelformulierungen haben. Es ist jedoch sicher, daß ein Zusammenschalten von gleichbewerteten Einzelkomponenten nicht unbedingt dieselbe Qualitätsstufe ergibt.

Kapitel 11 beschreibt den Aufbau einer Werkzeuge- und Methodenliste, die für die Hersteller von IT-Systemen der höheren Qualitätsstufen unbedingt notwendig ist. Es ist verständlich, daß die Evaluationsbehörde nur eine kleine Anzahl ihr bekannter Werkzeuge und Methoden unterstützen kann.

Kapitel 12 beinhaltet die Abbildung auf andere Kriterienkataloge. Dies wird exemplarisch dargestellt durch die Abbildung auf die Klassen der "Trusted Computer System Evaluation Criteria" des amerikanischen Verteidigungsministeriums.

Es schließt sich ein Glossar der wichtigsten im IT-Evaluationshandbuch verwendeten Begriffe an.

Die vorliegende Ausgabe (1. Fassung vom 22. Februar 1990) des IT-Evaluationshandbuches wird infolge der ständig fortschreitenden Entwicklung auf dem informationstechnischen Sektor und den Erfahrungen bei Evaluationen laufender Überarbeitung bedürfen. Der Herausgeber ist daher jederzeit an Verbesserungsvorschlägen und konstruktiven Anregungen interessiert.

Inhaltsverzeichnis

Vorwort	i
Zusammenfassung	iii
Inhaltsverzeichnis	1
1. Erläuterungen zur Bewertung von Mechanismen	3
2. Erläuterungen zu den Funktionalitätsklassen	23
3. Erläuterungen zu den Qualitätskriterien	26
Qualitätsstufe Q1	27
Qualitätsstufe Q2	30
Qualitätsstufe Q3	34
Qualitätsstufe Q4	38
Qualitätsstufe Q5	42
Qualitätsstufe Q6	47
Qualitätsstufe Q7	51
4. Erläuterungen zu den geforderten Dokumenten	54
4.1 Beschreibung der Sicherheitsanforderungen	55
4.2 Spezifikation der zu evaluierenden Systemteile	56
4.3 Beschreibung der Abgrenzung zu den nicht zu evaluierenden Systemteilen und der Schnittstellen zu diesen Teilen	61
4.4 Dokumentation für den Anwender	61
4.5 Beschreibung der verwendeten Hard- und Firmware mit Darlegung der Funktionalität der in Hard- bzw. Firmware realisierten Schutzfunktionen	62
4.6 Testdokumentation	63

5. Erläuterungen zur Abgrenzung	64
6. Evaluationsumfeld	67
7. Beschreibung des Evaluationsprozesses	68
7.1 Organisatorischer Aufbau des Evaluations-Teams	68
7.2 Der Reviewprozeß	70
7.3 Starten einer Evaluation	72
7.4 Ablauf einer Evaluation	74
7.5 Bewertungsschritte bei einer Teilevaluation	80
7.6 Das Zertifikat	81
7.7 Konsequenzen für den Hersteller	83
8. Begleitende Evaluation	84
9. Reevaluation	86
10. Evaluation von IT-Systemen, die bereits evaluierte Komponenten enthalten	91
11. Werkzeuge und Methoden	93
12. Abbildung auf andere Kriterienkataloge	94
Glossar	97

1. Bewertung von Mechanismen

Die an ein IT-System gestellten Sicherheitsanforderungen werden durch Sicherheitsfunktionen erfüllt. Mechanismen sind diejenigen Methoden und Verfahren, mit denen diese Sicherheitsfunktionen in einem System realisiert werden. Die Bewertung der Mechanismen ist ein wesentlicher Teil der Evaluation eines Systems. Somit ist es das Ziel, zu untersuchen, ob die verwendeten Mechanismen in der Lage sind, die zu erfüllenden Sicherheitsanforderungen mit ausreichender Stärke abzudecken. Kapitel 4 der IT-Sicherheitskriterien beschreibt für jede Grundfunktion mögliche Schwächen der Mechanismen und ist Ausgangspunkt für die Bewertung. Bei der Bewertung soll unter Einbeziehung aller, auch der auf dem detailliertesten Spezifikationslevel erkennbaren Details der Realisierung sowie mit Hilfe spezieller Tests nach Schwächen gesucht werden. Schwächen liegen dann vor, wenn die Wirksamkeit eines Mechanismus unter Berücksichtigung seiner Einbettung in das System entweder generell oder in bestimmten Situationen eingeschränkt ist.

Können bestimmte Details, die zur Bewertung der Mechanismen notwendig sind, nicht aus der Spezifikation abgeleitet werden, so müssen sie durch Tests geklärt werden. Aufgabe der Tests ist dabei nicht die Suche nach Implementierungsfehlern, sondern sie sollen helfen, solche Details der Mechanismen zu klären, die nicht aus der Spezifikation erkennbar sind.

Werden Schwächen gefunden, so kann eine Abwertung des Mechanismus erfolgen. Ob eine Abwertung erfolgen muß, hängt davon ab, welche Auswirkungen diese Schwächen auf die Erfüllung der Sicherheitsanforderungen an das Gesamtsystem besitzen.

Ein Mechanismus muß nicht abgewertet werden, wenn eine (oder mehrere) seiner Schwächen durch andere Mechanismen in der Weise kompensiert werden, daß durch die Kombination dieser Mechanismen die Sicherheitsanforderungen in allen denkbaren Situationen erfüllt werden. Deshalb kann es auch durchaus vorkommen, daß ein und derselbe Mechanismus in zwei unterschiedlichen Systemen mit unterschiedlichen Sicherheitsanforderungen auch unterschiedlich bewertet wird.

Die Untersuchung der einzelnen Mechanismen kann zwar in einer ersten Stufe noch unabhängig von anderen verwendeten Mechanismen und auch unabhängig von den konkreten Sicherheitsanforderungen erfolgen, vor einer endgültigen Bewertung des Mechanismus im jeweiligen System müssen jedoch die Auswirkungen der Schwächen auf die Einhaltung der Sicherheitsanforderungen analysiert werden, wobei eine eventuelle Kompensation durch andere Mechanismen berücksichtigt werden muß.

Die Bewertung eines Mechanismus bei gefundenen Schwächen hängt dann davon ab, welche Kenntnisse und welcher Aufwand zur Ausnutzung seiner Schwächen erforderlich ist und wie die Bedrohung durch die Ausnutzung der Schwächen einzuschätzen ist. Da diese Bedrohung im allgemeinen nicht objektiv meßbar ist und auch von der konkreten Einsatzumgebung abhängt, muß das Evaluations-Team in Einzelfällen relativ subjektiv bewerten.

Das Zusammenwirken mehrerer Schwächen kann zu einer stärkeren Abwertung führen, als dies nach der Einzelbewertung der Schwächen erforderlich erscheint. Keinesfalls kann ein Mechanismus höher eingestuft werden als die schwächste Einzelbewertung.

Die Bewertungsergebnisse früherer Evaluationen können bei späteren Evaluationen nicht ungeprüft übernommen werden, weil sich eine Bewertung durch neue technische Entwicklungen ändern kann. So kann z.B. die Ausnutzung einer Schwäche heute noch einen relativ hohen technischen Aufwand erfordern, in Zukunft aber mit deutlich weniger Aufwand möglich sein.

Bei den folgenden Beispielen werden einige Mechanismen grob skizziert und ihre Schwächen aufgezeigt. Es wird nicht erläutert, wie die Schwächen gefunden wurden, sondern es wird angenommen, daß diese Schwächen entweder aus der Systemspezifikation erkennbar waren oder durch Tests gefunden wurden. Sinn der Beispiele ist es, den Vorgang der Bewertung von Mechanismen zu erläutern, wobei die meisten der ausgewählten Beispiele zwar an Mechanismen aus realen Systemen angelehnt sind, jedoch im allgemeinen stark vereinfacht wurden. Auch werden nur sehr wenige Annahmen über die Sicherheitsanforderungen gemacht. Deshalb können die Ergebnisse dieser Beispielbewertungen bei einer Evaluation in der Regel nicht direkt übernommen werden.

Beispiele zur Bewertung von Mechanismen

Grundfunktion Identifikation und Authentisierung

Beispiel: Identifikation und Authentisierung von Benutzern durch eine Kombination von Benutzererkennung und Paßwort

Inhärente Schwächen des Mechanismus

Paßwörter können außerhalb des Systems weitergegeben werden.

Paßwörter werden häufig so gewählt, daß sie leicht erraten oder bestimmt werden können.

Bewertung wegen dieser Schwächen:

Die Kombination Benutzererkennung und Paßwort kann wegen dieser Schwächen maximal als "sehr starker" Mechanismus bewertet werden.

Bewertung der Eindeutigkeit einer Identität:

Hier ist zu prüfen, ob vom IT-System die Eindeutigkeit erzwungen wird, d.h. ob eine Benutzererkennung nur einmal vergeben werden kann.

Falls nicht, dann ist die Bewertung abhängig von der Zahl der möglichen Benutzerkennungen und der notwendigen organisatorischen Maßnahmen sowie deren Dokumentation in den entsprechenden Handbüchern. Dies ist ein Beispiel für eine Schwachstelle, deren Auswirkungen nur ein Betreiber für sein konkretes System bewerten kann. Die Bewertung hängt von der Zahl der Benutzer in seinem System ab, d.h. der Betreiber muß selbst entscheiden, ob diese Zahl so klein ist, daß die organisatorischen Maßnahmen zur Erzwingung der Eindeutigkeit für sein System ausreichend sind. Ziel der Evaluation kann in diesem Fall nur sein, ihn auf diese Schwachstelle hinzuweisen.

Für die in den Kriterien aufgeführten drei Bedrohungen bei einer Authentisierung durch Wissen ist bei dem Mechanismus der Identifikation und Authentisierung von Benutzern durch eine Kombination von Benutzererkennung und Paßwort zu untersuchen:

- ob und mit welchem Aufwand ein Paßwort bei der Eingabe ausgespäht werden kann,
- ob und mit welchem Aufwand ein sogenanntes "Spoofing"-Programm erstellt werden kann, durch das ein Benutzer zur unfreiwilligen Preisgabe seines Paßwortes verleitet werden kann,

- wie und wo Paßworte im System gespeichert werden, wie der Zugriff zu diesen Bereichen geregelt ist und wie groß der Aufwand für ein "Trojanisches Pferd" ist, an Paßworte zu gelangen und diese an Unbefugte weiterzugeben.

Entsprechend der Relevanz dieser Bedrohungen ist der Mechanismus zur Identifikation und Authentisierung von Benutzern durch eine Kombination von Benutzererkennung und Paßwort zu bewerten.

Der folgende Passus soll zeigen, wie die Bewertung des Mechanismus zur Identifikation und Authentisierung von Benutzern im Evaluationsbericht einer solchen Implementierung aussehen könnte.

Beschreibung des Mechanismus

Es wird eine Kombination von Benutzererkennung und Paßwort zur Identifikation und Authentisierung von Benutzern verwendet. Paßworte sind maximal 8 Zeichen lang, wobei jedes Zeichen aus einem weiten Bereich des ASCII-Alphabets stammen kann. Der Paßwortraum ist daher sehr groß (mehr als 10^{17} Möglichkeiten). Paßworte werden intern nur in verschlüsselter Form abgespeichert. Dabei wird eine Einwegverschlüsselung verwendet. Die Stärke des Verschlüsselungsalgorithmus ist nicht untersucht worden.

Von dem Mechanismus abzudeckende Sicherheitsanforderungen

Durch den Mechanismus sollen Benutzer eindeutig identifiziert und authentisiert werden. Die Authentisierungsinformationen sollen vor unberechtigten Zugriffen und unbefugter Kenntnisnahme geschützt sein.

Bewertung der inhärenten Schwächen des Mechanismus

Wegen inhärenter Schwächen des Mechanismus (bewußte oder unbewußte Weitergabe von Paßworten, falsche Wahl von Paßworten) kann der Mechanismus maximal mit "sehr stark" bewertet werden.

Bewertung anhand der Kriterien

1. Erzwingung der Eindeutigkeit einer Identität ist nicht gegeben.

====> leichte Abwertung

Begründung:

Die möglichen Auswirkungen dieser Bedrohung hängen sehr stark von der Einsatzart des Systems und der Zahl der Benutzer ab.

2. Das Paßwort wird bei der Eingabe nicht am Bildschirm angezeigt und (im Normalfall) auch nicht im lokalen Bildschirmspeicher zwischengespeichert. Allerdings kann es vorkommen, daß ein unachtsamer Benutzer sein Paßwort bereits eingibt, bevor die Aufforderung dazu erscheint. In diesem Fall wird dann der eingegebene Text am Bildschirm angezeigt. Dies wird jedoch nur als eine minimale Bedrohung aufgefaßt.

====> keine Abwertung

Begründung:

Die Bedrohung kann durch Unterrichtung der Benutzer verringert werden. Es ist nicht möglich, diese Schwachstelle gezielt auszunutzen.

3. Ein "Spoofing"-Programm ist sehr einfach zu erstellen und wird vom Benutzer kaum bemerkt. Zur Erstellung eines solchen Programms werden keine besonderen Systemkenntnisse benötigt.

====> starke Abwertung, der Mechanismus kann wegen dieser Schwachstelle noch maximal mit "mittelstark" bewertet werden.

Begründung:

Ein böswilliger Benutzer benötigt keine besonderen Kenntnisse oder Hilfsmittel zur Erstellung eines solchen "Spoofing"-Programms. Gutwillige Benutzer können sich gegen eine Bedrohung durch diese Schwachstelle kaum schützen. Daher ist nach den Kriterien zur Bewertung von Mechanismen maximal noch eine Bewertung "mittelstark" möglich.

4. Paßworte werden zwar verschlüsselt abgespeichert, jedoch in einer Datei, die für alle Benutzer lesbar ist. Da der Verschlüsselungsalgorithmus bekannt ist, kann praktisch jeder Benutzer die verschlüsselten Paßworte lesen, auf einen anderen Rechner bringen und dort versuchen, die Paßworte zu entschlüsseln, notfalls indem er bestimmte Worte nimmt, sie verschlüsselt und vergleicht, ob das so verschlüsselte Wort in der Paßwortdatei enthalten ist. Allerdings ist der Paßwortraum sehr groß (mehr als 10^{17} mögliche Paßworte). Trotzdem ist dieser Schutz der Paßworte im System als unzureichend zu betrachten.

====> Abwertung, der Mechanismus kann wegen dieser Schwachstelle noch maximal mit "stark" bewertet werden.

Begründung:

Bei dieser Art von Schutz der Paßworte ist folgende Attacke möglich: Es werden Paßworte ausgewählt, verschlüsselt und geprüft, ob der Schlüsseltext in der Paßwortdatei vorkommt. Zu dieser Attacke werden Kenntnisse des Systems (des Verschlüsselungsalgorithmus) benötigt und es ist für einen Erfolg ein relativ großer Rechenaufwand nötig, um eine geeignet große Menge von Paßworten durchzuprüfen. Ein gutwilliger Benutzer kann sich gegen eine Bedrohung durch diese Schwachstelle durch die Wahl eines geeigneten Paßwortes relativ gut schützen.

Bewertung des Mechanismus

Insgesamt kann der verwendete Mechanismus zur Identifikation und Authentisierung von Benutzern nur als "**mittelstark**" bewertet werden, da er mit mittelgroßem Aufwand von Personen mit normalen Systemkenntnissen zu überwinden ist.

Auswirkung auf die Gesamtbewertung des Systems:

Identifikation und Authentisierung von Benutzern ist ein wichtiger Aspekt der Sicherheitsanforderungen des Systems. Wegen der Bewertung des Mechanismus zur Identifikation und Authentisierung von Benutzern kann das System **maximal noch die Qualitätsstufe Q2** erreichen.

Beispiel: Identifikation und Authentisierung mittels eines maschinenlesbaren Ausweises und einer persönlichen Kennziffer, die nicht frei wählbar ist. Der Ausweis sei nur mit sehr großem Aufwand zu fälschen.

Inhärente Schwächen des Mechanismus:

Kennziffern können außerhalb des Systems weitergegeben werden.

Ausweise können außerhalb des Systems an Unbefugte gelangen.

Beide Bedingungen müssen gleichzeitig eintreten, um die Bedrohung der falschen Identifikation und Authentisierung wirksam werden zu lassen. Der Mechanismus kann wegen dieser Schwachstelle nicht besser als mit "sehr stark" bewertet werden.

Beschreibung des Mechanismus

Jeder Ausweis trägt ein eindeutiges Identifikationskennzeichen. Dieses ist maschinell lesbar. Die Kennziffer bestehe aus genau 4 Dezimalziffern. Damit ergibt sich ein Paßwortraum von 10000 möglichen Kennziffern. Die Anzahl der erlaubten Identifikationsversuche ist auf 3 begrenzt. Die Kennziffer wird vorgegeben, ist also nicht vom Benutzer frei wählbar.

Von dem Mechanismus abzudeckende Sicherheitsanforderungen

Der Mechanismus soll Benutzer identifizieren und authentisieren. Authentisierungsinformationen sind vor unbefugter Kenntnisnahme zu schützen. Der Ausweis ist gegen Fälschung und unbefugte Manipulationen zu schützen.

Bewertung anhand der Kriterien

Jeder Ausweis ist eindeutig identifizierbar. Somit ist die Eindeutigkeit gegeben. Ein Gutachten bestätigt, daß die Herstellung eines falschen Ausweises nur mit sehr hohem Aufwand möglich ist. (**Hinweis:** Die Evaluationsstelle kann dies nicht nachprüfen, sie kann aber die Vorlage eines Gutachtens einer unabhängigen Instanz verlangen, in dem diese Fragen geklärt werden.).

Da der Raum der möglichen Kennziffern auf 10000 beschränkt ist, ergibt sich die Wahrscheinlichkeit einer falschen Identifikation durch Ausprobieren von Kennziffern ungefähr zu 3/10000. Der Ausweis kann auch leicht gestohlen werden. Wegen dieser Schwachstelle kann der Mechanismus daher noch maximal mit "mittelstark" bewertet werden.

Untersuchungen ergaben, daß sich durch relativ einfache Manipulationen an dem Ausweis die Zahl der möglichen Fehlversuche bei der Identifikation und Authentisierung beliebig steigern läßt. Dies führt zu einer weiteren Abwertung.

Bewertung des Mechanismus

Wegen der gefundenen Schwachstellen kann der Mechanismus nur mit "**schwach**" bewertet werden.

Auswirkungen auf die Gesamtbewertung des Systems

Wegen dieser Bewertung kann das System **maximal noch die Qualitätsstufe Q1** erreichen, da die Identifikation und Authentisierung von Benutzern als wichtige Sicherheitsanforderung angesehen wird.

Grundfunktion Rechteverwaltung

Beispiel: Rechteverwaltung mit Zugriffskontrolllisten

Beschreibung des Mechanismus

Zur Rechteverwaltung sind Zugriffskontrolllisten implementiert, die in speziellen Dateien aufbewahrt werden. Diese Dateien sind gegen unbefugte Zugriffe geschützt. Zur Rechtevergabe und Rechteänderung sind Systemfunktionen vorhanden. Rechte an einem Objekt können nur der "Besitzer" (Erzeuger) des Objektes und der Systemverwalter vergeben. Es gilt immer das zeitlich zuletzt vergebene Recht. Rechte können nur explizit und zwischen einzelnen Subjekten und einzelnen Objekten eingerichtet werden. Beim Löschen oder Umbenennen eines Benutzers erfolgt keine Bereinigung der Zugriffskontrolllisten. Zugriffsberechtigte Benutzer können für ein Objekt die Zugriffe durch andere Benutzer zeitweise blockieren.

Von dem Mechanismus abzudeckende Sicherheitsanforderungen

Der Mechanismus soll Zugriffsrechte von Benutzern zu Dateien verwalten. Dabei soll es möglich sein, für jeden Benutzer und jede Datei separat die Zugriffsberechtigung festzulegen. Zugriffsrechte vergeben, entziehen oder ändern darf nur dem Besitzer der Datei und dem Systemverwalter möglich sein.

Bewertung anhand der Kriterien:

Vollständigkeit

Die Vollständigkeit ist gegeben. Es ist möglich, für jeden Benutzer und jede Datei eigene Zugriffsrechte einzurichten.

Widerspruchsfreiheit

Ein Widerspruch kann nur eintreten, wenn Systemverwalter und Besitzer unterschiedliche Rechte zu einem Objekt vergeben. Dieser Konflikt ist dadurch gelöst, daß das zeitlich zuletzt vergebene Recht gilt. Wenn sowohl Systemverwalter als auch Besitzer die Möglichkeit besitzen, sich die Zugriffsrechte zu einem Objekt auflisten zu lassen, ist die Widerspruchsfreiheit gegeben.

Überschaubarkeit

Sowohl der Systemverwalter als auch der Besitzer eines Objektes können sich alle zu diesem Objekt vergebenen Zugriffsrechte anschauen. Da keine impliziten (zum Beispiel durch Regeln eingerichtete) Rechte bestehen, ist die Überschaubarkeit gegeben. Allerdings ist es nicht möglich, daß ein Benutzer sich auflistet, zu welchen Objekten er welche Zugriffsrechte besitzt. Dies wird jedoch nur als sehr geringe Schwäche gesehen, die keine Abwertung nach sich zieht.

Schutz vor verdeckten Rechteänderungen

Die Systemfunktionen zur Rechteverwaltung sind von normalen Benutzerprogrammen aus aufrufbar. Damit können Rechte verdeckt (zum Beispiel durch "Trojanische Pferde") eingerichtet, gelöscht oder geändert werden. Auch ist es möglich, daß der Systemverwalter sich selbst sperrt, d.h. seine eigenen Rechte entzieht.

==> Abwertung, der Mechanismus kann maximal noch mit "stark" bewertet werden.

Begründung:

Diese Schwachstelle stellt eine ernstzunehmende Bedrohung dar. Dadurch ist eine Einrichtung, Änderung oder Löschung von Rechten durch Unbefugte möglich. Allerdings muß ein zu der Aktion berechtigter Benutzer das Programm explizit starten, welches die Rechteänderung verdeckt durchführt.

Rechteverwaltung beim Löschen oder Umbenennen von Subjekten oder Objekten

Die Zugriffskrollisten werden beim Löschen oder Umbenennen eines Subjektes nicht bereinigt. Dies kann zu ungewollten Rechtebeziehungen führen. Diese Schwachstelle stellt eine mittlere Bedrohung dar.

==> Abwertung, der Mechanismus kann wegen dieser Schwachstelle maximal noch mit "sehr stark" bewertet werden.

Schutz vor Einschränkung bei der Ausübbarkeit von Rechten

Das System läßt zu, daß Objekte von zugriffsberechtigten Benutzern blockiert werden. Es sind keine Vorkehrungen getroffen, die die Dauer dieser Blockade beschränken.

Die Sicherheitsanforderungen enthalten keine Verfügbarkeitsaspekte. Daher erfolgt keine Abwertung wegen dieser Schwäche, jedoch wird darauf hingewiesen, daß dieses System nicht für Aufgaben eingesetzt werden sollte, bei denen erhöhte Anforderungen bezüglich der Verfügbarkeit von Daten aus normalen Dateien bestehen.

Bewertung des Mechanismus

Wegen der aufgezeigten Schwachstellen wird der Mechanismus mit **"stark"** bewertet.

Auswirkungen auf die Gesamtbewertung des Systems

Durch diese Bewertung kann das Gesamtsystem **maximal noch die Qualitätsstufe Q4** erreichen.

Beispiel: Capabilities

Beschreibung des Mechanismus

Betrachtet wird ein verteiltes System, bei dem Zugriffsrechte über Capabilities verwaltet werden. Die Capabilities sind gegen unberechtigte Modifikationen durch einen Verschlüsselungsmechanismus geschützt. Der dabei verwendete Verschlüsselungsmechanismus ist mit "nicht überwindbar" bewertet worden. Ein Zurückziehen von Capabilities ist durch Änderung des Schlüssels beim Objekt realisiert. Dadurch verlieren dann jedoch alle bisher zu diesem Objekt vergebenen Capabilities ihre Gültigkeit. Eine "Garbage Collection" für Objekte, zu denen keine Capabilities mehr existieren, ist als privilegierte Prozedur vorhanden, die von Benutzern mit der entsprechenden Capability gestartet werden kann. Die Weitergabe bzw. das Kopieren von Capabilities ist problemlos von jedem Programm aus möglich.

Von dem Mechanismus zu erfüllende Sicherheitsanforderungen

Der Mechanismus soll es ermöglichen, Zugriffsrechte zwischen Benutzern und Prozessen zu Dateien, Programmen und Prozessen zu verwalten. Es soll möglich sein, ein Recht, welches ein Benutzer oder Prozeß besitzt, kontrolliert weiterzugeben. Es muß möglich sein, Rechte wieder zu entziehen.

Generelle Bemerkungen

Es existieren bei diesem Mechanismus bekannte Problembereiche, denen bei der Untersuchung und Bewertung besondere Aufmerksamkeit gewidmet werden muß. Diese Problembereiche sind:

- Zurückrufen von Capabilities.
- Beschränkung der Weitergabe von Capabilities.
- Entstehung von Objekten, zu denen keine Capabilities mehr im System existieren.

Bewertung anhand der Kriterien

Vollständigkeit

Die Granularität der Rechte entspricht den Sicherheitsanforderungen. Der Aspekt der Vollständigkeit ist somit gegeben.

Widerspruchsfreiheit

Da der Entzug von Capabilities für ein Objekt nur global erfolgen kann, ist die Widerspruchsfreiheit gegeben.

Überschaubarkeit

Ein Benutzer kann seine Capabilities auflisten und weiß damit, zu welchen Objekten er welche Zugriffsrechte besitzt. Damit besitzt er alle notwendigen Informationen. Es ist nicht notwendig, daß er die Namen von Objekten kennt, zu denen er kein Zugriffsrecht besitzt. Im Normalfall ist es auch nicht nötig, daß zu einem Objekt eine Liste der zugriffsberechtigten Subjekte erstellt wird. Lediglich zur Prüfung, ob überhaupt noch ein Subjekt im System eine Capability für dieses Objekt besitzt, ist eine solche Funktion sinnvoll und vorhanden ("Garbage Collection").

Schutz vor verdeckten Rechteänderungen

Da Capabilities von jedem Programm weitergegeben bzw. kopiert werden können, ist kein Schutz gegen verdeckte Rechteänderungen gegeben. Rechte können somit zum Beispiel durch "Trojanische Pferde" beliebig weitergegeben werden.

====> Abwertung, der Mechanismus kann maximal noch mit "stark" bewertet werden.

Begründung:

Dadurch ist eine ungewollte Weitergabe von Rechten möglich, die nachträglich nur sehr schwer rückgängig gemacht werden kann. Einem gutwilligen Benutzer ist es nur bedingt möglich, sich vor dieser Bedrohung zu schützen.

Rechteverwaltung beim Löschen oder Umbenennen von Subjekten oder Objekten

Beim Löschen eines Subjektes werden die Capabilities mit gelöscht, beim Umbenennen eines Subjektes bleiben die Capabilities unverändert. Beim Löschen eines Objektes werden die Capabilities zu diesem Objekt nicht automatisch gelöscht, der Benutzer erfährt lediglich, daß dieses Objekt nicht mehr existiert. Beim Umbenennen eines Objektes bleiben die Capabilities gültig.

Schutz vor der Einschränkung bei der Ausübbarkeit von Rechten

Das System läßt zu, daß Objekte von zugriffsberechtigten Benutzern blockiert werden. Es sind keine Vorkehrungen getroffen, die die Dauer dieser Blockade beschränken.

Die Sicherheitsanforderungen enthalten keine Verfügbarkeitsaspekte. Daher erfolgt keine Abwertung wegen dieser Schwäche, jedoch wird darauf hingewiesen, daß dieses System nicht für Aufgaben eingesetzt werden sollte, bei denen erhöhte Anforderungen bezüglich der Verfügbarkeit von Daten aus normalen Dateien bestehen.

Bewertung des Mechanismus

Wegen der aufgezeigten Schwachstellen wird der Mechanismus mit "**stark**" bewertet.

Auswirkungen auf die Gesamtbewertung des Systems

Durch diese Bewertung kann das Gesamtsystem **maximal noch die Qualitätsstufe Q4** erreichen.

Grundfunktion Rechteprüfung

Beispiel: Prüfung der Rechte beim Aufbau einer logischen Verbindung

Beschreibung des Mechanismus

Es wird ein System angenommen, welches Zugriffsrechte von Benutzern zu Dateien kennt und mit Zugriffskontrolllisten verwaltet. Die Prüfung auf Zugriffsberechtigung erfolgt beim Eröffnen einer Datei. Beim eigentlichen Zugriff erfolgt dann keine Prüfung mehr. Beim Entzug eines Zugriffsrechtes wird nicht geprüft, ob der Benutzer, dem das Recht entzogen wird, die Datei noch geöffnet hat.

Von dem Mechanismus abzudeckende Sicherheitsanforderungen

Der Mechanismus soll bei jedem Versuch eines Benutzers, auf eine Datei zuzugreifen, die Berechtigung für diesen Zugriff prüfen.

Bewertung anhand der Kriterien

Vollständigkeit der Rechteprüfung

Aus der Spezifikation sind keine Wege ersichtlich, durch die ein Zugriff zu Daten in einer Datei ohne vorheriges Eröffnen dieser Datei möglich ist. (**Hinweis:** Durch Implementierungsfehler können solche Wege natürlich im realen System noch existieren. Nach solchen Fehlern wird bei der Qualitätsprüfung des Systems gesucht, nicht jedoch bei der Prüfung des Mechanismus.)

Zeitpunkt der Rechteprüfung

Geprüft wird vor dem eigentlichen Zugriff beim Eröffnen einer Datei. Die tatsächlichen Zugriffe können sehr viel später erfolgen. Wird zwischenzeitlich das Zugriffsrecht entzogen, so kann der Benutzer trotzdem noch auf die Datei zugreifen solange sie geöffnet ist. Es bleibt dem Benutzer überlassen, wie lange er die Datei offen hält.

==> Abwertung, der Mechanismus kann maximal noch mit "stark" bewertet werden.

Begründung:

Diese Schwachstelle kann von böswilligen Benutzern ausgenutzt werden. Voraussetzung ist allerdings, daß sie das Zugriffsrecht besessen haben. Daher wird die Bedrohung durch die Ausnutzung dieser Schwachstelle als nicht so gravierend angesehen. Daher kann der Mechanismus trotz dieser Schwäche noch mit "stark" bewertet werden.

Verfügbarkeit der Entscheidungsdaten

Durch Hardware-Fehler (z.B. Ausfall der Platte mit den Zugriffskontrolllisten) kann eine Situation entstehen, in der die Entscheidungsdaten nicht zur Verfügung stehen, das System im Prinzip jedoch in der Lage wäre, einen Teil seiner Aufgaben noch zu erfüllen. In dieser Situation verweigert das System jedoch jedem Benutzer den Zugriff zu Dateien. Dadurch kann keine der Aufgaben des Systems weiter erfüllt werden.

Ob und wie stark der Mechanismus wegen dieser Schwachstelle abgewertet werden muß, hängt von der Wahrscheinlichkeit ab, mit der die oben beschriebene Situation eintreten kann.

Integrität der Entscheidungsdaten

Die Zugriffskontrolllisten sind in einer Datei abgespeichert. Der Zugriff zu dieser Datei wird über die Mechanismen der Rechteverwaltung und Rechteprüfung überwacht. Eine gezielte Manipulation der Zugriffskontrolllisten durch Unbefugte ist dadurch vom Design her weitgehend ausgeschlossen. Zur Erkennung von Fehlern bei der Speicherung werden Prüfsummen verwendet. Dadurch ist die Wahrscheinlichkeit für einen nicht erkannten stochastischen Fehler bei der Datenspeicherung so gering, daß keine Abwertung erfolgen muß.

Bewertung des Mechanismus

Wegen der aufgezeigten Schwachstellen wird der Mechanismus mit "**stark**" bewertet.

Auswirkungen auf die Gesamtbewertung des Systems

Durch diese Bewertung kann das Gesamtsystem **maximal die Qualitätsstufe Q4** erreichen.

Grundfunktion Beweissicherung

Beispiel: Beweissicherung auf normalen Dateien über Systemfunktionen

Beschreibung des Mechanismus

Die Beweissicherung erfolgt auf normalen Dateien, die durch die Mechanismen der Rechteverwaltung und Rechteprüfung geschützt werden können. Ein automatischer Schutz ist nicht gegeben. Die Beweissicherung wird über Systemschnittstellen aufgerufen.

Von dem Mechanismus abzudeckende Sicherheitsanforderungen

Der Mechanismus soll jede Benutzung des Identifikations- und Authentisierungsmechanismus sowie jeden Zugriffsversuch auf Dateien mit Datum, Uhrzeit und Benutzernamen protokollieren. Der Mechanismus soll Protokolldaten vor unberechtigten Zugriffen schützen. Die gesammelten Protokolldaten sollen Beweiskraft besitzen.

Bewertung anhand der Kriterien

Untäuschbarkeit der Beweissicherung

Tests ergaben, daß Benutzerprogramme Protokollsätze mit beliebigem Inhalt erzeugen können. Dadurch ist es möglich, "Ereignisse" zu protokollieren, die tatsächlich nicht stattgefunden haben. Dadurch ist der Mechanismus täuschbar.

====> sehr starke Abwertung, der Mechanismus kann nur mit "ungeeignet" bewertet werden.

Begründung:

Der Mechanismus ist nicht in der Lage, die an ihn gestellten Anforderungen zu erfüllen, da die protokollierten Informationen keinerlei Beweiskraft haben.

Vollständigkeit

Alle in den Sicherheitsanforderungen aufgeführten Ereignisse werden mit den geforderten Informationen protokolliert.

Bewertung des Mechanismus

Wegen der aufgezeigten Schwachstelle wird der Mechanismus mit "**ungeeignet**" bewertet.

Auswirkungen auf die Gesamtbewertung des Systems

Durch diese Bewertung kann das Gesamtsystem **nur die Qualitätsstufe Q0** erreichen.

Grundfunktion Wiederaufbereitung

Beispiel: Überschreiben der Daten von gelöschten Dateien mit binären Nullen.

Beschreibung des Mechanismus

Beim Löschen einer Datei wird nicht nur der Katalogeintrag gelöscht, sondern auch der von dieser Datei belegte Platz auf dem Datenträger mit binären Nullen überschrieben.

Von dem Mechanismus abzudeckende Sicherheitsanforderungen

Der von einer Datei belegte Platz auf dem Speichermedium muß beim Löschen dieser Datei so wiederaufbereitet werden, daß es danach nicht mehr möglich ist, die in dieser Datei abgelegten Informationen zu rekonstruieren.

Bewertung anhand der Kriterien

Art der Wiederaufbereitung

Bei Wechseldatenträgern besteht die Gefahr, daß sie außerhalb des Systems analysiert werden. Mit aufwendigen Verfahren ist es unter Umständen möglich, den Inhalt von gelöschten Dateien zu rekonstruieren. Ob und mit welchem Aufwand dies möglich ist, wird im Rahmen der Evaluation nicht geprüft. Es ist nicht möglich, den Inhalt gelöschter Dateien mit Hilfe von Systemfunktionen zu rekonstruieren.

==> leichte Abwertung, der Mechanismus kann maximal mit "sehr stark" bewertet werden.

Begründung:

Es besteht die Möglichkeit, daß die Informationen auf dem Datenträger durch eine sehr aufwendige Analyse rekonstruiert werden können. Diesem Risiko kann durch organisatorische Maßnahmen begegnet werden. Die Einhaltung dieser Maßnahmen läßt sich allerdings nicht durch das IT-System überwachen. Daher kann der Mechanismus nach den Regeln der IT-Sicherheitskriterien maximal noch die Bewertung "sehr stark" erhalten.

Zeitpunkt der Wiederaufbereitung

Die Wiederaufbereitung erfolgt als Teil der Systemfunktion zum Löschen der Datei. Nach Beendigung des Löschvorganges besteht keine Möglichkeit mehr, auf die Daten der gelöschten Datei zuzugreifen.

Bewertung des Mechanismus

Wegen der aufgezeigten Schwachstelle wird der Mechanismus mit "**sehr stark**" bewertet.

Auswirkungen auf die Gesamtbewertung des Systems

Durch diese Bewertung kann das Gesamtsystem **maximal noch die Qualitätsstufe Q6** erreichen

Grundfunktion Fehlerüberbrückung

Beispiel: Behandlung von Programmfehlern durch das Betriebssystem

Beschreibung des Mechanismus

Bestimmte von der Hardware bzw. Firmware erkannte Programmfehler (z.B. Zugriffsversuch außerhalb des zur Verfügung stehenden Hauptspeicherbereiches, ungültiger Maschinenbefehl) erzeugen eine Unterbrechung. Beim Auftreten einer solchen Unterbrechung analysiert das Betriebssystem, welches Programm die Unterbrechung erzeugte und beendet dann dieses Programm.

Von dem Mechanismus abzudeckende Sicherheitsanforderungen

Das System soll bei den unten aufgezählten Programmfehlern das Programm, welches diesen Fehler verursachte, kontrolliert beenden. Alle von dem Programm bis zum Zeitpunkt des Auftretens des Fehlers abgesetzten Schreiboperationen auf Dateien oder andere externe Datenträger müssen kontrolliert zu Ende geführt werden. Dabei sollen keine Daten verlorengehen.

Folgende Fehler müssen erkannt und behandelt werden:

- Zugriff zu geschützten Hauptspeicherbereichen.
- Versuch der Ausführung ungültiger oder privilegierter Operationen.
- Ganzzahl-Division durch Null.

Bewertung anhand der Kriterien

Vollständigkeit der Fehlererkennung

Aus den Designunterlagen des Prozessors geht hervor, daß es keine Ausnahmen bei der Fehlerbehandlung gibt. Auch bei Tests wurden keine Ausnahmen gefunden.

Korrektheit der Fehleranalyse

Zur Fehleranalyse werden bei diesem Mechanismus folgende Informationen benötigt:

- die Fehlerart,
- die Adresse der Instruktion, die den Fehler verursachte,
- der Prozeß bzw. das Programm, welches den Fehler verursachte.

Aus den Designunterlagen des Prozessors geht hervor, daß die Fehlerart durch eine Unterbrechungskennziffer eindeutig bestimmt werden kann. Aus diesen Unterlagen geht außerdem hervor, daß die Instruktion, die den Fehler verursachte eindeutig bestimmbar ist. Aus der Systemspezifikation geht hervor, daß zu jedem Zeitpunkt eindeutig bestimmbar ist, welcher Prozeß bzw. welches Programm aktiv ist.

Tests ergaben keine Hinweise auf eine falsche Fehleranalyse.

Funktions-, Daten- oder Zeitverlust

Programme werden im Fehlerfall vom Betriebssystem beendet. Somit entsteht Funktionsverlust.

Ausgabepuffer im Hauptspeicher werden im Fehlerfall nicht auf die Dateien hinausgeschrieben. Dateien werden im Fehlerfall nicht korrekt geschlossen. Dadurch kann nicht unerheblicher Datenverlust entstehen.

Zeitverlust entsteht durch die Notwendigkeit, Daten zu rekonstruieren und durch das Neustarten des Programms, welches den Fehler verursachte.

==> sehr starke Abwertung, der Mechanismus kann nur als "ungeeignet" eingestuft werden.

Begründung:

Die Sicherheitsanforderungen verlangen, daß auch im Fehlerfall alle bis zu diesem Zeitpunkt geschriebenen Daten verfügbar sind.

Der Mechanismus ist nicht in der Lage eine der Sicherheitsanforderungen, die er abdecken soll, zu erfüllen. Daher muß er als "ungeeignet" eingestuft werden.

Unabhängigkeit des Korrekturverfahrens von der Fehlerquelle

Es wurden keine Wege gefunden, bei denen durch das Auftreten eines Fehlers das Korrekturverfahren selbst beeinflußt werden kann.

Fehler in der Fehlerüberbrückung

Es ist durchaus möglich, daß einer der zu überbrückenden Fehler in der Fehlerüberbrückung, die das Betriebssystem vornimmt, selbst auftritt. Es sind keine Vorkehrungen getroffen, die einen solchen Fall erkennen und speziell behandeln. Dadurch kann es zu einem nicht endenden rekursiven Aufruf der Fehlerüberbrückungsprogramme kommen. Die Wahrscheinlichkeit für das Eintreffen eines solchen Falles ist allerdings sehr gering.

==> Abwertung, der Mechanismus kann wegen dieser Schwäche maximal noch mit "stark" bewertet werden.

Begründung:

Die geringe Wahrscheinlichkeit für das Eintreffen eines solchen Falles begründet, warum der Mechanismus trotz dieser Schwachstelle noch mit "stark" bewertet werden kann.

Bewertung des Mechanismus

Wegen der gefundenen Schwachstellen kann der Mechanismus nur mit "**ungeeignet**" bewertet werden.

Auswirkungen auf die Gesamtbewertung des Systems

Durch diese Bewertung kann das Gesamtsystem **nur noch die Qualitätsstufe Q0** erreichen.

Beispiel: Fehlerüberbrückung bei der Datenfernübertragung durch fehlererkennende und fehlerkorrigierende Übertragungsprotokolle.

Beschreibung des Mechanismus:

Mit jedem Datenpaket wird eine Prüfsumme übertragen. Diese Prüfsumme sei so gestaltet, daß beliebige Fehler in einem 8 Bit langen Teil eines Datenpaketes sicher erkannt werden können. Im Protokoll ist vorgesehen, daß die Empfängerseite nach jedem Datenpaket dem Sender mitteilt, ob die Daten korrekt empfangen wurden. Bei nicht korrektem Empfang der Daten wird das Datenpaket nochmals gesendet. Wird ein Datenpaket auch nach dem dritten Senderversuch nicht korrekt empfangen, so wird die Übertragung vollständig abgebrochen.

Von dem Mechanismus abzudeckende Sicherheitsanforderungen

Der Mechanismus soll nicht absichtlich herbeigeführte Fehler bei der Datenübertragung erkennen und korrigieren.

Bewertung anhand der Kriterien

Vollständigkeit der Fehlererkennung

Es muß die Klasse der nicht erkannten Fehler sowie die Wahrscheinlichkeit für das Eintreten eines solchen Fehlers bestimmt werden. Entsprechend dieser Wahrscheinlichkeit ist der Mechanismus dann zu bewerten. Als Grundlage für die Bewertung eines Mechanismus ist es im allgemeinen sinnvoller die Wahrscheinlichkeit für das Auftreten eines solchen Fehlers pro Tag zu ermitteln und dabei das mittlere Datenaufkommen auf der Leitung zugrunde zu legen. Dadurch fließt dann auch die Menge der über die Leitung übertragenen Daten mit in die Bewertung ein. Als Faustregel kann dabei gelten:

Sei P die Wahrscheinlichkeit für das Eintreten eines nicht erkannten Übertragungsfehlers pro Tag. Dann soll gelten:

Falls P größer ist als 0,5 so wird der Mechanismus mit "schwach" bewertet.

Falls P größer ist als 0,1 und kleiner oder gleich 0,5 so wird der Mechanismus mit "mittelstark" bewertet.

Falls P größer ist als 0,001 und kleiner oder gleich 0,1 so wird der Mechanismus mit "stark" bewertet.

Falls P kleiner oder gleich 0,001 so wird der Mechanismus mit "sehr stark" bewertet.

Falls besonders strenge oder besonders schwache Anforderungen bezüglich der Datenintegrität bestehen, muß diese Faustregel entsprechend angepaßt werden.

Im konkreten Beispiel sei P mit 0,0005 errechnet worden.

====> der Mechanismus kann maximal noch mit "sehr stark" bewertet werden.

Korrektheit der Fehleranalyse

Eine Analyse der Fehlerquelle findet nicht statt.

Daten-, Funktions- oder Zeitverlust

Datenverlust tritt nur bei einem nicht erkannten Übertragungsfehler auf. Dieser Fall wurde schon oben bewertet.

Funktionsverlust tritt nur auf, wenn bei drei aufeinanderfolgenden Sendeversuchen ein erkannter Fehler auftrat. Auch hier ist die Wahrscheinlichkeit für das Eintreten eines solchen Falles abzuschätzen. Die Bewertung wegen dieser Schwäche hängt von den Anforderungen an die Verfügbarkeit der Daten im Empfängersystem ab.

Ein kleiner Zeitverlust tritt bei jedem erkannten Fehler durch das nochmalige Senden des Datenpaketes auf. Die Wahrscheinlichkeit für das Auftreten eines erkennbaren Fehlers in einem Datenpaket muß abgeschätzt werden. Ob und in welchem Maße der Mechanismus wegen dieser Schwachstelle abgewertet werden muß, hängt von dieser Wahrscheinlichkeit ab. Im konkreten Beispiel enthalten die Sicherheitsanforderungen keine Bedingungen bezüglich der Verfügbarkeit der Daten im Empfängersystem. Falls dort die Anforderung nach sofortiger Verfügbarkeit ohne Zeitverlust bestehen würde, müßte der Mechanismus entsprechend stark abgewertet werden. Im konkreten Beispiel braucht jedoch keine Abwertung wegen dieser Schwachstelle zu erfolgen; jedoch muß im Evaluationsbericht darauf hingewiesen werden, daß dieses System nur bedingt geeignet ist für Einsatzzwecke, die eine unmittelbare Verfügbarkeit der gesendeten Informationen im Empfängersystem fordern.

Bewertung des Mechanismus

Wegen der gefundenen Schwachstellen wird der Mechanismus mit "**sehr stark**" bewertet.

Auswirkungen auf die Gesamtbewertung des Systems

Durch diese Bewertung kann das System im allgemeinen **maximal die Qualitätsstufe Q6** erreichen. Lediglich falls die durch diesen Mechanismus abgesicherten Datenübertragungswege nach übereinstimmender Auffassung von Auftraggeber und Evaluations-Team keine besonders sicherheitskritischen Aufgaben erfüllen müssen, kann auch eine Einstufung in die Qualitätsstufe Q7 noch möglich sein.

2. Erläuterungen zu den Funktionalitätsklassen

Ein Anwender wird vor der Auswahl eines Systems aufgrund der Erkenntnisse aus der Bedrohungsanalyse das Vorhandensein bestimmter Sicherheitsfunktionen fordern. Will er nun aus der Liste der evaluierten Produkte ein für seine Zwecke geeignetes auswählen, so ist es zweckmäßig, ihm Anhaltspunkte zu geben, welche Produkte seine funktionalen Anforderungen erfüllen können, bzw. welche Produkte für ihn nicht geeignet sind. Dies ist der Zweck der Funktionalitätsklassen.

Dabei sind die Anforderungen in den einzelnen Funktionalitätsklassen mit Absicht sehr abstrakt formuliert. Ein Anwender sollte sich nun auf diesem Abstraktionsniveau klar werden, welche Funktionalitätsklasse(n) er für sein System fordert. Im allgemeinen sind diese Forderungen detaillierter als die Beschreibungen der Funktionalitätsklassen. Der Anwender kann sich nun jedoch bei der Auswahl eines Systems auf die Betrachtung derjenigen Systeme beschränken, die in die für ihn geeignete(n) Funktionalitätsklasse(n) sowie in die seinen Anforderungen genügende Qualitätsstufe evaluiert wurden. Bei diesen Systemen wird er dann seine Sicherheitsanforderungen mit der detaillierten Beschreibung der Sicherheitsfunktionen in den einzelnen Evaluationsberichten abgleichen. Durch die Vorauswahl über die Funktionalitätsklassen bleibt es ihm jedoch erspart, alle evaluierten Systeme in seinem Auswahlprozeß zu betrachten.

Es ist natürlich auch möglich, daß ein System, welches in die vom Anwender geforderte Funktionalitätsklasse evaluiert wurde, trotzdem nicht für die Erfordernisse des Anwenders geeignet ist. Dies ist immer dann der Fall, wenn der Anwender bei der Präzisierung der globalen Anforderungen einer Funktionalitätsklasse Detailforderungen aufstellt, die nicht mehr von allen Systemen der Funktionalitätsklasse erfüllt werden. So kann zum Beispiel ein Anwender die Funktionalitätsklasse F2 fordern, die Sicherheitsanforderungen jedoch dahingehend präzisieren, daß er die Zugriffsrechte Lesen, Schreiben und Ausführen bzw. Kombinationen dieser Rechte für Dateien als Objekte der Rechteverwaltung fordert. Ein virtueller Maschinenmonitor, der nur die Zugriffsrechte Lesen, Schreiben sowie Lesen und Schreiben auf der Ebene logischer Platten bzw. Plattensegmente kennt, kann zwar (wenn auch die anderen Anforderungen von F2 erfüllt werden) prinzipiell in die Funktionalitätsklasse F2 evaluiert werden, er ist jedoch für den Anwender mit den oben beschriebenen Anforderungen nicht geeignet.

Andererseits bedeutet dies, daß es nicht ausreicht, bei der Anmeldung eines Systems zur Evaluation lediglich eine oder mehrere Funktionalitätsklassen mit der angestrebten Qualitätsstufe anzugeben. Für die Evaluation ist eine detaillierte Auflistung der Sicherheitsanforderungen zwingend notwendig. Diese müssen die abstrakten Forderungen der angestrebten Funktionalitätsklasse(n) abdecken und Präzisierungen und Erweiterungen dieser Anforderungen sein.

Dabei können Erweiterungen zusätzliche Sicherheitsanforderungen sein, die sich nicht aus den angestrebten Funktionalitätsklassen ableiten lassen. Auch diese zusätzlichen Sicherheitsanforderungen werden bei der Evaluation geprüft und im Evaluationsbericht beschrieben.

Die Funktionalitätsklassen F1 bis F5 sind aus der Funktionalität der Klassen der amerikanischen "Trusted Computer System Evaluation Criteria" (dem sogenannten "Orange Book") abgeleitet. Dadurch soll gewährleistet werden, daß einerseits Systeme, die in den USA nach den Kriterien des "Orange Book" evaluiert wurden, auch bezüglich ihrer Funktionalität in die nationalen IT-Sicherheitskriterien eingeordnet werden können. Andererseits ist dadurch in bestimmten Fällen auch die umgekehrte Abbildung möglich, wenn ein System bezüglich Funktionalität und Qualität nach den nationalen IT-Sicherheitskriterien in Klassen evaluiert wurde, die die Kriterien einer "Orange Book"-Klasse umfassen. Wie diese Abbildung im einzelnen aussieht, wird im Kapitel 12 dieses Handbuches beschrieben.

Entsprechend den Klassen des "Orange Book" sind die Funktionalitätsklassen F1 bis F5 hierarchisch geordnet, d.h. in der Funktionalitätsklasse F1 werden die geringsten, in der Funktionalitätsklasse F5 die höchsten Anforderungen an die Sicherheitsfunktionen gestellt. Die restlichen Funktionalitätsklassen besitzen keine äquivalente Klasse im "Orange Book" und sind auch nicht hierarchisch geordnet. Bei allen Funktionalitätsklassen wurden die Anforderungen zu den einzelnen Grundfunktionen zusammengefaßt. Dadurch sollen die Anforderungen der einzelnen Funktionalitätsklassen besser überschaubar werden.

An einigen Stellen wurden die Anforderungen des "Orange Book" umformuliert und teilweise verallgemeinert, da sie in der dort niedergelegten Form nicht in die Philosophie der IT-Sicherheitskriterien passen. Dies gilt insbesondere für die Fälle, in denen das "Orange Book" Mechanismen vorschreibt (z.B. bei "Labels", bei Adreßräumen etc.).

Auch die "Mandatory Access Control" wurde verallgemeinert, da die im "Orange Book" aufgestellten Regeln nicht bei allen Einsatzzwecken der Systeme sinnvoll sind. Es wird lediglich verlangt, daß sich (z.B. durch eine spezielle Konfigurierung des Systems) auch die im "Orange Book" aufgestellten Regeln realisieren lassen.

Bei den Funktionalitätsklassen, die keine Entsprechung mehr im "Orange Book" besitzen, d.h. in den Funktionalitätsklassen F6 bis F10, wurde dann nicht mehr versucht, möglichst viele Grundfunktionen abzudecken. Im wesentlichen stellt jede dieser Funktionalitätsklassen schwerpunktmäßig Sicherheitsanforderungen zu einer speziellen Grundfunktion. Lediglich die Funktionalitätsklasse F6 bildet hier eine Ausnahme, da dort Anforderungen in stark voneinander abhängigen Grundfunktionen "Identifikation und Authentisierung", "Rechteverwaltung", "Rechteprüfung" und "Beweissicherung" gestellt werden.

Dadurch soll es möglich sein, die Sicherheitsanforderungen zu den einzelnen Grundfunktionen weitgehend unabhängig voneinander festzulegen (soweit dies sinnvoll ist) und dann Funktionalitätsklassen auszuwählen, die die aufgestellten Sicherheitsanforderungen abdecken. Es ist also durchaus denkbar und auch sinnvoll, wenn ein System die Sicherheitsanforderungen mehrerer Funktionalitätsklassen abdeckt oder Sicherheitsanforderungen an das System gestellt werden, die in dieser Kombination in keiner der bisherigen Funktionalitätsklassen enthalten sind. Im Zertifikat sind dann alle diese Funktionalitätsklassen aufgeführt. Eventuell vorhandene zusätzliche Sicherheitsfunktionen, die über die Anforderungen der im Zertifikat aufgeführten Funktionalitätsklassen hinausgehen sind im Zertifikat aufgeführt und werden im Evaluationsbericht vollständig beschrieben.

Es ist jederzeit möglich, neue Funktionalitätsklassen zu definieren und als Nachtrag in die IT-Sicherheitskriterien aufzunehmen. Ob neue Funktionalitätsklassen aufgenommen werden und wie diese gestaltet sein sollen, bleibt der Evaluationsbehörde überlassen. Jedoch sollten Vorschläge für solche neuen Funktionalitätsklassen durchaus auch von außen an die Evaluationsbehörde herangetragen werden. Falls neue Funktionalitätsklassen in die IT-Sicherheitskriterien aufgenommen werden, können die Auftraggeber von früheren Evaluationen eine Prüfung beantragen, ob ihr bereits evaluiertes Produkt die Kriterien einer neuen Klasse erfüllt. Dazu ist keine neue Produktprüfung erforderlich, sondern es werden die Anforderungen der neuen Klasse mit den im Evaluationsbericht beschriebenen Sicherheitsfunktionen des evaluierten Systems verglichen. Ist daraus ersichtlich, daß das System den Anforderungen der neuen Funktionalitätsklasse genügt, so wird dies in einem Nachtrag zum Zertifikat bestätigt. Nur falls durch diesen Abgleich nicht eindeutig geklärt werden kann, ob das evaluierte System die Anforderungen der neuen Funktionalitätsklasse erfüllt, ist eine (im allgemeinen recht kurze) Produktnachprüfung notwendig, durch die die bestehenden Unklarheiten geklärt werden sollen.

Wie bereits erläutert, ist es auch möglich, Systeme zu evaluieren, die nicht alle Kriterien einer in den IT-Sicherheitskriterien aufgeführten Funktionalitätsklasse erfüllen. In diesem Fall werden im Evaluationsbericht die Sicherheitsfunktionen des Systems vollständig beschrieben. Im Zertifikat wird für solche Systeme dann nur die erreichte Qualitätsstufe aufgeführt und auf die Beschreibung der Sicherheitsfunktionen im Evaluationsbericht verwiesen.

3. Erläuterungen zu den Qualitätskriterien

Das folgende Kapitel enthält Erläuterungen zu den einzelnen Qualitätsstufen, die einerseits zum besseren Verständnis der Qualitätskriterien beitragen sollen, andererseits aber auch Hinweise für die Handhabung der Kriterien bei der Evaluation geben sollen. Zwar ist dieses Kapitel vollständig analog zur Gliederung des entsprechenden Kapitels in den IT-Sicherheitskriterien gestaltet, jedoch sind hier - im Gegensatz zu den IT-Sicherheitskriterien - auch alle Erläuterungen zu beachten, die für niedrigere Qualitätsstufen gemacht wurden. Es werden also zu jeder Qualitätsstufe im wesentlichen nur die Aspekte erläutert, die entweder neu hinzugekommen sind oder sich gegenüber der nächstniedrigeren Qualitätsstufe geändert haben. Interpretationsschwierigkeiten, die sich bei den ersten Evaluationen ergeben werden, sollten durch zusätzliche Erläuterungen im IT-Evaluationshandbuch beseitigt werden. Dies wird voraussichtlich dazu führen, daß das IT-Evaluationshandbuch einem stärkeren Wandel unterworfen sein wird als die IT-Sicherheitskriterien selbst.

Es folgen nun die Erläuterungen zu den einzelnen Qualitätsstufen, wobei zur Stufe Q0 keine Erläuterungen gegeben werden.

Qualitätsstufe Q1

Erläuterungen zu den Kriterien

Die Qualitätsstufe Q1 ist vorgesehen für Systeme bzw. Einzelkomponenten, an die keine besonders hohen Anforderungen bezüglich der Qualität der Erfüllung der Sicherheitsanforderungen gestellt werden. Die Evaluation soll hier lediglich sicherstellen, daß die Sicherheitsanforderungen bei der Implementierung beachtet wurden und keine groben Fehler vorhanden sind. Systeme der Qualitätsstufe Q1 können für nicht sicherheitskritische Bereiche durchaus ausreichend sein. Sie gewährleisten immerhin, daß bei gutwilligem Benutzerverhalten die Sicherheitsanforderungen erfüllt werden; jedoch verbleibt ein relativ hohes Restrisiko, daß trotz der Evaluation noch Schwachstellen im System existieren, durch die Sicherheitsfunktionen umgangen oder außer Kraft gesetzt werden können.

Qualität der Sicherheitsanforderungen

Erläuterungen zu den Kriterien

Die Sicherheitsanforderungen brauchen zur Erreichung der Qualitätsstufe Q1 nur sehr grob und oberflächlich festgelegt zu sein und können durchaus noch großen Interpretationsspielraum lassen. Allerdings dürfen bei einmaligem Durchlesen der Sicherheitsanforderungen keine Widersprüche gefunden werden. Während der Evaluation gefundene, eventuell auf bestimmten Interpretationen der Sicherheitsanforderungen beruhende Widersprüche müssen dann zwischen dem Auftraggeber und dem Evaluations-Team geklärt werden.

Qualität der Spezifikation

Erläuterungen zu den Kriterien

Aus der Spezifikation muß sich ableiten lassen, welche Mechanismen zur Erfüllung der Sicherheitsanforderungen benutzt werden, auch wenn nicht alle Details dieser Mechanismen beschrieben sind. Allerdings muß entweder die Beschreibung ausreichend zur Bewertung der Mechanismen sein, oder aber die zur Bewertung noch fehlenden Informationen müssen sich durch einfache Tests ermitteln lassen. Der Aufwand zur Durchführung dieser Tests muß jedoch so gering sein, daß diese im Rahmen des Evaluationsplans durchgeführt werden können.

Qualität der verwendeten Mechanismen

Erläuterungen zu den Kriterien

"Mittelstark" sollte die Minimalbewertung für einen Mechanismus sein, der allein für die Erfüllung einer bestimmten Sicherheitsanforderung verantwortlich ist. Ein als "schwach" bewerteter Mechanismus sollte nur verwendet werden, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Der Mechanismus wird in Kombination mit anderen Mechanismen eingesetzt. Die Kombination dieser Mechanismen ist mit "mittelstark" oder besser bewertet worden.
- Der Mechanismus dient zur Erfüllung einer Sicherheitsanforderung, die nach übereinstimmender Auffassung von Auftraggeber und Evaluations-Team nur eine untergeordnete Rolle spielt.
- Der Aufwand für die Verwendung eines stärkeren Mechanismus steht nach übereinstimmender Auffassung von Auftraggeber und Evaluations-Team in keinem vertretbarem Verhältnis zu den dadurch entstehenden Kosten.

Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen

Erläuterungen zu den Kriterien

Auch für die Erreichung der Qualitätsstufe Q1 ist eine Abgrenzung der Sicherheitsfunktionen von nicht zu evaluierenden Teilen des Systems unabdingbar. Systeme, die dies nicht bieten oder aber dazu nur einen mit "mittelstark" oder gar nur mit "schwach" bewerteten Mechanismus benutzen, können lediglich in die Qualitätsstufe Q0 eingeordnet werden. Die Tests zu diesem Bereich sollen im wesentlichen zeigen, daß sich die Schnittstellen zwischen den zu evaluierenden und den nicht zu evaluierenden Systemteilen so verhalten, wie es in der Dokumentation beschrieben ist.

Qualität des Herstellungsvorganges

Erläuterungen zu den Kriterien

Da für eine Evaluation in die Qualitätsstufe Q1 keine Vorlage des Quellcodes der Implementierung verlangt wird, ist es auch nicht sinnvoll, Anforderungen hinsichtlich der Implementierungssprache, der Implementierungsumgebung oder der inneren Struktur dieses Quellcodes zu stellen. Die Prüfung der Implementierung besteht für diese Qualitätsstufe lediglich aus der Durchführung einer Reihe von Tests, die demonstrieren sollen, daß das System bei normaler Benutzung die Sicherheitsanforderungen erfüllt.

Besonders ausgefeilte Penetrationstests sind nicht erforderlich. Allerdings darf bei diesen einfachen Tests nichts gefunden werden, was eine Verletzung der Sicher-

heitsanforderungen bedeutet. Die Auswahl der Tests und die Bewertung der gefundenen Schwachstellen bleibt dem Evaluations-Team überlassen.

Betriebsqualität

Erläuterungen zu den Kriterien

Der Auftraggeber legt vor Beginn der Evaluation fest, welche Konfigurationen (Hardware und Software) evaluiert werden sollen. Die Anforderungen bezüglich der Konfigurierbarkeit des Systems besagen, daß jemand, der ein System konfiguriert, nach dem Lesen der Dokumentation in der Lage sein muß, die Auswirkungen der von ihm gewählten Konfiguration auf die Sicherheitsfunktionen des Systems in den wesentlichen Punkten beurteilen zu können. Zum Testen sind einige wenige Konfigurationsmöglichkeiten auszuwählen, das System danach zu konfigurieren und die gewählten Testfälle durchzuspielen (wobei diese Testfälle im wesentlichen für alle Konfigurationen gleich sind und nur dann angepaßt werden, wenn der Test in der ursprünglichen Fassung für die gewählte Konfiguration nicht durchführbar oder nicht sinnvoll ist).

Qualität der anwenderbezogenen Dokumentation

Erläuterungen zu den Kriterien

Die anwenderbezogene Dokumentation muß gut handhabbar sein und dem Anwender des Systems alle sicherheitsrelevanten Funktionen vollständig und verständlich beschreiben. Bei Abweichungen zwischen dem realen Systemverhalten und der Beschreibung in der anwenderbezogenen Dokumentation ist dem Auftraggeber in jedem Fall eine Frist zur Nachbesserung der Dokumentation einzuräumen. Alle gefundenen Unstimmigkeiten sind dem Auftraggeber mitzuteilen.

Qualitätsstufe Q2

Erläuterungen zu den Kriterien

Die Qualitätsstufe Q2 ist vorgesehen für Systeme bzw. Einzelkomponenten, an die mäßige Anforderungen bezüglich der Qualität der Erfüllung der Sicherheitsanforderungen gestellt werden. Ziel der Evaluation ist es, ein recht hohes Maß an Vertrauen zu gewinnen, daß die Sicherheitsfunktionen nicht durch Fehler umgangen oder außer Kraft gesetzt werden können. Systeme der Qualitätsstufe Q2 sind für Bereiche mit geringen bis mittleren Sicherheitsanforderungen häufig ausreichend. Die Evaluation soll zeigen, daß in diesem System bei einfach gearteten Penetrationsversuchen keine Fehler gefunden wurden, durch die Sicherheitsanforderungen des Systems nicht mehr erfüllt sind.

Qualität der Sicherheitsanforderungen

Erläuterungen zu den Kriterien

Die Sicherheitsanforderungen werden für die Qualitätsstufe Q2 im allgemeinen nur in natürlicher Sprache abgefaßt und sind die Zielsetzungen für die Sicherheitsfunktionen. Der Bezug zu den möglichen Bedrohungen und zu den Grundfunktionen ist in den Sicherheitsanforderungen darzustellen. Eine formale Konsistenzprüfung ist in diesem Fall nicht möglich. Daher kann nur nach verbalen Widersprüchen gesucht werden. Falls ein solcher Widerspruch entdeckt wird, muß mit dem Auftraggeber über diesen Punkt diskutiert werden, da es sich unter Umständen um das Ergebnis einer Fehlinterpretation der Sicherheitsanforderungen handeln kann. Auf jeden Fall sind die Sicherheitsanforderungen in einer Form neu zu formulieren, in der die gefundenen Widersprüche und Unklarheiten nicht mehr auftreten. Auf diese Weise müssen alle verbalen Unstimmigkeiten aus den Sicherheitsanforderungen beseitigt werden.

Qualität der Spezifikation

Erläuterungen zu den Kriterien

Die Spezifikation darf zwar eine recht oberflächliche natürlichsprachliche Beschreibung der Implementierung sein, jedoch dürfen keine Unklarheiten über die verwendeten Algorithmen und Mechanismen bestehen. Außerdem muß sich die Spezifikation auf die Sicherheitsanforderungen beziehen und erläutern, welcher Teil der Sicherheitsanforderungen mit welchen Algorithmen und Mechanismen abgedeckt werden soll. Nur auf diese Weise ist es dem Evaluations-Team möglich, mit vertretbarem Aufwand die Konsistenz zwischen den Sicherheitsanforderungen und der Spezifikation zu prüfen.

Treten bei dieser Prüfung Unklarheiten auf, so sind diese mit dem Auftraggeber oder dem Hersteller zu klären. In einigen Fällen kann allerdings die Klärung auch durch Tests erreicht werden. Nach der Klärung aller Unklarheiten ist vom Auftraggeber eine bereinigte Version der Spezifikation vorzulegen.

Nebeneffekte, durch die Sicherheitsfunktionen umgangen oder außer Kraft gesetzt werden können, sind in einer verbal formulierten Spezifikation natürlich nur recht schwer zu finden. Allerdings deuten Unklarheiten beim Verständnis der Spezifikation häufig auf solche Nebeneffekte hin. Dies sind dann Bereiche, die besonders sorgfältigen Tests unterzogen werden müssen.

Zu solchen Unklarheiten gehören insbesondere Parameterwerte der Sicherheitsfunktionen, deren Effekte in der Spezifikation nicht oder nur unvollständig beschrieben sind.

Qualität der verwendeten Mechanismen

Erläuterungen zu den Kriterien

Die Bewertung eines Mechanismus mit "mittelstark" besagt, daß er bereits einen brauchbaren Schutz bei mutwilligen Verstößen gegen die Sicherheitsanforderungen bietet. Daher ist ein solcher Mechanismus für die Zielrichtung der Qualitätsstufe Q2 durchaus als ausreichend zu betrachten.

Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen

Erläuterungen zu den Kriterien

Die Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen ist ein sehr wichtiger Aspekt bei der Beurteilung der Penetrations- und Manipulationssicherheit von Systemen oder Einzelkomponenten. Viele Systempenetrierungen beruhen auf Schwachstellen in diesem Bereich. Solche Schwachstellen sind insbesondere:

- unzureichende Parameterprüfung an den Schnittstellen,
- unzureichender Schutz von Datenbereichen,
- unzureichender Schutz vor Mißbrauch der erlaubten Funktionen.

In der Spezifikation muß daher angegeben sein, welche Schutzmechanismen zur Abgrenzung benutzt werden. Das Evaluations-Team muß diese Schutzmechanismen, die oft durch Hardware bzw. Firmware realisiert sind, sorgfältig prüfen und bewerten. Danach ist an Hand der Spezifikation zu prüfen, ob diese Schutzmechanismen adäquat eingesetzt werden. Unklarheiten oder vermutete Schwachstellen dienen dabei als Grundlage für die Generierung von Penetrationstests.

Zusätzlich muß in der Spezifikation begründet sein, warum die Sicherheitsfunktionen von nicht zu evaluierenden Systemteilen nicht umgangen werden können. Es muß klar erkennbar sein, daß nur die zur Evaluation vorgelegten Systemteile die zur Realisierung der Sicherheitsfunktionen benötigten Privilegien besitzen. Auch dies muß durch spezielle Penetrationstests bei der Evaluation untermauert werden.

Qualität des Herstellungsvorganges

Erläuterungen zu den Kriterien

Die Prüfung der Implementierungsqualität beschränkt sich auf die Durchführung von Tests aus der vom Auftraggeber bereitgestellten Testbibliothek und solchen, die bei der Prüfung der Sicherheitsanforderungen und der Spezifikation formuliert wurden. Diese Tests müssen ausreichend sein, zu zeigen, daß die in der Spezifikation aufgeführten Sicherheitsfunktionen vorhanden sind und entsprechend der Spezifikation und Dokumentation benutzt werden können.

Stichprobenartig sind außerdem durchzuführen:

- Benutzung der Sicherheitsfunktionen mit unzulässigen oder unsinnigen Parameterwerten.
- Suche nach nicht dokumentierten Funktionen (falls die Spezifikation deren Existenz vermuten läßt).
- Benutzung der Sicherheitsfunktionen mit Parameterwerten, die im Grenzbereich der zulässigen Parameterwerte liegen.

Werden dabei Widersprüche zur Spezifikation gefunden (dazu gehören auch Funktionen, die in der Spezifikation nicht erwähnt sind), so sind entweder die Spezifikation und, falls erforderlich, auch die Sicherheitsanforderungen oder aber die Implementierung so abzuändern, daß die Konsistenz zwischen Sicherheitsanforderungen, Spezifikation und Implementierung erreicht wird. Durch solche nachträglichen Korrekturen wird im allgemeinen der Evaluationsaufwand erhöht, da bereits geprüfte Teile nochmals untersucht werden müssen. Daher sollten solche Nachbesserungen nur in geringem Umfang zugelassen werden.

Betriebsqualität

Erläuterungen zu den Kriterien

Unter die Betriebsqualität fallen alle die Aspekte, die die Einhaltung der Sicherheitsanforderungen im laufenden Betrieb gewährleisten sollen. Diese Aspekte können je nach Art des IT-Systems sehr unterschiedlich sein. Auf der Grundlage der Sicherheitsanforderungen sind für das zu evaluierende System alle relevanten Bereiche festzulegen und zu prüfen.

Haben unterschiedliche Konfigurationen Auswirkungen auf die Sicherheitsanforderungen, so müssen diese auch in der Spezifikation der Sicherheitsfunktionen erkennbar sein. Zusätzlich sind alle Konfigurationsmöglichkeiten zu dokumentieren, um dem Anwender des Systems die Auswirkungen unterschiedlicher Konfigurationen transparent zu machen.

Es muß möglich sein, Eingriffe bei der Generierung des Systems zu protokollieren. Die Untäuschbarkeit der Protokollierung ist durch geeignete Tests nachzuprüfen. Um sicherzustellen, daß bei der Einspielung der Software keine unerkannten Übertragungsfehler auftreten, muß ein von der Evaluationsbehörde zugelassenes Verfahren eingesetzt werden, das derartige Fehler erkennen kann.

Hardware-Wartung und Änderungen an der Software der Sicherheitsfunktionen sind oft Bereiche, bei denen die volle Funktionalität der Sicherheitsfunktionen nicht kontinuierlich aufrecht erhalten werden kann. Bei der Evaluation des Systems sind auch diese Bereiche zu untersuchen und eventuell an Hand von speziell konstruierten Beispielen durchzuspielen. Als Ergebnis dieser Untersuchungen sollten organisatorische Maßnahmen vorgeschlagen werden, die auch im Wartungsfall noch ein Maximum an Sicherheit gewährleisten.

Für einige Hardware-Komponenten muß das System Selbsttesteinrichtungen besitzen, um ein korrektes Ablaufen der Sicherheitsfunktionen zu gewährleisten.

Qualität der anwenderbezogenen Dokumentation

Erläuterungen zu den Kriterien

Die Qualität der für den Anwender bestimmten Dokumentation wird am Ende der Evaluation bewertet. Das Evaluations-Team sollte zu diesem Zeitpunkt genügend Erfahrungen mit dem System gesammelt haben, um die Korrektheit, Verständlichkeit und Vollständigkeit dieser Dokumentation beurteilen zu können. Abweichungen zwischen dem realen Systemverhalten und der Dokumentation sind dem Auftraggeber bekannt zu geben. Dieser muß dann die Dokumentation nachbessern bevor die Zertifizierung erfolgt.

Qualitätsstufe Q3

Erläuterungen zu den Kriterien

Die Qualitätsstufe Q3 ist vorgesehen für Systeme bzw. Einzelkomponenten, an die mittlere Anforderungen bezüglich der Qualität der Erfüllung der Sicherheitsanforderungen gestellt werden. Ziel der Evaluation in die Qualitätsstufe Q3 ist es, durch Prüfung der Spezifikation und stichprobenhafte Prüfung der Implementierung nachzuweisen, daß das System weitgehend resistent gegen einfach geartete Penetrationsversuche ist. Systeme der Qualitätsstufe Q3 sind für Bereiche mit mittleren Anforderungen an das Vertrauen bezüglich der Einhaltung der Sicherheitsanforderungen in vielen Fällen ausreichend. Es bleibt ein mäßiges Restrisiko, daß durch gezielte Penetrationsversuche noch Schwachstellen im System gefunden werden können, durch die Sicherheitsfunktionen umgangen oder außer Kraft gesetzt werden können.

Qualität der Sicherheitsanforderungen

Erläuterungen zu den Kriterien

Auch für die Qualitätsstufe Q3 ist eine verbale Formulierung der Sicherheitsanforderungen noch ausreichend, jedoch kann die Benutzung semiformaler Darstellungsmethoden die Prüfung durch das Evaluations-Team erleichtern und damit auch verkürzen. Je nach Umfang der Sicherheitsanforderungen setzen sich mehrere Mitglieder des Evaluations-Teams eingehend mit diesem Dokument auseinander. Interpretationsschwierigkeiten sind mit dem Auftraggeber abzuklären.

Qualität der Spezifikation

Erläuterungen zu den Kriterien

Zur Erreichung der Qualitätsstufe Q3 ist eine detaillierte Spezifikation Voraussetzung, in der die Implementierung der Sicherheitsfunktionen sowie der sonstigen Software, die nicht oder nicht ausreichend von den Sicherheitsfunktionen abgegrenzt ist, beschrieben ist. Bei der Evaluation des Systems wird im wesentlichen diese Spezifikation untersucht und nur bei Unklarheiten oder vermuteten Schwachstellen der Quellcode der Implementierung hinzugezogen. Für größere Systeme ist die Verwendung graphischer Darstellungsmethoden zumindest für die höheren Abstraktionsebenen der Spezifikation sehr hilfreich. Da die Spezifikation noch verbal sein darf, ist die Aussagekraft einer solchen Prüfung noch schwach. Größere Designfehler sollten allerdings auch bei einer solchen Prüfung gefunden werden.

Qualität der verwendeten Mechanismen

Erläuterungen zu den Kriterien

Die Bewertung "stark" sollte die Minimalbewertung sein, die ein Mechanismus besitzen muß, der allein für die Erfüllung einer bestimmten Sicherheitsanforderung verantwortlich ist. Dies entspricht der Zielsetzung der Qualitätsstufe Q3, die ja bereits einen guten Schutz gegen einfach geartete Penetrationsversuche gewährleisten muß. Ein als "mittelstark" bewerteter Mechanismus sollte nur verwendet werden, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Der Mechanismus wird in Kombination mit anderen Mechanismen eingesetzt. Die Kombination dieser Mechanismen ist mit "stark" oder besser bewertet worden.
- Der Aufwand für die Verwendung eines stärkeren Mechanismus steht nach übereinstimmender Auffassung von Auftraggeber und Evaluations-Team in keinem vertretbarem Verhältnis zu den dadurch entstehenden Kosten.

Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen

Erläuterungen zu den Kriterien

Auch bei der Prüfung der Abgrenzung zu den nicht zu evaluierenden Teilen des Systems sind bei der Generierung der Tests die unter der Qualitätsstufe Q2 angesprochenen Gesichtspunkte zu beachten. Zusätzlich ist für die Qualitätsstufe Q3 noch die Implementierung der Schnittstellen zu den nicht zu evaluierenden Teilen des Systems stichprobenartig auf Quellcode-Ebene zu überprüfen.

Qualität des Herstellungsvorganges

Erläuterungen zu den Kriterien

Für die Qualitätsstufe Q3 wird erstmals das Vorliegen des Quellcodes der Implementierung der Sicherheitsfunktionen verlangt. Daher werden auch erstmals Voraussetzungen an die Implementierungssprache(n) gemacht. Diese Voraussetzungen sind allerdings noch schwach. Es wird im wesentlichen verlangt, daß die zur Implementierung verwendeten Sprachen klar definiert sind. Das Evaluations-Team kann verlangen, daß der Auftraggeber die notwendige Dokumentation über die verwendeten Implementierungssprachen zur Verfügung stellt. Dies ist insbesondere dann erforderlich, wenn eine nicht allgemein verfügbare Sprache bei der Implementierung verwendet wurde. Dies gilt auch für Preprozessoren oder andere Hilfsmittel, die bei der Codegenerierung eingesetzt wurden.

Die Penetrationstests werden in etwa nach den gleichen Kriterien wie für die Qualitätsstufe Q2 ausgewählt, allerdings sind bei einer Evaluation in die Qualitätsstufe Q3 auch Unklarheiten oder vermutete Schwachstellen mit einzubeziehen, die sich bei der (stichprobenartigen) Prüfung des Quellcodes der Implementierung ergaben. Bedingt durch die sorgfältigere Prüfung der Spezifikation werden diese Tests im allgemeinen wesentlich zielgerichteter sein. Eine Evaluation in die Qualitätsstufe Q3 soll dem System ja eine weitgehende Resistenz gegen einfache Penetrationsversuche bescheinigen.

Zur Evaluation in die Qualitätsstufe Q3 muß der Auftraggeber eine der Größe der zu evaluierenden Systemteile entsprechende Bibliothek von Testprogrammen nebst zugehöriger Testdokumentation vorlegen. Diese Programme sollen so gestaltet sein, daß alle Sicherheitsfunktionen mit mehreren Parameterwerten getestet werden. Ebenso muß die Bibliothek Testfälle mit Grenzwerten der Parameter sowie Testfälle für ungültige Parameterwerte enthalten, durch die das Verhalten der Sicherheitsfunktionen in diesen Fällen stichprobenhaft geprüft werden kann. Die Bibliothek muß so gestaltet sein, daß es dem Evaluations-Team problemlos möglich ist, diese Testfälle nachzuvollziehen sowie leicht modifizierte Testfälle zu generieren und ablaufen zu lassen.

Die Voraussetzungen an die Implementierungsumgebung sind in der Qualitätsstufe Q3 noch relativ schwach. Es wird lediglich verlangt, daß Prozeduren zur Verfügung stehen, mit denen es dem Evaluations-Team ohne großen Aufwand möglich ist, alle zu evaluierenden Systemteile aus den Quellprogrammen zu generieren. Die Versions- und Änderungskontrolle kann z.B. daraus bestehen, daß bei einer Neugenerierung von Systemteilen lediglich solche Teile auch neu compiliert werden, bei denen seit der letzten Generierung eine Änderung erfolgt ist. Nur für große Systeme (dies wird im Einzelfall vom Evaluations-Team entschieden) muß der Hersteller die Rollentrennung im Software-Entwicklungsprozeß sowie ein kontrolliertes Integrations- und Abnahmeverfahren nachweisen. Dieser Nachweis kann durch Vorlage von Abnahmeprotokollen geschehen, aus denen die für die Implementierung (Codierung) sowie für die Abnahme der einzelnen Funktionseinheiten Verantwortlichen hervorgehen. Auch sollte aus diesen Protokollen hervorgehen, welche Tests aus der Testbibliothek für diese Funktionseinheit durchgeführt wurden, und wann die Abnahme und Integration erfolgte.

Betriebsqualität

Erläuterungen zu den Kriterien

In der Qualitätsstufe Q3 kommen lediglich die Forderung nach einem sicheren Anfangszustand nach einem Systemstart sowie die Protokollierung der Systemgenerierungsparameter hinzu. Damit soll verhindert werden, daß das System nach dem Start in einen Zustand gelangen kann, in dem Teile der Sicherheitsfunktionen außer

Kraft gesetzt sind. Dies darf höchstens in speziellen Wartungsfällen geschehen und muß protokollierbar sein. Andererseits soll durch die Protokollierung der Systemgenerierungsparameter dem Systemverantwortlichen die Möglichkeit gegeben werden, nachzuvollziehen, wie sein System generiert wurde. Dies ist insbesondere dann notwendig, wenn sich die Evaluation nur auf bestimmte Generierungen und Konfigurationen des Systems bezieht.

Qualität der anwenderbezogenen Dokumentation

Erläuterungen zu den Kriterien

Die Anforderungen an die anwenderbezogene Dokumentation sind identisch mit den in der Qualitätsstufe Q2 aufgestellten Anforderungen. Für die Evaluation gelten die dort niedergelegten Bemerkungen unverändert auch für die Qualitätsstufe Q3.

Qualitätsstufe Q4

Erläuterungen zu den Kriterien

Die Qualitätsstufe Q4 ist vorgesehen für Systeme bzw. Einzelkomponenten, an die mittlere bis gehobene Ansprüche bezüglich der Qualität der Erfüllung der Sicherheitsanforderungen gestellt werden. Bei einer Evaluation in diese Qualitätsstufe wird außer der Spezifikation auch der Quellcode der Implementierung in Stichproben analysiert, und es werden ausgefeilte Penetrationsversuche durchgeführt. Dadurch soll ein hohes Maß an Vertrauen gewonnen werden, daß das System auch in einer Umgebung, in der nicht unbedingt von einem gutartigen Benutzerverhalten ausgegangen werden kann, die an es gestellten Sicherheitsanforderungen erfüllt. Systeme der Qualitätsstufe Q4 sind daher für Bereiche mit mittleren bis gehobenen Ansprüchen an das Vertrauen in die Einhaltung der Sicherheitsanforderungen geeignet. Es bleibt ein kleines Restrisiko, daß durch ausgefeilte Penetrationsversuche noch Schwachstellen im System gefunden werden können, durch die Sicherheitsfunktionen umgangen oder außer Kraft gesetzt werden können.

Qualität der Sicherheitsanforderungen

Erläuterungen zu den Kriterien

Die dem zu evaluierenden System zugrundeliegende Sicherheitsphilosophie muß zur Erreichung der Qualitätsstufe Q4 deutlich detaillierter als bei der Qualitätsstufe Q3 dargelegt werden. Für jede der Sicherheitsanforderungen muß begründet werden, welchen Zweck sie in dem Gesamtsicherheitskonzept erfüllen soll, also insbesondere, welche Bedrohung durch diese Anforderung abgewehrt oder verringert werden soll. Außerdem muß bei den einzelnen Sicherheitsanforderungen erläutert werden, welche Bedrohungen bei der Erfüllung der Sicherheitsanforderungen insgesamt abgewehrt werden können. Dazu können graphische Darstellungen z.B. der Abhängigkeiten der einzelnen Sicherheitsfunktionen untereinander zum besseren Verständnis beitragen.

Qualität der Spezifikation

Erläuterungen zu den Kriterien

Die Verwendung semiformaler Hilfsmittel sowie die hierarchische Strukturierung der Spezifikation sollen dem Evaluations-Team ein besseres Verständnis für die verwendeten Algorithmen und Mechanismen sowie deren Zusammenwirken geben.

Die Spezifikation muß außerdem so gestaltet sein, daß das Evaluations-Team die Arbeitsweise einzelner Funktionen (wie z.B. die Identifikation und Authentisierung von Benutzern) nachvollziehen kann, d.h. daß für die Implementierung dieser

Funktion nach der vorliegenden Spezifikation keine großen Freiheiten mehr gegeben sind. Dadurch kann bereits in der Spezifikation detailliert nach Schwachstellen oder Widersprüchen gesucht werden. Dies ist deshalb besonders wichtig, da die Schwachstellenanalyse bei einer Evaluation in die Qualitätsstufe Q4 im wesentlichen eine sorgfältige Prüfung der Spezifikation umfaßt. Die Implementierung wird bei der Evaluation in diese Qualitätsstufe informell analysiert, wobei im wesentlichen Unklarheiten oder vermutete Schwachstellen, die sich bei der Prüfung der Spezifikation ergaben, die Grundlage für die Auswahl der Analysen bildet. Die Realisierung der Sicherheitsanforderungen wird im Quellcode nachvollzogen.

Qualität der verwendeten Mechanismen

Erläuterungen zu den Kriterien

Es muß aufgeschlüsselt sein, welche Bedrohung ein verwendeter Mechanismus abwehren soll. Dabei müssen alle in den Sicherheitsanforderungen aufgeführten Bedrohungen durch entsprechende Mechanismen abgedeckt werden. Jeder Mechanismus muß so beschrieben sein, daß eine Bewertung innerhalb der speziellen Metrik möglich ist. Diese Bewertung muß bei der Evaluation für jeden der verwendeten Mechanismen vorgenommen werden, wobei die in den IT-Sicherheitskriterien aufgeführten bzw. die bei vorangegangenen Evaluationen vorgenommenen Einstufungen von Mechanismen als Anhaltspunkte zu betrachten sind. Dabei ist die Bewertung "stark" die Minimalbewertung für einen Mechanismus.

Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen

Erläuterungen zu den Kriterien

Zur Erreichung der Qualitätsstufe Q4 muß die Abgrenzung zu nicht zu evaluierenden Systemteilen sehr sorgfältig durchgeführt werden. Alle Schnittstellen zu solchen Bereichen müssen sorgfältig auf Quellcode-Ebene geprüft werden. Hierbei ist insbesondere die Korrektheit und Vollständigkeit der Parameterprüfung zu betrachten. Dazu gehört auch eine Analyse, ob Parameter nach ihrer Prüfung auf Korrektheit eventuell noch von parallel laufenden, nicht vertrauenswürdigen Prozessen modifiziert werden können (Time-of-Check versus Time-of-Use (TOCTOU)-Problem). An die Qualität der Mechanismen zur Abgrenzung werden in Q4 höhere Anforderungen gestellt als in Q3. Für die Abgrenzungsmechanismen ist "sehr stark" die Minimalbewertung.

Qualität des Herstellungsvorganges

Erläuterungen zu den Kriterien

Wird kein offiziell geprüfter Compiler verwendet, muß das Evaluations-Team vom Auftraggeber die Bereitstellung einer Bibliothek mit Testprogrammen verlangen, mit deren Hilfe die korrekte Funktionalität des Compilers vom Evaluations-Team nachgeprüft werden kann. Diese Bibliothek von Testprogrammen sollte die möglichen Sprachkonstrukte möglichst weitgehend abdecken. Art und Umfang der Testprogramme können vom Evaluations-Team vorgeschrieben werden. Dem Evaluations-Team muß es möglich sein, für alle verwendeten Compiler eigene Tests durchzuführen.

Die Verwendung einer ungebräuchlichen Programmiersprache bei der Implementierung schränkt die Nachprüfbarkeit der Qualität durch das Evaluations-Team ein. Es kann nicht vorausgesetzt werden, daß im Evaluations-Team das notwendige Wissen in allen Programmiersprachen vorhanden ist. Deshalb ist es unerlässlich, daß ein Katalog von unterstützten Spezifikations- und Implementierungswerkzeugen (zu denen auch Programmiersprachen und Compiler zählen) herausgegeben wird. Es ist selbstverständlich, daß dieser Katalog im Laufe der Zeit Änderungen und Ergänzungen erfahren wird. Um Fehlinvestitionen bei einem Auftraggeber zu vermeiden, sollte in diesem Katalog für jedes Werkzeug angegeben sein, für welche Qualitätsstufen das Werkzeug geeignet ist und wie lange die Evaluationsbehörde dieses Werkzeug mindestens noch unterstützen wird.

Bei Verwendung von nicht in dem Katalog aufgeführten Werkzeugen kann das Evaluations-Team vom Auftraggeber verlangen, daß im Rahmen der Evaluation eine oder mehrere Personen des Evaluations-Teams in der Benutzung des Werkzeuges ausgebildet werden.

Wie bereits erwähnt, wird bei der Evaluation in die Qualitätsstufe Q4 eine informelle Analyse des Quellcodes verlangt. Die Auswahl der zu analysierenden Teile des Quellcodes bleibt dem Evaluations-Team überlassen und sollte sich im wesentlichen an Unklarheiten oder vermuteten Schwachstellen orientieren, die sich bei der Prüfung der Spezifikation ergaben. Allerdings muß sie sich nicht auf diese Bereiche beschränken. Bei allen Analysen ist vom Evaluations-Team zu prüfen, wie gut sich die Spezifikation auf den Quellcode abbilden läßt. Sind Teile, die untersucht werden sollen, im Quellcode nicht eindeutig lokalisierbar, oder ergibt die Prüfung Abweichungen zwischen Spezifikation und Quellcode, so kann keine Evaluation in die Klasse Q4 erfolgen.

Betriebsqualität

Erläuterungen zu den Kriterien

Die Prüfung der Auswirkungen unterschiedlicher Konfigurationen kann in den meisten Fällen nur stichprobenartig bis auf den Quellcode durchgeführt werden. Auch hierbei sollten Unklarheiten oder vermutete Schwachstellen, die sich bei der Prüfung der Spezifikation ergaben, die Grundlage für die Auswahl der Stichproben bilden.

Der Vorgang des Systemstarts sollte sorgfältig analysiert und getestet werden, damit sichergestellt ist, daß eine Außerkraftsetzung von Sicherheitsfunktionen durch spezielle Eingriffe während des Systemstarts nur in genau protokollierten Ausnahmefällen möglich ist. Diese Ausnahmefälle (z.B. spezielle Wartungsfälle) dürfen jedoch nur ein eingeschränkt funktionsfähiges System zur Verfügung stellen, bei dem eine manuelle Überwachung möglich ist. Die gleichen Einschränkungen müssen auch erfüllt sein, wenn in anderen Wartungsfällen Teile der Sicherheitsfunktionen außer Kraft gesetzt werden.

Qualität der anwenderbezogenen Dokumentation

Erläuterungen zu den Kriterien

Abweichungen zwischen Anwenderdokumentation und realem Systemverhalten deuten häufig auf Schwachstellen hin. Solche Abweichungen sollten daher ebenfalls stichprobenartig bis auf den Quellcode überprüft werden. Nach einer Klärung der Unstimmigkeiten muß das Evaluations-Team dem Auftraggeber die Chance zur Bereinigung der anwenderbezogenen Dokumentation geben.

Qualitätsstufe Q5

Erläuterungen zu den Kriterien

Die Qualitätsstufe Q5 ist vorgesehen für Systeme bzw. Einzelkomponenten, an die gehobene bis hohe Ansprüche bezüglich der Qualität der Erfüllung der Sicherheitsanforderungen gestellt werden. In dieser Qualitätsstufe wird erstmals die Vorlage eines formalen Sicherheitsmodells verlangt. Ziel der Evaluation ist es, durch sorgfältige Analyse von Spezifikation und Implementierung darzulegen, daß das System in hohem Maße resistent gegen Penetrationen ist. Systeme der Qualitätsstufe Q5 sind für Systeme mit gehobenen bis hohen Ansprüchen bezüglich des Vertrauens in die Erfüllung der Sicherheitsanforderungen geeignet.

Qualität der Sicherheitsanforderungen

Erläuterungen zu den Kriterien

Das formale Modell muß die vom Auftraggeber als wichtig erachteten Sicherheitsanforderungen in den Bereichen Vertraulichkeit und Integrität abdecken (sofern diese Aspekte bei den Sicherheitsanforderungen eine Rolle spielen). Der Aspekt der Verfügbarkeit ist im allgemeinen nur sehr schwer oder gar nicht formal erfaßbar. Daher kann ein formales Modell, welches alle Aspekte der Sicherheitsanforderungen abdeckt, hier nicht verlangt werden.

Die Konsistenzbeweise für das Modell müssen vom Auftraggeber bei Beginn der Evaluation dem Evaluations-Team zusammen mit den restlichen Dokumenten vorgelegt werden. Es kann vom Evaluations-Team nicht erwartet werden, daß es diese Beweise während der Evaluation erstellt. Ebenso sind dem Evaluations-Team alle bei der Erstellung der Beweise benutzten Hilfsmittel zur Verfügung zu stellen. Aufgabe des Evaluations-Teams ist es dann, die vorgelegten Beweise nachzuvollziehen und dadurch als korrekt zu akzeptieren. Außerdem sind die verbal formulierten Sicherheitsanforderungen, die ja im allgemeinen mehr abdecken als das formale Modell, sehr sorgfältig auf Konsistenz untereinander und mit dem Sicherheitsmodell zu untersuchen. Dabei sind die nicht durch das Modell abgedeckten Teile mit besonderer Sorgfalt zu prüfen.

Qualität der Spezifikation

Erläuterungen zu den Kriterien

Um die Umsetzung des Sicherheitsmodells in der Spezifikation mit adäquater Qualität nachvollziehen zu können, ist es unabdingbar, daß neben der verbalen Spezifikation auch eine Spezifikation in semiformaler Notation vorliegt. Die Spezifikationen

müssen hierarchisch strukturiert sein und in jeder Hierarchieebene in klar definierte, weitgehend unabhängige Funktionseinheiten untergliedert sein. Für die semiformale Spezifikation muß eine Sprache mit eindeutig definierter Syntax verwendet werden.

Alle im Sicherheitsmodell definierten Funktionen müssen sich in der Spezifikation lokalisieren lassen. Dazu ist es fast immer unabdingbar, daß diese auch in der Spezifikation wieder als Funktionseinheiten definiert sind.

Die in der obersten Hierarchieebene vorgenommene Strukturierung muß bis in die unterste Ebene beibehalten werden, d.h. sie darf immer nur "lokal" verfeinert werden, ohne daß sich Schnittstellen oder Verbindungen von bereits in der höheren Spezifikationsebene vorhandenen Funktionseinheiten bei der Verfeinerung verändern. Bei der Evaluation muß das Evaluations-Team die Spezifikation in allen Hierarchieebenen auf Konsistenz und Erfüllung der Sicherheitsanforderungen prüfen. Treten dabei Unklarheiten auf oder werden Schwachstellen vermutet, so müssen diese Fälle sorgfältig erfaßt werden, da dies Schwerpunkte bei der Prüfung der Implementierung sind.

Qualität der verwendeten Mechanismen

Erläuterungen zu den Kriterien

Für die Klasse Q5 werden stärkere Anforderungen an die Qualität der verwendeten Mechanismen gestellt als für die Klasse Q4. Bei der Bewertung der Mechanismen bzw. der Kombinationen von Mechanismen ist große Sorgfalt anzuwenden.

Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen

Erläuterungen zu den Kriterien

Die Prüfung der Abgrenzung zu nicht zu evaluierenden Systemteilen beinhaltet ab der Qualitätsstufe Q5 auch die Suche nach Nebeneffekten, die als verdeckte Kanäle mißbraucht werden können, d.h. durch die Informationen in einer Weise übertragen werden können, die im Gegensatz zu den Sicherheitsanforderungen steht. Dabei bilden verdeckte Kanäle nicht nur in Systemen eine Gefahr, in denen Informationen mit hierarchisch geordneten Einstufungen verarbeitet werden, sondern generell in allen Systemen, bei denen bestimmten Subjekten der lesende Zugriff zu bestimmten Informationen verwehrt werden soll. Solche verdeckten Kanäle können ja z.B. auch dazu mißbraucht werden, um in den Besitz von Authentisierungsinformationen zu gelangen, wie das folgende Beispiel zeigt:

Ein System verlangt zur Ausübung einer bestimmten Funktion die Übergabe eines korrekten Paßwortes. Das übergebene Paßwort wird intern byteweise mit dem korrekten Paßwort verglichen. Sobald Ungleichheit festgestellt wird, bricht die

Funktion ab und gibt den Fehlercode x an das aufrufende Programm zurück. Legt man nun das zu übergebende Paßwort so im Speicher ab, daß nur die ersten n Zeichen noch in einem Speicherbereich liegen, zu dem der Zugriff erlaubt ist, so kann man an Hand des Fehlercodes entscheiden, ob die ersten n Zeichen mit dem korrekten Paßwort übereinstimmen (sobald die Vergleichsfunktion auf das $(n+1)$ -te Zeichen zugreifen will, wird das Programm mit einem Fehlercode y für unerlaubten Speicherzugriff abgebrochen). Ist die Paßwortlänge z.B. 8 Zeichen und jedes Zeichen aus einem Alphabet aus 36 möglichen Zeichen, so erhält man durch diesen verdeckten Kanal das korrekte Paßwort im Mittel nach 144 statt 1.4×10^{12} Versuchen.

Dieses Beispiel zeigt auch deutlich, daß die Begrenzung der Bandbreite eines verdeckten Kanals in bestimmten Fällen nicht ausreichend ist. Im geschilderten Fall würde eine Begrenzung der Bandbreite des verdeckten Kanals auf 1 Bit/Sekunde lediglich bedeuten, daß es im Mittel 64 Sekunden dauert bis ein korrektes Paßwort ermittelt ist. Es versteht sich von selbst, daß ein solcher Kanal keinesfalls tolerierbar ist. Dies zeigt deutlich, daß die Bandbreite eines verdeckten Kanals nicht das einzige Kriterium sein kann, nach dem entschieden wird, ob ein solcher Kanal noch tolerierbar ist. Es muß zusätzlich sorgfältig geprüft werden, welche Art von Informationen über diesen Kanal übertragen werden kann, von welchen Subjekten der Kanal benutzt werden kann, wie groß der Aufwand zur Ausnutzung dieses Kanals ist und wie groß die Wahrscheinlichkeit ist, daß die Ausnutzung dieses Kanals nicht bemerkt wird. Die in den Kriterien angegebene maximale Bandbreite sollte für solche Kanäle gelten, die nicht ohne starke Einschränkungen der Systemverfügbarkeit oder der Systemfunktionalität beseitigt werden können. Das oben angeführte Beispiel ist dagegen ein verdeckter Kanal, der sich ohne großen Aufwand und ohne Einschränkung der Systemverfügbarkeit oder Systemfunktionalität beseitigen läßt.

Das Beispiel zeigt aber auch, an welchen Stellen an den Schnittstellen zu nicht zu evaluierenden Systemteilen verdeckte Kanäle auftreten können. Durch die Rückgabe eines Fehlercodes wird unter Umständen mehr an Information preisgegeben, als nach den Sicherheitsanforderungen notwendig und sinnvoll ist. Dies ist ein Bereich, der vom Evaluations-Team besonders sorgfältig zu analysieren ist.

Qualität des Herstellungsvorganges

Erläuterungen zu den Kriterien

Bei der Evaluation in die Qualitätsstufe Q5 muß vom Evaluations-Team auch der Quellcode der Implementierung vollständig analysiert werden. Eine stichprobenartige und informelle Kontrolle reicht hier nicht mehr aus. Bei der Prüfung ist dabei insbesondere das Zusammenwirken der einzelnen Funktionseinheiten und deren Schnittstellen untereinander zu untersuchen.

Unklarheiten oder vermutete Schwachstellen, die sich bei der Prüfung der Sicherheitsanforderungen, des Sicherheitsmodells, der Spezifikation und der Implementierung ergaben, sind Ausgangspunkte für gezielte Penetrationstests. Dabei können sich die Penetrationstests auch lediglich auf einzelne Funktionseinheiten (z.B. Module) beziehen, wobei bei der Wahl der Parameter beim Aufruf der Funktionseinheit nicht geprüft werden soll, ob diese Funktionseinheit im Gesamtsystem jemals mit den gewählten Parametern aufgerufen wird. Die Funktionseinheit muß sich bei allen Parameterwerten korrekt bezüglich ihrer Spezifikation bzw. bezüglich der Sicherheitsanforderungen verhalten, da ansonsten ein Fehlverhalten nach einer Quellcodeänderung nicht auszuschließen ist.

Der Einsatz eines Konfigurationsverwaltungs- und Kontrollsystems soll einerseits die Konsistenz des Objektcodes mit dem Quellcode sicherstellen, andererseits den Werdegang der Software nachvollziehbar machen. Daher die Forderung an die Protokollierungsmöglichkeiten dieses Systems und Trennung der einzelnen Rollen.

Betriebsqualität

Erläuterungen zu den Kriterien

Um den Nachweis der Erfüllung der Sicherheitsanforderungen auch im laufenden Betrieb in einer der Qualitätsstufe Q5 adäquaten Form durchführen zu können, darf die Konfigurierbarkeit nur einen sehr geringen Einfluß auf die Funktionalität besitzen. Dies läuft im allgemeinen darauf hinaus, daß bei der Konfiguration lediglich noch einige Konstanten undefiniert werden können, die Ablauflogik im wesentlichen jedoch erhalten bleibt.

Als neuer Punkt kommt ab der Qualitätsstufe Q5 die Forderung nach einer vertrauenswürdigen Software-Verteilung, die auch einen Schutz gegen absichtliche Manipulationen bieten soll. Hierzu werden im allgemeinen verschlüsselte Prüfsummen oder ähnlich geartete Verfahren eingesetzt, bei denen die Wahrscheinlichkeit für das Nichterkennen einer Manipulation, bei der der Manipulierende den verwendeten Schlüssel nicht kennt, sehr genau bestimmbar ist. Dabei ist ein von der Evaluationsbehörde zugelassener Weg bei der Software-Verteilung einzuhalten.

Die Anforderungen bezüglich der Wartung sind dahingehend verschärft, daß bei der Software-Wartung keine Einschränkungen der Sicherheitsfunktionen in Kauf genommen werden dürfen. Dies bedeutet, daß im Falle einer Änderung der Software der Sicherheitsfunktionen selbst das System in einen Zustand versetzt werden muß, in dem keine Bedrohungen von außen mehr wirksam sind. Dies bedeutet z.B., daß in einem solchen Fall kein Benutzer mehr am System arbeiten darf und alle Verbindungen nach außen unterbrochen sein müssen. Zusätzlich müssen

Prüfverfahren eingesetzt werden, die Manipulationen an der Software der Sicherheitsfunktionen beim Starten des Systems erkennen lassen.

Alle Forderungen an die Betriebsqualität müssen vom Evaluations-Team an exemplarischen Beispielen geprüft werden, d.h. das Evaluations-Team muß verschiedene Konfigurationen durchspielen (falls unterschiedliche Konfigurationen möglich sind), an einem Beispielfall die Wartung der Sicherheitssoftware durchexerzieren und Systemabstürze herbeiführen oder simulieren, um das sichere Wiederaufsetzen nach solchen Fehlern zu testen. Dabei soll das Evaluations-Team als *Advocatus Diaboli* durchaus durch gezieltes Fehlverhalten versuchen, die Sicherheitsfunktionen des Systems zu überlisten.

Qualität der anwenderbezogenen Dokumentation

Erläuterungen zu den Kriterien

Die Anforderungen an die anwenderbezogene Dokumentation sind gegenüber der Qualitätsstufe Q4 gleichgeblieben. Bei Unstimmigkeiten ist dem Auftraggeber eine angemessene Frist zur Nachbesserung zu gewähren.

Qualitätsstufe Q6

Erläuterungen zu den Kriterien

Die Qualitätsstufe Q6 ist vorgesehen für Systeme bzw. Einzelkomponenten, an die hohe bis sehr hohe Ansprüche bezüglich der Qualität der Erfüllung der Sicherheitsanforderungen gestellt werden. Zur Erlangung dieser Qualitätsstufe muß formal bewiesen werden, daß die oberste Hierarchieebene der Spezifikation alle Forderungen des formalen Sicherheitsmodells erfüllt. Außerdem wird der Quellcode sehr genau analysiert. Ziel der Evaluation in die Qualitätsstufe Q6 ist es, ein sehr hohes Maß an Vertrauen zu gewinnen, daß das System die an es gestellten Sicherheitsanforderungen erfüllt und in sehr hohem Maße resistent gegen Penetrationsversuche ist. Systeme der Qualitätsstufe Q6 sind für Systeme mit hohen bis sehr hohen Ansprüchen bezüglich der Qualität der Erfüllung der Sicherheitsanforderungen geeignet.

Qualität der Sicherheitsanforderungen

Erläuterungen zu den Kriterien

Das formale Sicherheitsmodell muß zur Erreichung der Qualitätsstufe Q6 umfassender sein als in den niedrigeren Qualitätsstufen. Alle Sicherheitsanforderungen in den Bereichen Vertraulichkeit und Integrität müssen durch das Sicherheitsmodell abgedeckt sein. Lediglich der sehr schwer formal zu fassende Aspekt der Verfügbarkeit darf ausgeklammert werden. Allerdings müssen die Auswirkungen der nicht im formalen Modell erfaßten Teile der Sicherheitsanforderungen auf das formale Modell sehr genau analysiert werden. Diese Auswirkungen dürfen nicht gegen die im formalen Modell formulierten Axiome verstoßen.

Qualität der Spezifikation

Erläuterungen zu den Kriterien

Zur Erreichung der Qualitätsstufe Q6 ist es notwendig, daß formal bewiesen wird, daß zumindest die oberste Hierarchieebene der Spezifikation dem formalen Sicherheitsmodell genügt. Dazu ist es unabdingbar, daß dieser Teil der Spezifikation in einer formal definierten, auf mathematischer Logik basierenden Spezifikationsprache niedergelegt ist. Um den Konsistenzbeweis zwischen Modell und Spezifikation führen zu können, ist es zumindest erforderlich, daß die Sprache, in der das Modell niedergelegt wurde und die verwendete Spezifikationsprache sorgfältig aufeinander abgestimmt sind. In den meisten Fällen wird es sogar die gleiche Sprache sein.

Die zum Beweis der Konsistenz von Modell und Spezifikation aufzustellenden Verifikationsbedingungen können bei nicht-trivialen Systemen kaum ohne maschinelle Hilfsmittel aufgestellt und bewiesen werden.

Zumindest ist es dem Evaluations-Team nicht möglich, ohne solche Hilfsmittel die Vollständigkeit der Verifikationsbedingungen nachzuvollziehen. Auch die Einzelbeweise sind meistens so umfangreich, daß sie nicht mit der erforderlichen Sorgfalt im Rahmen einer Evaluation nachvollzogen werden können, wenn keine maschinellen Hilfsmittel dazu zur Verfügung stehen.

Für die niedrigeren Hierarchieebenen der Spezifikation braucht zwar keine formale Verifikation auf Konsistenz mit der höchsten Spezifikationsebene durchgeführt zu werden, jedoch müssen auch diese Ebenen in der gleichen Spezifikationssprache niedergelegt sein, und die Art der Abbildung von einer Hierarchieebene auf die nächstniedrigere muß formal beschrieben sein. Dadurch wäre theoretisch die Möglichkeit einer Verifikation bis auf die niedrigste Hierarchieebene der Spezifikation möglich, doch wird zur Erreichung der Qualitätsstufe Q6 nicht verlangt, daß dies auch durchgeführt worden ist. Hier genügt eine sorgfältige, nicht formale Prüfung der Konsistenz bis auf die niedrigste Hierarchieebene der Spezifikation. Die Erfüllung der Sicherheitsanforderungen wird bis auf den Quellcode nachvollzogen.

Qualität der verwendeten Mechanismen

Erläuterungen zu den Kriterien

In Abstimmung mit der Zielrichtung der Qualitätsstufe Q6 ist "sehr stark" die minimale Bewertung, die ein Mechanismus bei Systemen dieser Stufe noch besitzen darf. Dies schließt im allgemeinen aus, daß zur Wirksamkeit des Mechanismus noch größere organisatorische Maßnahmen erforderlich sind. Im allgemeinen ist es auch sehr schwer, einen schwächer bewerteten Mechanismus ohne größere Designänderungen zu einem "sehr starken" Mechanismus zu machen. Falls also im Laufe der Evaluation festgestellt wird, daß ein Mechanismus nicht die geforderte Stärke besitzt, sollte in einer Diskussion mit dem Auftraggeber geklärt werden, ob der Mechanismus so abgeändert werden kann, daß er die erforderliche Bewertung erreicht, ob die Evaluation abgebrochen wird, oder ob eine niedrigere Qualitätsstufe angestrebt werden soll.

Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen

Erläuterungen zu den Kriterien

Bei einer Evaluation in die Qualitätsstufe Q6 ist die Analyse der Schnittstellen zu den nicht zu evaluierenden Systemteilen mit besonderer Sorgfalt auf Maschinenebene durchzuführen. Mit ausgefeilten Penetrationstests soll versucht werden, diese Schnittstellen zu Aktionen zu mißbrauchen, mit denen Sicherheitsfunktionen umgangen oder außer Kraft gesetzt werden. Bei diesen Tests sollte auch ein Maschinencode-Debugger verwendet werden. Jede so gefundene Lücke muß geschlossen werden, da eine bekannte Lücke des Systems eine Evaluation in eine andere Qualitätsstufe außer der Stufe Q0 ausschließt.

Ab dieser Qualitätsstufe wird die maximale Bandbreite von verdeckten Kanälen stark eingeschränkt.

Qualität des Herstellungsvorganges

Erläuterungen zu den Kriterien

Zur Erreichung der Qualitätsstufe Q6 ist eine sorgfältige Analyse des Quellcodes der Implementierung erforderlich. Eine solche Analyse kann jedoch nur noch von Personen mit fundierter Erfahrung in der Anwendung der verwendeten Implementierungssprachen durchgeführt werden. Dies schränkt die anwendbaren Programmiersprachen auf solche ein, die von der Evaluationsbehörde zugelassen sind, d.h. auf die, für die entsprechendes Know-How bei den Evaluationsstellen vorhanden ist. Die Behörde wird daher in regelmäßigen Abständen eine Liste der bei einer Evaluationen zugelassenen Programmiersprachen sowie eventuell sogar der anwendbaren Compiler veröffentlichen.

Ab der Qualitätsstufe Q6 umfaßt die Evaluation auch eine stichprobenartige Analyse des Maschinencodes. Hier wird insbesondere die Abbildbarkeit des Quellcodes auf den Maschinencode betrachtet. Diese Prüfung sollte sich besonders auf die Stellen erstrecken, bei denen compilerinterne Mechanismen (wie z.B. die Art der Parameterübergabe an Unterprogramme, die Art der Typprüfung, die Art der Prüfung auf Bereichsüberschreitung oder die Fehlerbehandlung) unter Umständen Möglichkeiten zur Penetration des Systems ergeben oder zur Eröffnung von verdeckten Kanälen führen können. Dazu sind ein Quellcode-Debugger und ein Maschinencode-Debugger zur Verfügung zu stellen. Dies impliziert, daß diese Bereiche (die sich auch teilweise auf das Laufzeitsystem des Compilers erstrecken) genau dokumentiert sein müssen.

Die Entwicklung und Wartung des Systems muß durch ein Konfigurationsverwaltungs- und Versionskontrollsystem überwacht werden. Modifikationen an Objekten, die der Kontrolle dieses Systems unterliegen, müssen protokolliert werden.

Betriebsqualität

Erläuterungen zu den Kriterien

Zur Erreichung der Qualitätsstufe Q6 ist eine sehr sorgfältige Analyse aller möglichen Konfigurationen sowie deren Auswirkungen auf die Sicherheitsanforderungen erforderlich. Dies bedeutet einen enormen Aufwand, wenn viele Konfigurationsmöglichkeiten vorhanden sind. Daher wird der Auftraggeber im allgemeinen nur bestimmte dieser Konfigurationsmöglichkeiten evaluieren lassen (unter Umständen auch nur eine einzige). Dies ist ohne weiteres möglich, jedoch müssen dann im Evaluationsbericht diese Konfigurationen beschrieben sein. Die Evaluation gilt dann nur für diese geprüften Konfigurationen. Durch autorisierte Rollen muß die aktuelle Konfiguration des Systems jederzeit während des laufenden Betriebs feststellbar sein.

Für die Verteilung der Software muß ein von der Evaluationsbehörde zugelassener Weg eingehalten werden. Sind auf diesem Weg nicht vertrauenswürdige Stationen, so muß sichergestellt sein, daß an diesen Stationen keine Manipulationen sowohl an der Software als auch an dem Speichermedium vorgenommen werden können.

Werden bei Hardware-Wartungen Sicherheitsfunktionen außer Kraft gesetzt, so darf eine Hardware-Wartung nur mit dem expliziten Einverständnis des Systemverwalters möglich sein.

Qualität der anwenderbezogenen Dokumentation

Erläuterungen zu den Kriterien

Die Anforderungen an die anwenderbezogene Dokumentation haben sich gegenüber der Qualitätsstufe Q5 nicht verändert. Bei Unstimmigkeiten zwischen dem realen Systemverhalten und der Anwenderdokumentation ist dem Auftraggeber eine angemessene Frist zur Nachbesserung zu gewähren.

Qualitätsstufe Q7

Erläuterungen zu den Kriterien

Die Qualitätsstufe Q7 ist vorgesehen für Systeme bzw. Einzelkomponenten, an die sehr hohe Ansprüche bezüglich der Qualität der Erfüllung der Sicherheitsanforderungen gestellt werden. Zur Erlangung dieser Qualitätsstufe muß formal bewiesen werden, daß alle Hierarchieebenen der Spezifikation und der Quellcode der Implementierung konsistent mit dem formalen Sicherheitsmodell sind. Ziel der Evaluation in die Qualitätsstufe Q7 ist es, ein sehr hohes Maß an Vertrauen zu gewinnen, daß das System die an es gestellten Sicherheitsanforderungen erfüllt und in sehr hohem Maße resistent gegen Penetrationsversuche ist. Der Aufwand zur Erstellung und Evaluation eines solchen Systems ist so hoch, daß diese Qualitätsstufe mit heutigen technischen Mitteln nur für sehr kleine Systeme bzw. Einzelkomponenten mit einfacher Struktur realisierbar ist.

Qualität der Sicherheitsanforderungen

Erläuterungen zu den Kriterien

Zur Erreichung der Qualitätsstufe Q7 ist ein formales Modell der Sicherheitsanforderungen erforderlich, welches alle Sicherheitsanforderungen vollständig erfaßt und abdeckt. Dies bedeutet, daß an ein solches System keine Sicherheitsanforderungen gestellt werden dürfen, die nicht in einem formalen Modell erfaßbar sind. Dies allein schränkt die Systeme, die mit heutigen technischen Mitteln in die Qualitätsstufe Q7 evaluiert werden können bereits deutlich ein.

Qualität der Spezifikation

Erläuterungen zu den Kriterien

Zur Erreichung der Qualitätsstufe Q7 muß der Beweis der Konsistenz von formalem Sicherheitsmodell und Spezifikation bis auf die unterste Hierarchieebene der Spezifikation durchgeführt werden. Nur so ist dann durch Beweis der Konsistenz von niedrigster Hierarchieebene der Spezifikation und Quellcode eine Codeverifikation sinnvoll. Bis auf den Quellcode wird bewiesen, daß die Sicherheitsanforderungen erfüllt sind. Dies setzt ebenso wie bei der Qualitätsstufe Q6 voraus, daß nur die von der Evaluationsbehörde zugelassenen Methoden und Werkzeuge verwendet wurden. Anderenfalls ist es dem Evaluations-Team nicht möglich, die Vollständigkeit und Korrektheit der vom Auftraggeber gelieferten Beweise nachzuvollziehen.

Qualität der verwendeten Mechanismen

Erläuterungen zu den Kriterien

Entsprechend dem Qualitätsanspruch der Klasse Q7 können hier nur noch nach heutigem Stand der Technik mit "nicht überwindbar" bewertete Mechanismen zum Einsatz kommen. Mit "sehr stark" bewertete Mechanismen sollten nur dort verwendet werden, wo mit heutigen technischen Mitteln kein als "nicht überwindbar" einzustufender Mechanismus realisierbar ist.

Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen

Erläuterungen zu den Kriterien

Die einzigen Unterschiede zur Qualitätsstufe Q6 sind die höhere Anforderung an die Qualität des Abgrenzungsmechanismus und die weitere Beschränkung der maximal erlaubten Bandbreite eines verdeckten Kanals. Bei der Prüfung dieses Teils der Sicherheitsanforderungen kommen gegenüber der Qualitätsstufe Q6 keine weiteren Aspekte hinzu.

Qualität des Herstellungsvorganges

Erläuterungen zu den Kriterien

Die gravierendsten Unterschiede zwischen den Qualitätsstufen Q6 und Q7 betreffen die Prüfung des Quellcodes der Implementierung. Damit eine Verifikation bis auf den Quellcode durchführbar ist, muß die verwendete Programmiersprache eine in allen Punkten formal definierte Semantik besitzen. Im allgemeinen können jedoch nicht alle Punkte der Semantik unabhängig von der Ziel-Hardware definiert werden. Daher die Forderung, daß solche Punkte dann in der Dokumentation des verwendeten Compilers formal definiert sein müssen. In der Qualitätsstufe Q7 muß auch der erzeugte Maschinencode sorgfältig analysiert werden. Damit die Abbildung zwischen dem Quellcode und dem Maschinencode manuell mit der erforderlichen Exaktheit nachvollziehbar ist, darf der Compiler keine komplexen Optimierungen durchführen. Auch die Maschinensprache der verwendeten Ziel-Hardware muß weitgehend formal definiert sein. Auch sollte der Compiler einen Ausdruck erzeugen können, welcher Quellcode und erzeugten Maschinencode in einer Form darstellt, der eine schnelle und eindeutige Zuordnung zwischen diesen beiden ermöglicht.

Alle Testbeispiele aus der Testbibliothek werden nachvollzogen und müssen die dokumentierten Ergebnisse liefern. Auch die Suche nach verdeckten Kanälen muß mit äußerster Sorgfalt durchgeführt werden.

Falls ein gefundener verdeckter Kanal nicht beseitigt werden kann, muß sorgfältig analysiert werden, in welcher Form er ausgenutzt werden kann und welche Art von Informationen über diesen Kanal preisgegeben werden könnten. Es ist sorgfältig abzuwägen, ob die Existenz eines solchen Kanals noch eine Einstufung in die Qualitätsstufe Q7 erlaubt.

An der Entwicklung und Wartung solcher Systeme darf nur überprüfetes Personal mitarbeiten.

Betriebsqualität

Erläuterungen zu den Kriterien

Der einzige wesentliche Unterschied zu den Kriterien für die Qualitätsstufe Q6 sind die gezielten Tests der Recovery-Prozeduren. Dazu soll das Evaluations-Team gezielt versuchen, bestimmte Fehler, die zu einem Systemabsturz führen können herbeizuführen oder zu simulieren. Auch gehören die Recovery-Programme dann zum zu evaluierenden Teil des Systems, wenn sie bestimmte Sicherheitsfunktionen umgehen oder außer Kraft setzen (was bei Recovery-Programmen sehr häufig der Fall ist). Dies bedeutet, daß verifiziert werden muß, daß diese Programme korrekt bezüglich ihrer Spezifikation sind, und daß sich das System nach Ablauf dieser Programme wieder in einem sicheren Zustand befindet.

Zusätzlich müssen mit gezielten Tests die Selbsttesteinrichtungen des Systems für alle Hardware-Komponenten überprüft werden, da sie ja das korrekte Ablaufen der Sicherheitsfunktionen gewährleisten sollen.

Qualität der anwenderbezogenen Dokumentation

Erläuterungen zu den Kriterien

In diesem Bereich sind in der Qualitätsstufe Q7 keine neuen Kriterien hinzugekommen.

4. Erläuterungen zu den geforderten Dokumenten

Die folgenden Erläuterungen sollen einen Überblick darüber geben, was in den Dokumenten, die in der Beschreibung der einzelnen Qualitätsstufen gefordert werden, stehen muß. Der tatsächliche Inhalt (Umfang und Detaillierungsgrad) dieser Dokumente hängt stark von dem zu evaluierenden System und von der angestrebten Qualitätsstufe ab.

Es ist nicht notwendig, daß alle zu einem Thema oder zu einem bestimmten Teilaspekt gehörenden Beschreibungen auch tatsächlich in einem einzigen Dokument zu finden sind. Verweise auf andere Dokumente sind zulässig, wobei darauf zu achten ist, daß die Lesbarkeit von Dokumenten nicht unter zu vielen Verweisen leiden darf.

Generell gilt, daß das Evaluations-Team in allen Zweifelsfällen über die Zulässigkeit von Darstellungsart, Inhalt und Verständlichkeit bzw. Nachvollziehbarkeit von Dokumenten entscheidet.

Hier werden vorerst nur Erläuterungen zu den Forderungen in den Qualitätsstufen Q1 bis Q3 gegeben. In den höheren Qualitätsstufen gelten diese Erläuterungen ebenfalls, zum Teil sind dann aber strengere Forderungen zu berücksichtigen (detailliertere Darstellung, Darstellung in semiformalen oder formaler Notation, usw.). Genauere Erläuterungen zu den Forderungen ab der Qualitätsstufe Q4 werden in einer zukünftigen Fassung des IT-Evaluationshandbuches gegeben.

In den IT-Sicherheitskriterien werden für eine Evaluation in eine der Qualitätsstufen Q1 bis Q3 die folgenden Dokumente gefordert:

- Beschreibung der Sicherheitsanforderungen,
- Spezifikation der zu evaluierenden Systemteile,
- Beschreibung der Abgrenzung zu nicht zu evaluierenden Systemteilen und der Schnittstellen zu diesen Teilen,
- Dokumentation für den Anwender, d.h.
 - Beschreibung der Anwendung der Sicherheitsfunktionen, aufgeteilt nach den in den Sicherheitsanforderungen festgelegten Rollen,
 - Beschreibung der sicherheitsrelevanten Aspekte bei Systemgenerierung, Systemstart, Systemverwaltung und Systemwartung,
- Beschreibung der verwendeten Hard- und Firmware mit Darlegung der Funktionalität der in Hardware bzw. Firmware realisierten Schutzmechanismen,
- Testdokumentation (ab Q2).

4.1 Beschreibung der Sicherheitsanforderungen

Was sind Sicherheitsanforderungen ?

Die Sicherheitsanforderungen legen fest, welche Sicherheitsfunktionen von einem IT-System gefordert werden. Sie bilden somit die Grundlage für die Evaluation, bei der geprüft wird, ob die Sicherheitsfunktionen des IT-Systems die Sicherheitsanforderungen erfüllen.

Normalerweise hat ein System noch weitere Funktionen. Wenn diese Funktionen aber in den Sicherheitsanforderungen nicht als sicherheitsrelevant gekennzeichnet werden, so werden sie auch nicht geprüft, sofern sie nicht irgendwelche Auswirkungen auf die zu evaluierenden Systemteile haben.

Die Sicherheitsanforderungen werden normalerweise vom Hersteller eines Systems formuliert. Da es aber auch möglich ist, daß ein Anwender die Evaluation eines Systems in Auftrag geben kann, ist es denkbar, daß der Anwender die Sicherheitsanforderungen definiert und damit festlegt, welche Funktionalität des Systems im Sinne seiner Sicherheitsanforderungen geprüft werden soll.

Erläuterungen zu den Forderungen in den IT-Sicherheitskriterien:

In den Sicherheitsanforderungen muß beschrieben sein, welche Sicherheitsfunktionen und -teilkfunktionen ein System oder eine Einzelkomponente beinhaltet.

Ein Verweis auf eine bestimmte Funktionalitätsklasse reicht nicht aus, sondern die Beschreibung muß detaillierter sein.

Beispiel: In F2 wird verlangt, daß das System Zugriffsrechte zwischen Subjekten und Objekten verwalten muß. Damit ist aber noch keine Aussage darüber gemacht, welche Objekte nun tatsächlich der Rechteverwaltung unterliegen (z.B. Volumes, Dateien, Bibliothekselemente, Records, usw.). Die genaue Aufzählung der zu schützenden Objekte muß deshalb in den Sicherheitsanforderungen erfolgen.

Eine detailliertere Beschreibung der Sicherheitsanforderungen ist auch deshalb erforderlich, weil ein System nicht notwendigerweise die Anforderungen genau einer oder mehrerer Funktionalitätsklassen erfüllen muß. Es ist auch möglich, daß ein System nur ganz bestimmte Sicherheitsanforderungen erfüllt, die in dieser Kombination in keiner der bisher definierten Funktionalitätsklassen enthalten sind, oder daß es die Anforderungen einer oder mehrerer Funktionalitätsklassen und zusätzlich einige weitere Sicherheitsanforderungen erfüllt.

Ab Q2 muß aus den Sicherheitsanforderungen hervorgehen, welche Bedrohung bzw. welche Bedrohungen mit den einzelnen Sicherheitsfunktionen abgewehrt werden soll,

und zu welcher Grundfunktion (Identifikation und Authentisierung, Rechteverwaltung, usw.) bzw. zu welchen Grundfunktionen die einzelnen Sicherheitsfunktionen gehören.

Es bleibt dem Hersteller überlassen, welche Darstellungsform er wählt (Strichaufzählung, verbale Beschreibung, Graphik). Es muß jedoch erkennbar sein, welche Sicherheitsanforderungen erfüllt werden.

4.2 Spezifikation der zu evaluierenden Systemteile

Was ist eine Spezifikation ?

Eine Spezifikation muß die Realisierung der zu evaluierenden Systemteile eines IT-Systems vollständig, verständlich und nachvollziehbar beschreiben.

Bei komplexen Systemen muß diese Beschreibung aus mehreren Beschreibungsebenen (Hierarchiestufen) aufgebaut sein, da die zu evaluierenden Systemteile nur auf diese Art und Weise ausreichend verständlich und nachvollziehbar spezifiziert werden können. Im Zweifelsfall entscheidet das Evaluations-Team über eine notwendige Mehrstufigkeit der Beschreibung. In der obersten Beschreibungsebene wird allgemein das "was" und das "wo" stehen (z.B. Funktionsbeschreibung, Zerlegung des Systems in einzelne Funktionen, usw.), in weiteren Stufen wird diese grobe Beschreibung gemäß den Definitionen im Duden-Fremdwörterbuch ^{<2>} verfeinert (zergliedert) werden, d.h. hier wird dann das "wie" beschrieben (z.B. Algorithmen, Kontrollfluß, Daten, Details der Implementierung usw.).

Die Bezeichnungen für die einzelnen Beschreibungsebenen der Spezifikation sind nicht genormt. Es wird nicht einmal der Begriff "Spezifikation" einheitlich angewendet.

^{<2>} Duden-Fremdwörterbuch

Spezifikation:

1. Einteilung der Gattung in Arten.
2. Einzelaufzählung.

spezifizieren:

1. einzeln aufführen, verzeichnen.
2. zergliedern.

Die oberste Beschreibungsebene wird manchmal in Anlehnung an die IEEE-Definitionen ^{<3>} auch "Design", die unterste Ebene (und die mittleren, falls solche existieren) "Designspezifikation" genannt.

In den IT-Sicherheitskriterien wird unter "Spezifikation" die Beschreibung der zu evaluierenden Teile des Systems über alle Hierarchiestufen verstanden.

Es ist nicht notwendig, daß für die verschiedenen Beschreibungsebenen der Spezifikation jeweils verschiedene Dokumente existieren, solange es möglich ist, die Informationen, die zu den einzelnen Beschreibungsebenen gehören, herauszufiltern. Über die Zulässigkeit der Darstellung entscheidet wiederum das Evaluations-Team. Unter der gleichen Voraussetzung ist auch die strikte Trennung zwischen "was" und "wo" (Design) auf der einen Seite und "wie" (Designspezifikation) auf der anderen Seite nicht zwingend erforderlich. Eine den obigen Definitionen folgende Gliederung der Dokumentation wird jedoch im allgemeinen die Verständlichkeit verbessern und somit die Nachprüfbarkeit erleichtern.

Erläuterungen zu den Forderungen in den IT-Sicherheitskriterien:

Inhalt und Umfang der Spezifikation sind von der angestrebten Qualitätsstufe und von der Komplexität des zu evaluierenden Systems abhängig. Somit ist die Formulierung in Q2 und Q3: "Falls die Spezifikation hierarchisch aufgebaut ist, ..." folgendermaßen zu verstehen:

Ein IT-System ist meistens zu komplex, als daß es möglich wäre, es mit nur einer Hierarchiestufe der Spezifikation so genau zu beschreiben, daß die Abbildung

^{<3>} IEEE Std 729-1983

Design:

The process of defining the software architecture, components, modules, interfaces, test approach, and data for a software system to satisfy specified requirements.

The result of a design process.

Design specification:

A specification that documents the design of a system or system component; for example a software configuration item. Typical contents include system or component algorithms, control logic, data structures, data set-use information, input/output formats and interface descriptions.

Specification:

A document that prescribes, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or system component.

The process of developing a specification.

A concise statement of a set of requirements to be satisfied by a product, a material or process indicating, whenever appropriate, the procedure by means of which it may be determined whether the requirements given are satisfied.

zwischen Sicherheitsanforderungen und Quellcode (in Q3) nachvollziehbar ist. In solch einem Fall ist die Beschreibung in mehreren Hierarchiestufen zwingend erforderlich.

Die Beschreibung muß ausreichend viele Hierarchiestufen besitzen, so daß man daraus ein Verständnis für den Aufbau der Sicherheitsfunktionen und je nach angestrebter Qualitätsstufe auch für die internen Abläufe erhalten kann.

Auf der obersten Hierarchiestufe der Spezifikation muß allgemein die Funktionalität der zu evaluierenden Teile des IT-Systems beschrieben werden und welche Sicherheitsanforderungen auf welche Weise umgesetzt werden. Bei einem kleinen System oder einer kleinen Einzelkomponente können hier auch schon die verwendeten Algorithmen beschrieben werden, bei einem komplexeren System hat dies in einer niedrigeren Hierarchiestufe zu geschehen.

Es ist weiterhin zu beschreiben, wie die Verteilung der Sicherheitsfunktionen auf einzelne Funktionseinheiten des Systems vorgenommen wurde. "Funktionseinheiten" können je nach angestrebter Qualitätsstufe und je nach aktueller Hierarchieebene komplexe Teile des Systems sein, die eine Sicherheitsfunktion erbringen (Q1, Q2), oder auch Modulgruppen, Module, Prozeduren, Routinen, Elementarfunktionen usw., die nur Teilfunktionen erbringen (Q2, Q3).

Die Benutzeroberfläche und somit die Schnittstellen der Sicherheitsfunktionen nach außen sind vollständig zu beschreiben. Ab Q2 sind "Benutzer" auch interne Funktionseinheiten; d.h. auch die internen Schnittstellen der Funktionseinheiten untereinander müssen beschrieben werden.

Der Kontroll- und Datenfluß zwischen System und Umwelt und zwischen den einzelnen Funktionseinheiten ist genau zu beschreiben, ab Q3 bis auf die Ebene von Modulen, Prozeduren, Routinen, Elementarfunktionen.

Ab Q3 sind auch der Kontroll- und Datenfluß innerhalb der einzelnen Funktionseinheiten und deren interne Datenstrukturen so exakt zu beschreiben, daß eine Abbildung auf den Quellcode möglich ist.

Ab Q2 ist besonderes Gewicht auch auf die Beschreibung von Parametervalidierung, Privilegienprüfung und Fehlerbehandlung zu legen.

Es folgt eine stichpunktartige Aufzählung von Mindestanforderungen an eine Spezifikation. Die Anwendbarkeit der einzelnen Forderungen und der Detaillierungsgrad der Ausführungen ist abhängig von der zu beschreibenden Hierarchiestufe der Spezifikation und der angestrebten Qualitätsstufe. **Es wird noch einmal betont, daß in höheren Qualitätsstufen die Ausführungen detaillierter**

und genauer sein müssen, auch wenn keine zusätzlichen Forderungen gemacht werden.

Neben diesen Anforderungen an die Spezifikation können weitere Punkte für das Verständnis des Systems notwendig sein (z.B. spezielle Hardware-Beschreibungen, Besonderheiten der Implementierung, usw.). Das Evaluations-Team legt im Zweifelsfall fest, welche weiteren Teile der Spezifikation vorgelegt werden müssen.

Forderungen zu **Funktionalität und Struktur**

☞ Ab Q1:

Grundsätzlich: Die interne Struktur der zu evaluierenden Systemteile muß nur grob dargestellt werden.

- Beschreibung von Aufgabe und Wirkung jeder Funktionseinheit und ihres Beitrags zu den Sicherheitsfunktionen,
- Beschreibung von Zusammenwirken und Abhängigkeiten mehrerer Funktionseinheiten,
- Beschreibung des Ablaufs und der Algorithmen,
- Beschreibung der Implementierung der Sicherheitsfunktionen,
- Beschreibung von Randbedingungen, die für das Verständnis notwendig sind,
- Beschreibung der Prüfung von Sonderrechten und Privilegien,
- Beschreibung von Besonderheiten einzelner Funktionseinheiten, die in der Anwenderdokumentation erläutert werden müssen.

☞ Zusätzlich ab Q2:

Grundsätzlich: Die interne Struktur muß detailliert dargestellt werden.

- Beschreibung der Aufrufhierarchie,
- Beschreibung besonderer Eigenschaften der Funktionseinheiten (resident, reentrant, serial reusable, usw.),
- Beschreibung der verwendeten Serialisierungs- und Synchronisierungsmechanismen.

Forderungen zu **Daten und Parametern**

☞ Ab Q1:

- Beschreibung der benutzten Speicherbereiche und deren Attribute (z.B. Speicherschutzattribut).

☞ Zusätzlich ab Q2:

- Beschreibung der Parameterprüfung (Validierung) an Aufrufschnittstellen,

- Beschreibung globaler Datenstrukturen, die für das Verständnis wichtig sind.

☞ Zusätzlich ab Q3:

- Beschreibung lokaler (d.h. spezifisch für eine Funktionseinheit) und übergeordneter oder globaler Daten und deren Struktur
- Beschreibung der Zugriffe und der Zugriffsarten auf Datenstrukturen,
- Beschreibung der benutzten Zugriffswege (z.B. Verkettung) auf übergeordnete oder globale Datenstrukturen.

Forderungen zu **Schnittstellen**

☞ Ab Q1:

- Beschreibung der Aufrufschnittstellen und der übergebenen Daten,
- Beschreibung der notwendigen Privilegien des Aufrufers.

☞ Zusätzlich ab Q2:

- Beschreibung der internen Schnittstellen zwischen einzelnen Funktionseinheiten,
- Beschreibung der aufgerufenen Funktionseinheiten.

Forderungen zur **Fehlerbehandlung**

Es wird davon ausgegangen, daß das System Mechanismen enthält, die grobe interne Fehler (ungültiger Operationscode, Adressierung nicht vorhandener Speicherbereiche) abfangen können, ohne daß die Gesamtfunktionalität beeinträchtigt wird. Falls weitergehende Forderungen zur Fehlerüberbrückung und zur Gewährleistung der Funktionalität bestehen, so sind diese in den Sicherheitsanforderungen festzulegen.

☞ Ab Q1:

- Beschreibung der Fehlerbehandlung bei fehlerhaften Eingabeparametern,
- Beschreibung von Fehlern und Ereignissen, die nicht auftreten dürfen, und wie dies verhindert wird.

☞ Zusätzlich ab Q2:

- Beschreibung der Fehlerbehandlung bei internen Fehlern.

ACHTUNG:

Die vorstehend genannten Forderungen gelten nicht nur für Funktionseinheiten, die Beiträge zu Sicherheitsfunktionen leisten, sondern auch - soweit anwendbar - für alle Funktionseinheiten des IT-Systems, die von den die Sicherheitsfunktionen realisierenden Funktionseinheiten nicht ausreichend getrennt sind (siehe auch Kapitel 4.3).

4.3 Beschreibung der Abgrenzung zu den nicht zu evaluierenden Systemteilen und der Schnittstellen zu diesen Teilen

Warum muß die Abgrenzung beschrieben werden ?

Angenommen, eine Sicherheitsfunktion ist praktisch nicht überwindbar, es gibt jedoch einen Weg, das System unter Umgehung dieser Sicherheitsfunktion zu kompromittieren, so ist diese Sicherheitsfunktion praktisch wertlos.

Beispiel: Beim Zugriff auf eine Datei über deren Namen wird die Berechtigung des Zugreifers geprüft, es ist jedoch für bestimmte Benutzer unter Umgehung des evaluierten Systemteils auch möglich, die einzelnen Sektoren der Platte, auf der die Datei abgespeichert ist, direkt zu lesen, und somit natürlich auch die Informationen, die in dieser Datei stehen.

Dieses Beispiel verdeutlicht, warum bei einer Evaluation neben den Abgrenzungsmechanismen zur Systemumwelt auch die Abgrenzungsmechanismen zu den nicht zu evaluierenden Systemteilen überprüft werden müssen.

Für weitere Erläuterungen siehe auch Kapitel 5 (Erläuterungen zur Abgrenzung).

Erläuterungen zu den Forderungen in den IT-Sicherheitskriterien:

Die in Kapitel 4.2 aufgestellten Forderungen bezüglich der Spezifikation der zu evaluierenden Systemteile gelten sinngemäß auch für die die Abgrenzung realisierenden Mechanismen und die Schnittstellen zwischen zu evaluierenden und nicht zu evaluierenden Systemteilen.

Hierbei ist insbesondere darauf zu achten, daß die Beschreibung der Abgrenzungsmechanismen vollständig ist und daß erläutert wird, warum diese nicht umgangen werden können.

4.4 Dokumentation für den Anwender

Erläuterungen zu den Forderungen in den IT-Sicherheitskriterien:

Die hier aufgestellten Forderungen beziehen sich auf die die Sicherheit des Systems betreffenden Funktionen, wobei mit Anwender sowohl der normale Benutzer als auch der Systemverwalter gemeint ist.

Die Dokumentation muß jedem Anwender ein so ausführliches Wissen über die ihn betreffenden Sicherheitsfunktionen des IT-Systems vermitteln, daß er in der Lage ist, diese Sicherheitsfunktionen fehlerfrei anzuwenden.

Sämtliche Benutzerschnittstellen der Sicherheitsfunktionen müssen mit ihren Parametern beschrieben sein. Falls Abhängigkeiten zu anderen Funktionen bestehen, so müssen diese ebenfalls beschrieben sein. Insbesondere muß der Anwender auch auf eventuelle Konsequenzen z.B. bestimmter Parameterkombinationen hingewiesen werden, die vielleicht nicht auf den ersten Blick sichtbar sind.

In der entsprechenden Dokumentation muß auch auf Sicherheitsprobleme bei Generierung, Installation, Start, Wartung des Systems eingegangen werden.

4.5 Beschreibung der verwendeten Hard- und Firmware mit Darlegung der Funktionalität der in Hardware bzw. Firmware realisierten Schutzmechanismen

In den IT-Sicherheitskriterien werden zum Inhalt dieser Dokumente keine expliziten Forderungen gemacht.

Es gilt die allgemeine Philosophie der IT-Sicherheitskriterien, daß mit steigender Qualitätsstufe die Anforderungen an die Qualität und Ausführlichkeit der Darstellung zunehmen.

Erläuterungen zu den Forderungen in den IT-Sicherheitskriterien:

Die Beschreibung von Hardware und Firmware ist notwendig für das Verständnis der Spezifikation von hardware-nahen Systemteilen und auch für die Bewertung von Mechanismen und die Bewertung der Abgrenzung zu nicht zu evaluierenden Systemteilen (z.B. Speicherschutzmechanismen, Ringarchitektur). Sie muß deshalb die hierfür erforderlichen Informationen enthalten.

In vielen Fällen kann hier auf die entsprechende Dokumentation des Hardware-Herstellers zurückgegriffen werden.

Die Dokumentation muß mindestens enthalten:

☞ Ab Q1:

- Befehlssatz des Prozessors,
- Beschreibung der wichtigsten Architekturmerkmale (z.B. Systemzustände, Speicherschutz).

☞ Zusätzlich ab Q2:

- Beschreibung der Peripherieansteuerung für die wichtigsten Teile.

☞ Zusätzlich ab Q3:

- Vollständige Architekturbeschreibung,
- vollständige Beschreibung der Peripherieansteuerung.

4.6 Testdokumentation

Forderungen bezüglich der Testdokumentation sind im Abschnitt "Qualität des Herstellungsvorganges" zu finden.

Erläuterungen zu den Forderungen in den IT-Sicherheitskriterien:

In der Dokumentation zu den Systemtests müssen sämtliche Informationen stehen, die zum Nachvollzug der einzelnen Tests durch das Evaluations-Team notwendig sind, außerdem die bei der Testdurchführung erzielten Ergebnisse.

Alle Testprogramme bzw. Testprozeduren sowie deren Eingabedaten müssen zusätzlich auf Datenträgern zur Verfügung stehen. Die zu dokumentierenden Informationen und Daten sind im einzelnen mindestens:

- Hardware-Konfiguration (mit Versions-und Revisionsnummer),
- Software-Konfiguration (mit Versions-und Revisionsnummer),
- Testplan und Testziel,
- Vorgehensweise beim Test,
- Testprogramm oder Testprozedur (mit Versions-und Revisionsnummer),
- Eingabedaten für die Testprogramme oder die Testprozeduren,
- Besonderheiten und Abhängigkeiten,
- Testergebnis.

5. Erläuterungen zur Abgrenzung

Dieses Kapitel enthält Erläuterungen zu dem in den Qualitätsstufen aufgeführten Qualitätsaspekt "Qualität der Abgrenzung zu nicht zu evaluierenden Systemteilen".

Bei einer Evaluation wird zunächst davon ausgegangen, daß das zu evaluierende IT-System aufgeteilt werden kann in zu evaluierenden Systemteile und nicht zu evaluierenden Systemteile.

Dabei sind unter den zu evaluierenden Systemteilen alle die Teile des IT-Systems zu verstehen,

1. die Sicherheitsfunktionen realisieren,
2. die für Sicherheitsfunktionen notwendige Systemdienste erbringen,
3. die nicht ausreichend von 1. und 2. getrennt sind und
4. die Abgrenzungsmechanismen realisieren.

Die nicht zu evaluierenden Systemteile umfassen alle die Teile des IT-Systems,

die keine Sicherheitsfunktionen erbringen,

die an der Erbringung von Sicherheitsfunktionen nicht beteiligt sind,

die keine Abgrenzungsmechanismen realisieren und

die durch Abgrenzungsmechanismen ausreichend (dies ist abhängig von der angestrebten Qualitätsstufe) von den zu evaluierenden Systemteilen getrennt sind.

Am Anfang einer Evaluation ist im allgemeinen noch unklar, wie die genaue Aufteilung des IT-Systems in die zu evaluierenden und die nicht zu evaluierenden Systemteile ist. Deshalb ist zu Beginn einer Evaluation vom Hersteller des IT-Systems ein Dokument vorzulegen, indem beschrieben ist, wie aus der Sicht des Herstellers die zu evaluierenden Systemteile von den nicht zu evaluierenden Systemteilen getrennt sind, welche Abgrenzungsmechanismen dabei zum Einsatz kommen und welche Schnittstellen zu den nicht zu evaluierenden Systemteilen existieren. Aus diesem Dokument ergibt sich eine erste Aufteilung des IT-Systems. Die endgültige Aufteilung ergibt sich erst im Verlauf der Evaluation.

Ein wichtiges Kriterium bei der Bewertung der Qualität eines IT-Systems ist die Stärke der Abgrenzungsmechanismen. Im Verlauf der Evaluation wird untersucht,

- ob die Sicherheitsfunktionen, die durch die zu evaluierenden Systemteile realisiert werden sollen, von anderen Komponenten des Systems umgangen werden können,
- ob die Sicherheitsfunktionen von anderen Systemkomponenten getäuscht werden können und

- ob die Sicherheitsfunktionen von anderen Systemkomponenten in einer Weise mißbraucht werden können, die einen Verstoß gegen die Sicherheitsanforderungen darstellt.

Dabei wird sich in vielen Fällen herausstellen, daß es Teile des Systems gibt, die zwar nicht direkt zur Erfüllung der Sicherheitsanforderungen beitragen, jedoch von den Sicherheitsfunktionen nicht oder nicht ausreichend getrennt sind. Da nicht ausgeschlossen werden kann, daß diese Teile die Funktionalität der Sicherheitsfunktionen beeinflussen, sind diese Teile auch einer Evaluation zu unterziehen.

Beispiele für Abgrenzungsmechanismen:

1. Zustandswechsel in einem Betriebssystem

Ein Betriebssystem kennt zwei Systemzustände; einen nicht-privilegierten und einen privilegierten Systemzustand. Im nicht-privilegierten Zustand laufen alle Anwenderprogramme ab, während im privilegierten Zustand alle Betriebssystemfunktionen ablaufen. Das Umschalten zwischen den beiden Zuständen wird von der Software unterstützt durch die Hardware und Firmware abgewickelt.

Bei einem Wechsel vom nicht-privilegierten in den privilegierten Betriebssystemzustand wird zunächst der Kontext des aufrufenden Programms gesichert, bevor das aufrufende Programm, versehen mit einem neuen Kontext, die gewünschte Betriebssystemfunktion, unter der Kontrolle des Betriebssystems, ausführen kann. Nach jedem Zustandswechsel wird überprüft, ob das aufrufende Programm den Zustandswechsel überhaupt durchführen darf. Nach der Ausführung der aufgerufenen Betriebssystemfunktion wechselt das aufrufende Programm, initiiert durch das Betriebssystem, vom privilegierten zurück in den nicht-privilegierten Betriebssystemzustand. Dazu wird der ursprüngliche Kontext des aufrufenden Programms wieder zurückgeladen und das aufrufende Programm arbeitet nun wieder mit diesem Kontext weiter.

Bei älteren Prozessoren wird die Zustandsumschaltung überwiegend durch die Software realisiert, da diese Prozessoren im allgemeinen noch keine besondere Hardware-Unterstützung für einen Zustandswechsel anbieten. Bei neueren Prozessoren werden große Teile der Zustandsumschaltung bereits durch die Firmware abgewickelt, so daß nur noch eine geringe Software-Unterstützung notwendig ist.

Unterstützt werden muß der Mechanismus für den Zustandswechsel durch geeignete Speicherschutzmechanismen. Sie müssen sicherstellen, daß die Kontext- und Verwaltungsdaten beim Zustandswechsel vor unberechtigtem Zugriff geschützt werden, da sonst eine Beeinflussung der Zustandsumschaltung durch andere Systemteile nicht ausgeschlossen werden kann.

Bei neueren Prozessoren wird auch die Parameterliste des Aufrufers bei einem Zustandswechsel in einen geschützten Bereich kopiert. Dadurch können (TOCTOU)-Probleme (Time-of-Check versus Time-of-Use) weitgehend ausgeschlossen werden.

Bei einer Evaluation müssen, wenn keine weiteren oder nicht ausreichende Abgrenzungsmechanismen innerhalb der privilegiert ablaufenden Systemteile vorhanden sind, alle privilegiert ablaufenden Betriebssystemteile evaluiert werden, da eine gegenseitige Beeinflussung von einzelnen Systemteilen nicht ausgeschlossen werden kann.

Bei einer Evaluation ist die Stärke des Abgrenzungsmechanismus zu bewerten. Bewertungsparameter sind unter anderem der Aufwand (realisiert durch die Software) für einen Zustandswechsel, für einen Aufruf und für den Parameterschutz beim Aufruf. Außerdem ist zu prüfen und zu bewerten, durch welche Schutzmechanismen die Kontextdaten und die Parameterliste des Aufrufers bei einem Zustandswechsel geschützt werden. Die Stärke der Speicherschutzmechanismen geht mit in die Bewertung des Abgrenzungsmechanismus ein.

2. Virtuelle Adreßräume

Ein Betriebssystem unterstützt die virtuelle Adressierung. Jeder Benutzer dieses Systems hat einen eigenen virtuellen Adreßraum. Innerhalb der virtuellen Adreßräume gibt es Speicherbereiche, die allen Adreßräumen gemeinsam sind. Die Umschaltung zwischen Benutzeradreßräumen erfolgt durch die Software mit Unterstützung der Hardware. Besonders kritisch bei diesem Abgrenzungsmechanismus ist der Schutz der Segment- und Seitentabellen für die Umsetzung der virtuellen in reale Adressen durch die Software sowie die Unabhängigkeit der einzelnen virtuellen Adreßräume. D.h. wie groß ist der allen Adreßräumen gemeinsame Speicherbereich und welche Informationen enthält er? Die Stärke dieses Abgrenzungsmechanismus ist deshalb abhängig von den Schutzmechanismen für die Tabellen der Adreßumsetzung und der Unabhängigkeit der Adreßräume.

Bei einer Evaluation ist insbesondere die Stärke der Schutzmechanismen für die Adreßumsetzungstabellen zu bewerten sowie die Unabhängigkeit der einzelnen virtuellen Adreßräume. Die vorhandene Hardware-Unterstützung geht ebenfalls mit in die Bewertung des Abgrenzungsmechanismus ein.

6. Evaluationsumfeld

Neben den technischen Regeln für das Verfahren müssen für die Prüfung und Bewertung von IT-Systemen bzw. IT-Komponenten auch rechtliche und organisatorische Rahmenbedingungen festgelegt werden.

Das Bundeskabinett hat hierzu am 21. Februar 1990 den Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) - die ZSI erhält die Bezeichnung Bundesamt - beschlossen. Das Gesetz und danach vorgesehene ergänzende Rechtsverordnungen werden die notwendigen rechtlichen Regelungen enthalten, soweit das Bundesamt oder von ihr beauftragte Stellen tätig werden. Bei Bedarf werden ergänzende organisatorische Regelungen in das Handbuch aufgenommen.

7. Beschreibung des Evaluationsprozesses

Allgemeine Bemerkungen

Die folgenden Kapitel geben Hinweise unterschiedlicher Art, z.B. wie die Evaluation eines Systems ablaufen sollte, welche organisatorischen Vorkehrungen zu treffen sind und welche Vorgehensweise adäquat erscheint. Dies sind wie gesagt Hinweise und keine unumstößlichen Regeln oder Vorgaben.

Die Ausführungen zeigen, daß für eine Evaluation ein erheblicher organisatorischer Aufwand nötig ist. Dieser ist umso mehr gerechtfertigt, wenn das zu evaluierende System entweder eine hohe Qualitätsstufe zum Ziel hat oder die Komplexität des Systems entsprechend hoch ist. Es muß jedoch davor gewarnt werden, bei einer Evaluation gleich ins Detail zu gehen und zu glauben, diesen organisatorischen Vorlauf könnte man sich ersparen.

Im Lauf mehrerer Evaluationen werden ausreichend Erfahrungen gesammelt werden, um die hier gemachten Aussagen noch einmal kritisch zu beleuchten.

7.1 Organisatorischer Aufbau des Evaluations-Teams

Ein Evaluations-Team setzt sich zusammen aus:

- dem organisatorischen Projektleiter (auch Projektverantwortlicher),
- dem technischen Projektleiter,
- den Evaluatoren und
- dem Moderator.

Im folgenden werden die Aufgaben und Verantwortlichkeiten der einzelnen Mitglieder eines Evaluations-Teams näher erläutert.

ORGANISATORISCHER PROJEKTLEITER (OPL)

Der organisatorische Projektleiter ist verantwortlich für den gesamten Ablauf und die Durchführung der Evaluation. Als Projektverantwortlicher muß er sicherstellen, daß der Zeitplan der Evaluation eingehalten wird und die Kosten der Evaluation den vorgegebenen Rahmen nicht überschreiten. Zu seinen Aufgaben gehört:

- die Vertragsgestaltung,
- die Mitarbeit an der Evaluationsplanung,
- die Zusammenstellung des Evaluations-Teams,
- die Teilnahme an Reviews während der Evaluation und
- die Berichterstattung.

Bei der Vertragsgestaltung legt der organisatorische Projektleiter in Abstimmung mit dem Hersteller das zu evaluierende Produkt, die angestrebte Funktionalität bzw. Funktionalitätsklasse und Qualitätsstufe (Evaluationsziel) fest und dokumentiert dies im Evaluationsvertrag. Als Projektverantwortlicher arbeitet er an der Evaluationsplanung mit. Der organisatorische Projektleiter berichtet seinem Vorgesetzten über Stand und Fortgang der Evaluation und über Probleme, die den Evaluationsprozeß aus Sicht der Evaluations-Teams gefährden.

Den Auftraggeber und die Evaluationsstelle unterrichtet er ebenfalls über anstehende Probleme, die den Fortgang der Evaluation gefährden. Zusätzlich informiert er den Auftraggeber über Nachbesserungszeiträume und über ungenügende Ressourcen.

TECHNISCHER PROJEKTLEITER (TPL)

Der technische Projektleiter ist verantwortlich für den technischen Ablauf der Evaluation. Er verteilt die anstehenden Aufgaben an die Evaluatoren. Dabei berücksichtigt er die speziellen Vorkenntnisse der einzelnen Evaluatoren. Zu seinen Aufgaben gehört:

- die Projektplanung,
- die aktive Teilnahme an der Evaluation,
- die Berichterstattung und
- die Entscheidung über technische Probleme.

Der technische Projektleiter legt im Projektplan den technischen Ablauf der Evaluation fest. Er nimmt Änderungen und Verfeinerungen am Projektplan vor, die aufgrund des Verlaufs der Evaluation notwendig werden. Die im Projektplan festgelegten Aufgaben werden von ihm an die Evaluatoren verteilt. Der technische Projektleiter ist bei allen technischen Reviews als normales Teammitglied mit allen Rechten, Pflichten und Verantwortlichkeiten zu betrachten. Darüber hinaus sollte er an allen sonstigen Sitzungen, die das Projekt betreffen teilnehmen, um einerseits sämtliche technische Informationen dem Projektverantwortlichen gegenüber vertreten und andererseits die Teammitglieder von Entscheidungen des Projektverantwortlichen zu unterrichten und diese erläutern zu können. Zusätzlich berichtet er dem Projektverantwortlichen über alle Probleme, die während der Evaluation auftreten. Er trifft Entscheidungen in allen Problemfällen, die nicht den Zeitrahmen der Evaluation oder das Evaluationsziel betreffen.

EVALUATOREN

Den Evaluatoren obliegt die Durchführung der Evaluation. Zu ihren Aufgaben gehört:

- die Beurteilung der einzelnen Dokumente, wie Spezifikation, etc.,
- die Entwicklung von Testprogrammen,
- die Erstellung von Testdatensätzen,

- die Durchführung von Tests,
- die Beurteilung der Anwender-Dokumentation und
- die Erarbeitung von Dokumenten zu allen Evaluationsvorgängen.

Zusätzlich berichten die Evaluatoren dem technischen Projektleiter über aufgetretene Probleme bei der Evaluation sowie über die vorzeitige Beendigung einer Teilevaluation. Innerhalb des Evaluations-Teams präsentieren und begründen sie im Rahmen einer Reviewsitzung ihre Prüfergebnisse bei Teilevaluationen.

MODERATOR

Der Moderator ist verantwortlich für die Planung und Durchführung von Reviews. Zu seinen Aufgaben gehört:

- die Planung von Reviewsitzungen,
- die Moderation von Reviewsitzungen und
- die Berichterstattung.

Bei der Planung von Reviewsitzungen legt der Moderator Zeit und Ort der Reviewsitzungen fest. Er benennt die am Review teilnehmenden Personen (dies sind im allgemeinen die Mitglieder des Evaluations-Teams), bereitet den eigentlichen Review vor, verteilt die Arbeitsunterlagen und benachrichtigt die Reviewteilnehmer rechtzeitig über Zeit und Ort des Reviews. Zu seine Aufgaben gehört die Moderation der Reviewsitzungen, deshalb sollte der Moderator auf diesem Gebiet bereits Erfahrungen gesammelt haben. Er protokolliert die Reviewsitzungen und verhindert unproduktive Diskussionen zwischen Reviewteilnehmern. Zusätzlich überwacht er den Zeitrahmen einer Reviewsitzung und legt Arbeitspakete fest, die sich aus dem Review ergaben. Reviewergebnisse sowie aufgetretene Probleme gibt der Moderator an den technischen Projektleiter und an den Projektverantwortlichen weiter.

Die Aufgaben des Moderators können bei Bedarf auch abwechselnd von den übrigen Mitgliedern des Evaluations-Teams wahrgenommen werden.

7.2 Der Reviewprozeß

Am Ende einer Evaluation steht eine Entscheidung an, ob das evaluierte System ein Zertifikat erhält oder nicht. Diese Entscheidung ist natürlich immer in Zusammenhang mit den zu erfüllenden Kriterien zu sehen. Da eine Vielzahl von Kriterien zu erfüllen sind, setzt sich die endgültige Entscheidung aus einer Vielzahl von Einzelentscheidungen zusammen.

Ebenso ist zu beachten, daß die in den IT-Sicherheitskriterien formulierten Anforderungen keine physikalisch meßbaren Größen sind. Natürlich ist es das Ziel der

Formulierung gewesen, bei der Anwendung der Kriterien objektive Aussagen zu ermöglichen. Trotzdem bleibt immer noch ein Rest Subjektivität erhalten. Hier spielt dann der Erfahrungshintergrund der Evaluatoren eine große Rolle.

Um nun den Einfluß dieser subjektiven Entscheidungen auf den Gesamtprozeß der Evaluation so gering wie möglich zu halten, wird bei der Evaluation die folgende Vorgehensweise empfohlen.

Der Evaluationsvorgang wird in einzelne Phasen unterteilt, diese wiederum in einzelne Stufen. Innerhalb dieser einzelnen Stufen sind vom Evaluator einzelne Arbeitspakete zu bearbeiten. Handelt es sich dabei um ein Arbeitspaket, das gezielt eine Entscheidung vorbereitet, ob ein Kriterienpunkt erfüllt ist oder nicht, so ist diese Entscheidung nicht dem einzelnen Bearbeiter dieses Arbeitspaketes überlassen. Seine Aufgabe ist die Vorbereitung einer Entscheidung. Ist ein Arbeitspaket aus der Sicht des Evaluators abgeschlossen, d.h. es liegen genügend Erkenntnisse vor, dann bittet er den Moderator eine Reviewsitzung einzuberufen.

Auf dieser Sitzung trägt der Evaluator seine Vorgehensweise, die durchgeführten Aufgaben/Tests, Problembereiche und sein vorgeschlagenes Evaluationsergebnis vor. Damit die Anwesenden (technischer Projektleiter, Evaluatoren und evtl. Projektverantwortlicher) zu einer Entscheidung gelangen können, muß ihnen natürlich vom Moderator schon eine grob ausgearbeitete Unterlage über das bei der Reviewsitzung zu bearbeitende Arbeitspaket vorgelegt worden sein. Die Ausarbeitung dieser Unterlage ist Aufgabe des Evaluators.

Unter Leitung des Moderators diskutieren die Anwesenden die vorgestellten Erkenntnisse mit dem Ziel, zu einer gemeinsam getragenen Entscheidung zu gelangen, ob das vorgetragene Evaluationsergebnis so akzeptiert wird, oder ob noch Unklarheiten bestehen, die zusätzliche Untersuchungen erforderlich machen.

Ziel sollte eine möglichst von allen Anwesenden getragene Entscheidung sein. Es ist jedoch nicht auszuschließen, daß ein Teilnehmer die Entscheidung nicht mittragen kann. In diesem Fall sind seine Argumente zu protokollieren und dem Endbericht für dieses Arbeitspaket hinzuzufügen.

Ein Evaluator kann den Moderator auch dann bitten eine Reviewsitzung einzuberufen, wenn er zur Überzeugung gekommen ist, daß ein vorgegebenes Kriterium nicht erfüllt ist und weitere Untersuchungen nicht mehr sinnvoll sind. Auch in diesem Fall ist es das Ziel der Reviewsitzung, zu einem abgestimmten Ergebnis zu kommen. Die Gründe dafür, daß eine weitere Untersuchung nicht mehr sinnvoll ist, müssen niedergelegt werden. Kommt die Mehrzahl der Teilnehmer zum Schluß, daß eine weitergehende Untersuchung doch noch sinnvoll ist, so müssen auch die dazu führenden Argumente niedergelegt werden.

Es liegt dann in der Entscheidung des technischen Projektleiters und des Projektverantwortlichen, ob sie sich diese Argumente zu eigen machen und eine

weitere Untersuchung befürworten. Bei unterschiedlichen Auffassungen von technischem Projektleiter und Projektverantwortlichem liegt die letzte Entscheidung beim Projektverantwortlichen, der auch die Gesamtverantwortung trägt.

7.3 Starten einer Evaluation

Prinzipiell gibt es zwei Möglichkeiten eine Evaluation zu starten.

- 1) Durch einen Hersteller, der ein Produkt anbietet oder
- 2) durch einen potentiellen Anwender eines Produktes.

Das Interesse des Herstellers besteht darin, die Qualität seines Produktes bezüglich bestimmter Sicherheitsanforderungen von einer unabhängigen Stelle bewerten zu lassen. Das Interesse des Anwenders besteht darin, herauszufinden, ob ein ihm aus rein funktionellen Gesichtspunkten zusagendes System auch seine Sicherheitsanforderungen erfüllt. Zusätzlich muß er die gewünschte Qualitätsstufe bestimmen, da diese Auswirkungen auf das Restrisiko hat, falls er dieses System in seiner Einsatzumgebung betreibt.

Im folgenden wird etwas näher auf die Vorarbeiten eingegangen, die beide leisten müssen, bevor sie den Antrag auf Evaluation eines Produktes stellen.

Vorarbeiten Hersteller:

Bei einem vorhandenen Produkt kann der Hersteller aus der gegebenen Sicherheitsfunktionalität seines Produktes eine Vielzahl von potentiell erfüllbaren Sicherheitsanforderungen generieren. Er wird einerseits versuchen die maximal mit seinem System erfüllbaren Sicherheitsanforderungen zu formulieren. Andererseits kann auch der Fall auftreten, daß verschiedene Generierungen des Systems unterschiedliche Sicherheitsanforderungen mit möglicherweise unterschiedlicher Qualität erfüllen können. Hat er nicht schon einen potentiellen Anwender im Auge, dessen Sicherheitsanforderungen er kennt, so ist es ebenfalls denkbar, daß er sich die Sicherheitsanforderungen einer Funktionalitätsklasse der IT-Sicherheitskriterien vornimmt. In den IT-Sicherheitskriterien ist ein Kapitel über Funktionalitätsklassen vorhanden, wobei die Klassen F1 - F5 die Sicherheitsanforderungen, wie sie das "Orange Book" in seinen Klassen (C-A) fordert, beschreiben. Die Beschreibung ist dabei so aufgebaut, daß sie sich an den definierten Grundfunktionen orientiert und die einzelnen Sicherheitsanforderungen der entsprechenden Grundfunktion zuordnet. Der Hersteller muß sich für einen Satz von Sicherheitsanforderungen entscheiden, auf deren Erfüllung das System evaluiert werden soll.

Die einzelnen Qualitätsstufen geben dem Hersteller einen Hinweis, welche Kriterien er bei der Erstellung, Wartung, etc., seines Systems zu erfüllen hat. Dies hilft ihm eine

Abschätzung zu machen, um zu sehen, in welche Qualitätsstufe das zu evaluierende System im günstigsten Fall eingestuft werden kann.

Zur Beantragung einer Evaluation muß der Hersteller der Evaluationsstelle die Funktionalität bzw. eine oder mehrere Funktionalitätsklassen und eine Qualitätsstufe benennen, nach der er sein Produkt untersucht haben will. Es liegt in der Verantwortung des Herstellers mit realistischen Forderungen an die Evaluationsstelle heranzutreten. Kann der Hersteller keine exakten Angaben über die Sicherheitsfunktionen seines Produktes machen, so wird folgendes Vorgehen vorgeschlagen:

Der Hersteller läßt auf seine Kosten durch externe unabhängige Berater, die bereits Erfahrungen mit Evaluationen haben und gegebenenfalls einen neutralen Beobachter der Evaluationsbehörde (kein offizieller Teilnehmer), sein Produkt vor-evaluieren. Ziel dieser Vor-Evaluation ist es, zu einer verbindlichen Aussage über die Funktionalität der Sicherheitsfunktionen des Produktes zu kommen. Eine derartige Vor-Evaluation sollte nicht länger als zwei Wochen dauern. Bei der Auswahl möglicher externer Berater sollte sich der Hersteller an die Evaluationsbehörde oder an eine autorisierte Evaluationsstelle wenden.

Eine Vor-Evaluation ist jedoch im allgemeinen nur für die Funktionalität bzw. Funktionalitätsklasse eines Produktes möglich. Realistische Aussagen über die erreichbare Qualitätsstufe können in so kurzer Zeit in den meisten Fällen nicht gemacht werden, es können allenfalls Hinweise gegeben werden.

Vorarbeiten Anwender eines Produktes:

Zur Erfüllung einer operationellen Aufgabe sucht sich der Anwender ein ihm geeignet erscheinendes System aus. Aus der Beurteilung der Bedrohung, die sich durch die Einsatzumgebung, die operationelle Funktionalität und sonstige Einflußfaktoren ergibt, erarbeitet er sich seine Sicherheitsanforderungen, zusammen mit der für die Bedrohung angemessenen Qualitätsstufe.

Die sich ergebende Qualitätsstufe hat natürlich eine Auswirkung auf die Darstellungsform der Sicherheitsanforderungen. Für die Qualitätsstufe Q5 ist z.B. ein formal definiertes Sicherheitsmodell der Sicherheitsanforderungen zu erstellen, welches dem Evaluations-Team mit übergeben wird. Die sich ergebenden Sicherheitsanforderungen müssen nicht einer vorgegebenen Funktionalitätsklasse entsprechen. Sie sind jedoch die Basis, gegen die das Evaluations-Team das System aus sicherheitstechnischer Sicht prüft. Da die zu erreichende Qualitätsstufe natürlich nicht nur von der Darstellungsform der Sicherheitsanforderungen abhängt, sondern auch von der Qualität des restlichen Systems, wird der Anwender gut beraten sein, sich möglichst frühzeitig mit dem Produkthersteller zusammzusetzen. Bei diesen Gesprächen muß der Hersteller dem Anwender die potentiell mögliche Qualitätsstufe, die sein Produkt bei einer Evaluation erreichen kann, aufzeigen. Gleichzeitig sollte

hierbei auch schon darauf geachtet werden, ob die Sicherheitsanforderungen, wie sie der Anwender wünscht, aus Sicht des Herstellers erfüllbar sind. Kommt man hier zu einer Übereinstimmung, dann wird der Hersteller zusammen mit dem Anwender die Sicherheitsanforderungen in der Form niederschreiben, wie es die gewünschte und auch als erreichbar angesehene Qualitätsstufe erfordert. Der Anwender ist wohl zur Zeit kaum in der Lage, ein formales Modell seiner Sicherheitsanforderungen allein zu erstellen. Es hat wenig Sinn, die Sicherheitsanforderungen in einer Form darzustellen, die weit über den Anforderungen steht, die das Software-Produkt auf Grund seiner durch die Konstruktion erreichbaren Qualitätsstufe verlangt. Der Hersteller muß natürlich auch bereit sein, die entsprechenden Unterlagen, wie sie für die Qualitätsstufe nötig sind, der Evaluationsstelle zur Verfügung zu stellen und falls noch nicht vorhanden, zu erstellen. Wenn alle diese Punkte geklärt sind, kann das System für diese Qualitätsstufe zusammen mit den Sicherheitsanforderungen zur Evaluation eingereicht werden. Es besteht von da an auch kein Unterschied mehr zwischen der Evaluation, die ein Hersteller oder ein Anwender anstößt.

7.4 Ablauf einer Evaluation

Phase 1 KONTAKTAUFNAHME

Stufe 1

Der Auftraggeber nimmt Kontakt mit einer Evaluationsstelle auf.
Er legt seine Wünsche in einem *Antrag auf Evaluation* dar.

Stufe 2

Bearbeitung des Evaluationsantrages, d.h. vor allem: Prüfung, ob der Zeitrahmen für die Evaluationsstelle akzeptabel ist. Bei Gesprächen mit dem Antragsteller sind weitere Informationen einzuholen, um die im folgenden aufgezählten Punkte bearbeiten und beantworten zu können.

- Festlegen der Ansprechpartner.
- Festlegen des voraussichtlichen Personalbedarfs.
- Festlegen, wieviel externes Personal notwendig ist.
- Angaben über den frühesten Anfangstermin.
- Angaben, ob Personalbeistellung des Herstellers ausreichend ist.

Stufe 3

Festlegen nach welchen Kriterien, d.h. Funktionalitätsklasse und Qualitätsstufe, evaluiert werden soll. Daraus folgt die Liste der zu übergebenden Dokumente und Objekte. Entsprechend der Qualitätsstufe wird festgelegt, wie die Objekte übergeben werden (Quellcode, Lademodul, etc.). Falls eine spezielle Maschinenausstattung benötigt wird, muß fixiert werden, wann diese angeliefert wird. Haftungsfragen für

die Hardware sowie Wartungsfragen sind zu klären. Festlegen des anzustrebenden Zeitrahmens der einzelnen Phasen für die Überprüfung mit dazugehörigen Ressourcen. Abstimmung über den Personalbedarf mit allen Beteiligten. Festlegen der Ausbildungsmaßnahmen.

Stufe 4

Ausarbeitung der Evaluationsverträge zwischen der Evaluationsstelle und dem Auftraggeber, sowie externen Unterstützungsfirmen.

Bestandteil des Vertrages sind alle ausgearbeiteten Dokumente der Stufe 3, z.B. Liste der zu übergebenden Dokumente, etc.

Mit dem Vertragsabschluß ist das zu überprüfende Objekt festgelegt, ebenso die dazugehörige Dokumentation. Eine Ausnahme bilden hier begleitende Evaluationen (siehe Kapitel 8).

Der Auftraggeber kann während des Ablaufs der Evaluation von sich aus keine geänderte Dokumentation oder ein geändertes Teil-Objekt in den Evaluationsprozeß einbringen. Dies ist nur mit Zustimmung der Evaluationsstelle möglich.

Phase 2 DOKUMENTENPRÜFUNG

Stufe 1

- Übernahme aller Objekte und Dokumente.
- Ausarbeitung eines ersten Arbeitsplans.
- Bildung einer Gruppe zur Bewertung der Anforderungen der Qualitätsstufe (Q-Gruppe).
- Bildung einer Gruppe zur Bewertung der Funktionalitätskriterien (F-Gruppe). Diese können durch eine Funktionalitätsklasse gegeben sein.
- Zuordnung der Dokumente zu den 2 Gruppen und Arbeitspaketen.
- Festlegung der ersten Reviews (Zeitplanung).
- Festlegung der gemeinsam zu verwendenden Werkzeuge (z.B. Textaufbereitung).

Stufe 2

Die Q-Gruppe prüft, ob entsprechend der angestrebten Qualitätsstufe

- alle notwendigen Dokumente vorhanden sind,
- nach oberflächlicher Betrachtung die Darstellungsform auch in Bezug auf identifizierbare Teilobjekte ausreichend ist.

Aufbau einer Verweisliste: In welchem Dokument befinden sich die Aussagen zu

- Sicherheitsanforderungen,
- Spezifikation der Sicherheitsfunktionen,
- Mechanismen,

- Herstellungsvorgang,
- Abgrenzung zu nicht zu evaluierenden Systemteilen,
- Betriebsqualität?

(Es kann nicht erwartet werden, daß die angelieferte Dokumentation nach der in den IT-Sicherheitskriterien niedergelegten Struktur aufgebaut ist.)

Die F-Gruppe überprüft die Sicherheitsanforderungen und extrahiert notwendige Grundfunktionen sowie Einzelanforderungen.

Ist die Dokumentation für Grundfunktionen und Einzelanforderung vorhanden?

Aufbau einer Verweisliste, die angibt, in welchem Dokument sich Aussagen zu den identifizierten Grundfunktionen und Einzelanforderungen befinden.

Stufe 3

Aus den durchgeführten Einzelreviews der Stufe 2 ist ein Gesamtdokument zu erstellen, in dem folgende Punkte angesprochen werden:

- Kann die Evaluation mit den vorgegebenen Zielkriterien weiter durchgeführt werden?
- Wo können sich kritische Bereiche ergeben?
- Nachbesserungsliste.

Stufe 4

Übergabe dieses Dokumentes an den Auftraggeber mit Abstimmung:

- Was kann bis zu welcher Zeit nachgebessert werden?
- Auswirkungen auf den Zeitplan und Personalsituation.

Stufe 5

Stufe 1 bis Stufe 3 werden noch einmal für die nachgebesserten Dokumente durchlaufen.

Stufe 6

Endgültige Entscheidung darüber, ob die Evaluation weitergeführt wird und ob die bisherigen Kriterien weiterhin gültig sind.

Falls die Evaluation abgebrochen wird:

- Ein Abbruchdokument erstellen mit Begründung.
- Die Verträge mit den Unterstützungsfirmen auflösen.
- Rückgabe der Objekte und Dokumente.
- Archivierung der im Projektablauf erstellten Dokumente.

Falls die Evaluation weitergeführt wird:

- Festlegen der ab jetzt gültigen Dokumente, Objekte und Evaluationskriterien.
- Den Personalbedarf und die Zeitplanung überprüfen.

- Die Korrekturen einleiten.
- Einen Zusatz zum Original-Evaluationsvertrag mit den geänderten Randbedingungen abschließen.

Phase 3 INHALTLICHE DOKUMENTEN- UND OBJEKTPRÜFUNG

Stufe 1

Installation des zu prüfenden Objektes durch den Hersteller, falls dies möglich ist.
Vertrautmachen des Evaluators mit dem Objekt.

Stufe 2

Erstellung des detaillierten Arbeitsplans

Wer bearbeitet wann und wie lange welche Komponente? Dies geschieht in mehreren Arbeitssitzungen des gesamten Evaluations-Teams. Durch die erste Durchsicht der Dokumente und das Vertrautmachen mit dem Objekt kann jeder Evaluator zusammen mit den IT-Sicherheitskriterien und den Vorarbeiten in der Phase 2, Stufe 2 detaillierte Arbeitspakete planen. Die ersten Zeitschätzungen sind nur vor dem Hintergrund der angestrebten Qualitätsstufe, der Komplexität und des eigenen Erfahrungshorizonts vorzunehmen. Rücksicht auf die Gesamtlaufzeit ist in dieser Phase nicht zu nehmen. Dann folgt ein Review mit Zeitabstimmung bzgl. Gesamt-Zeitplan.

Stufe 3

Beginn der Evaluation gemäß dem Arbeitsplan. Die einzelnen Mitarbeiter haben vom Projektleiter die ersten zu bearbeitenden Arbeitspakete zugewiesen bekommen. Sie konzentrieren sich anfangs stark darauf, sich möglichst detaillierte Kenntnisse über das System bei der Bearbeitung der Arbeitspakete anzueignen. Der Zeitpunkt der ersten Projektfortschrittsüberprüfung ist festzulegen.

Stufe 4

Projektfortschrittsüberprüfung

Hierbei wird ein erster Sachstand über den Fortgang der Arbeiten gegeben und falls notwendig, eine Nachbesserungsliste erstellt, die dem Hersteller übergeben wird.

Auf Grund dieser Liste und der Antworten des Herstellers läßt sich ableiten, ob Hinweise bestehen, die die angestrebte Qualitätsstufe oder eine Erfüllung der Sicherheitsanforderungen in Frage stellen.

Bei gravierenden Mängeln kann die Entscheidung getroffen werden, die Evaluation abzubrechen. Dies ist jedoch zu diesem Zeitpunkt als absolute Ausnahme zu sehen.

Die durch die Nachbesserungen möglicherweise auftretenden Zeitverzögerungen müssen in den Arbeitsplan eingearbeitet werden.

Abschließend den Termin für die nächste Projektfortschrittsüberprüfung festlegen.

Stufe 5

Evaluation gemäß Arbeitsplan

Durch die nachfolgende intensive inhaltliche Auseinandersetzung mit dem Produkt, auch durch Tests, können eine Vielzahl von potentiellen Schwachstellen aufgezeigt werden. Durch die internen Reviews muß für jeden Fall festgelegt werden, ob die positive Beendigung der Evaluation gefährdet ist. Sollte dieser Fall eintreten, ist

vorzeitig eine Projektfortschrittsüberprüfung einzuberufen. Wie oft der Evaluations-Zyklus gemäß Arbeitsplan und Projektfortschrittsüberprüfung angestoßen wird, hängt auch von der Komplexität des zu evaluierenden Systems ab. Durch die sich ergebenden Nachbesserungen treten natürlich immer Verzögerungen im Zeitplan auf, so daß auch aus diesem Grund dieser Zyklus nicht zu oft angestoßen werden soll und darf.

Stufe 6

Auswertung der Einzelergebnisse

Die Ergebnisse der einzelnen Arbeitspakete werden dargelegt und ein Vorschlag erarbeitet, welche Kriterien mit welcher Qualität erfüllt wurden.

Phase 4 VORARBEITEN FÜR DIE ZERTIFIKATERSTELLUNG

Stufe 1

Die Einzelprüfergebnisse werden zu einem internen Dokument komprimiert mit der endgültigen Festlegung, welche Sicherheitsanforderungen mit welcher Qualität erfüllt wurden.

Stufe 2

Erstellung eines Evaluationsberichtes für den Hersteller des Produktes.

In diesem Evaluationsbericht müssen nicht alle Einzelergebnisse aufgelistet werden. Es sollten jedoch Hinweise enthalten sein, wo und wie der Hersteller sein Produkt verbessern kann.

Stufe 3

Archivierung aller Ergebnisse, Rückgabe der Hardware, Software und der bereitgestellten Dokumente.

Phase 5 ERSTELLEN ZERTIFIKAT

Die Erstellung und Vergabe des Zertifikats obliegt allein der ZSI.

Stufe 1

Falls die Evaluation nicht durch die Evaluationsbehörde, sondern durch eine autorisierte Evaluationsstelle durchgeführt wurde, müssen alle erstellten Dokumente und Ergebnisse der Evaluationsbehörde übergeben werden.

Stufe 2

Prüfung der Evaluationsergebnisse durch die Evaluationsbehörde.

Stufe 3

Aufnahme in die Liste der evaluierten Produkte. Erstellung des Zertifikats mit Übergabe des Zertifikates an den Hersteller.

Bemerkungen zu den zwei Begriffen Dokumentenliste, Arbeitsplan.

Die Dokumente, die der Hersteller für eine Evaluation zur Verfügung stellt, werden in einer Liste zusammengefaßt, die später dann auch in den nicht öffentlichen Anhang des Zertifikates mit aufgenommen wird. Es ist nicht Sinn und Zweck dieser Liste, möglichst viele Einträge zu haben. Der Hersteller soll das Evaluations-Team nicht mit für die Evaluation irrelevanter Dokumentation überhäufen. Die Liste sollte nur Dokumente beinhalten, die Aussagen zu den Sicherheitsanforderungen machen, die das System zu erfüllen hat. Dies bezieht sich natürlich auf alle Stufen des Entwicklungsprozesses der Software und den dazugehörigen Dokumenten. Wird also z.B. in den Sicherheitsanforderungen die Benutzeridentifikation gefordert, so müssen alle Dokumente in die Liste aufgenommen werden, wo diese angesprochen ist. Die Liste muß so detailliert sein, daß sie selbst die Programmbeschreibung einzelner Module enthält. Damit diese Liste wirklich nur die relevanten Dokumente auflistet, ist aber eine Voruntersuchung der Sicherheitsanforderungen nötig.

Der Arbeitsplan wird im Lauf der Evaluation natürlich mehrere Änderungen und Verfeinerungen erfahren. Er ist aber das Hauptdokument, an dem sich der Ablauf der Evaluation orientiert. Er wird in der Phase 2, Stufe 2 in seiner ersten Version erstellt. Um diese erstellen zu können, muß sich das Evaluations-Team mit dem generellen Design und der Struktur des zu evaluierenden Systems vertraut machen. Ebenso sind die groben Beziehungen, die zu den Sicherheitsanforderungen bestehen, niederzuschreiben.

Erst in der Phase 3, Stufe 2 wird dann der detailliertere Arbeitsplan erstellt. Er sollte Nachbesserungszyklen im Rahmen der Evaluation in gewissem Umfang bereits berücksichtigen. Durch die Beschäftigung mit den Dokumenten, den Gesprächen mit dem Hersteller und den ersten Erfahrungen mit dem System selbst ist dafür nun genügend Information vorhanden. Der Arbeitsplan sollte von diesem Zeitpunkt an nur in begründeten Ausnahmefällen geändert werden können.

7.5 Bewertungsschritte bei einer Teilevaluation

Während der Evaluation eines IT-Systems werden die zu evaluierenden Systemteile, aufgeteilt in einzelne Arbeitspakete für die Evaluatoren, gemäß den IT-Sicherheitskriterien bewertet. Dabei müssen die Evaluatoren darauf achten, daß sie sich bei der Prüfung nicht in irrelevante Details verzetteln (z.B. Suche nach Implementierungsfehlern, die mit der Bewertung nichts zu tun haben).

Bei einer Evaluation wird geprüft, ob die Sicherheitsfunktionen des IT-Systems die Sicherheitsanforderungen erfüllen.

Die Bearbeitung eines Arbeitspaketes erfolgt in mehreren Bewertungsschritten. Sie ist ein iterativer Prozeß, d.h. es kann notwendig sein, zu bereits abgeschlossenen Bewertungsschritten zurückzukehren. Dies kann zum Beispiel dann der Fall sein, wenn bei der Bewertung einer Sicherheitsfunktion Abhängigkeiten zu anderen Systemteilen entdeckt werden, so daß weitere Dokumente für deren Bearbeitung benötigt werden. Ein mögliches Vorgehen bei der Bearbeitung eines Arbeitspaketes ist im folgenden dargestellt.

Bewertungsschritte:

1. Benötigte Dokumente zusammenstellen.
(Sicherheitsanforderungen, Spezifikation der zu bearbeitenden Systemteile, Schnittstellenbeschreibung, Manuale)
 2. Überblick über das Arbeitspaket verschaffen unter dem Blickwinkel Funktionalität und Systemeinbettung.
(Sicherheitsanforderungen, Spezifikation)
 3. Betroffene Sicherheitsanforderungen identifizieren und deren Konsistenz prüfen.
(Sicherheitsanforderungen)
 4. Sicherheitsrelevante Funktionen identifizieren und den Grundfunktionen zuordnen.
(Spezifikation)
- ====> Bisherige Ergebnisse im Evaluations-Team vortragen.
5. Detaillierte Einarbeitung in das Arbeitspaket.
(Spezifikation, Schnittstellenbeschreibung, Manuale)
 6. Abbildbarkeit der einzelnen Hierarchieebenen der Spezifikation (ab Q3 bis auf den Quellcode) prüfen.
(Spezifikation, ggf. Quellcode)
 7. Abhängigkeiten zu anderen Systemteilen ermitteln.
(Spezifikation)

8. Abgrenzungsmechanismen identifizieren und bewerten.
(Spezifikation der Abgrenzung, Schnittstellenbeschreibung)
 9. Mechanismen der Sicherheitsfunktionen identifizieren und bewerten.
(Spezifikation, ggf. Quellcode)
 10. Abdeckung der Sicherheitsanforderungen durch die Sicherheitsfunktionen prüfen.
(Sicherheitsanforderungen, Spezifikation, Schnittstellenbeschreibung)
- ====> Bewertungsergebnisse im Evaluations-Team vortragen.
11. Prüfvorgang und Ergebnis dokumentieren.

7.6 Das Zertifikat

Das auszustellende Zertifikat ist das Abschlußdokument einer Evaluation. Es besteht aus drei Teilen. Erstens dem Zertifikat selbst, welches die grundsätzlichen Aussagen über das evaluierte System enthält und als öffentliches Dokument verfügbar ist. Zweitens einem Anhang 1, der detaillierte Angaben zum evaluierten System enthält und ebenfalls öffentlich ist. Drittens einem Anhang 2, der ebenfalls Angaben zum evaluierten System enthält, aber nicht öffentlich ist, sondern nur für den Hersteller und die Evaluationsbehörde bestimmt ist. Zu beiden Anhängen gibt es dazugehörige Änderungslisten.

Im folgenden werden die in den drei Teilen aufgeführten Informationen je Teildokument aufgelistet.

1. Zertifikat

- Systemname mit Version und Revisionslevel.
- Hardware-Konfiguration auf der evaluiert wurde, mit Revisionslevel.
- Erreichte Qualitätsstufe.
- Erfüllte Funktionalitätsklasse(n) oder Beschreibung der erfüllten Sicherheitsanforderungen.
- Version der IT-Sicherheitskriterien, die bei der Evaluation Verwendung gefunden haben.

2. Anhang 1 (öffentlich)

- Beschreibung der evaluierten Software-Konfiguration mit Hinweis, ob andere Software-Generierungen ebenfalls unter das Zertifikat fallen.

- Beschreibung welche anderen Hardware-Einheiten (mit Revisionslevel) ebenfalls unter das Zertifikat fallen oder Hinweis, daß keine Änderungen an der Hardware-Konfiguration zulässig sind.
- Detaillierte Beschreibung der erfüllten Sicherheitsanforderungen.
- Liste der zum evaluierten System gehörigen Anwenderdokumentation
- Beschreibung der Evaluation mit Hinweisen auf kritische Bereiche
Änderungsliste zu Anhang 1
- Änderungseinträge, die sich auf Punkte im Anhang 1 beziehen.

3. Anhang 2 (nicht öffentlich)

- Liste der Module, Funktionseinheiten oder Teilkomponenten, die evaluiert wurden, mit Version und Revisionslevel.
- Liste der Module, Funktionseinheiten oder Teilkomponenten, die nicht verändert werden dürfen, mit Version und Revisionslevel.
- Liste zusätzlicher Teile, die zum evaluierten System gehören (z.B. Laderstände) mit Version und Revisionslevel.
- Liste der Werkzeuge, die bei der Herstellung des Systems Anwendung gefunden haben, mit Version und Revisionslevel.
- Liste der Gesamtdokumentation, die bei der Evaluation Verwendung gefunden hat.
- Kurzbeschreibung, wo das evaluierte System Schwächen hat.
- Hinweise, wo angesetzt werden müßte, um die Qualitätsstufe des Systems zu verbessern oder Hinweis, daß eine höhere Qualitätsstufe nicht erreicht werden kann.
Änderungsliste zu Anhang 2
- Änderungseinträge, die sich auf Punkte im Anhang 2 beziehen.
- Sonstige Änderungseinträge auf Grund der Regeln bzgl. Reevaluation

7.7 Konsequenzen für den Hersteller

Ist für ein System ein Zertifikat erteilt worden, so ergeben sich daraus für den Hersteller zwei wichtige Konsequenzen:

1. Die im Kapitel Reevaluation aufgezeigten Regeln sind zu befolgen, d.h. Änderungen unterliegen einer strengen Kontrolle durch die Evaluationsbehörde. Falls die Regel R4 (siehe Kapitel Reevaluation) Anwendung finden kann, ist die Evaluationsbehörde zumindest davon in Kenntnis zu setzen. Andernfalls verliert das Zertifikat seine Gültigkeit.
2. Will und muß der Hersteller Änderungen am evaluierten System vornehmen, die die Evaluationsbehörde, aus welchen Gründen auch immer, nicht abnehmen kann oder will, so muß das System eine neue Versionsnummer bekommen. Für dieses System ist das Zertifikat natürlich nicht gültig.

8. Begleitende Evaluation

Die Evaluationsstellen können neben der Evaluation eines fertigen Produktes auch begleitende Evaluationen durchführen. Bei einer begleitenden Evaluation ist das zu evaluierende Produkt noch kein fertiges Produkt, sondern es wird während der Evaluation noch entwickelt bzw. weiterentwickelt. Im allgemeinen sind mit einer begleitenden Evaluation eine Reihe von Besonderheiten verbunden, die sie von einer Evaluation eines fertigen Produktes unterscheidet.

Für den Ablauf einer begleitenden Evaluation sollte die Entwicklungsmethodik des Herstellers, wenn sie der angestrebten Qualitätsstufe angemessen ist, übernommen und im Projektplan festgeschrieben werden. Es kann vom Hersteller nicht erwartet werden, daß er seinen Entwicklungsprozeß an den Evaluationsablauf anlehnt. Auch der Zeitplan für die begleitende Evaluation wird sich im wesentlichen am Zeitrahmen für das in der Entwicklung befindliche Produkt orientieren.

Die bei einer Evaluation vorzulegende Dokumentation (z.B. Sicherheitsanforderungen, Spezifikation der Sicherheitsfunktionen, Sicherheitshandbücher, etc.) ist zu Beginn einer begleitenden Evaluation im allgemeinen noch nicht vorhanden oder befindet sich noch in der Entwicklung. Dadurch ist es einerseits schon sehr früh möglich, den Hersteller auf Dokumentationsfehler und Dokumentationslücken aufmerksam zu machen, andererseits wird die Anzahl der Änderungszyklen bei Dokumenten noch recht groß sein. Dies ist insbesondere bei den Spezifikationsdokumenten ein nicht zu vernachlässigendes Problem. Häufige Änderungszyklen in Spezifikationsdokumenten würden die Evaluation zu einem langwierigen Prozeß machen, da bereits evaluierte Spezifikationsdokumente aufgrund von Designänderungen mehrmals evaluiert werden müßten. Deshalb ist es bei begleitenden Evaluationen besonders wichtig, einen Zeitpunkt festzulegen, ab dem die Dokumente nur noch in Ausnahmefällen geändert werden dürfen. Erst ab diesem Zeitpunkt sollte mit der Evaluation der entsprechenden Dokumentation begonnen werden.

Dies gilt ebenso - und insbesondere in höheren Qualitätsstufen - für Nachbesserungszyklen am Produkt selbst. Auch hier muß die Anzahl der Nachbesserungszyklen so beschränkt werden, daß der Ablauf und der Zeitplan der Evaluation nicht gefährdet wird.

Die Bewertung des Herstellungsprozesses wird bei einer begleitenden Evaluation im Laufe des Entwicklungsprozesses vorgenommen werden. Dazu muß der Hersteller den Evaluatoren Einblick in alle Entwicklungs- und Qualitätssicherungsabläufe während der Entwicklung und Herstellung des Produktes geben.

In höheren Qualitätsstufen hat eine begleitende Evaluation mehr den Charakter einer Qualitätssicherung, da alle Phasen des Entwicklungsprozesses durch das Evaluations-

Team überwacht werden und aufgetretene Probleme direkt im Entwicklungsprozeß berücksichtigt werden können.

Bei einer begleitenden Evaluation ist insbesondere darauf zu achten, daß das Evaluations-Team während der Evaluation kontinuierlich ausgelastet ist. Dies kann dann ein Problem darstellen, wenn sich die einzelnen Phasen der Evaluation nicht nahtlos aneinander anschließen und es zu Leerlaufzeiten innerhalb des Evaluations-Teams kommt oder wenn der Entwicklungsprozeß durch Nachbesserungszyklen nicht kontinuierlich abläuft. Hier sollte es jedoch nicht dazu kommen, daß Evaluatoren in mehreren Evaluationen an unterschiedlichen Produkten mitarbeiten.

Bei der Beschreibung des Evaluationsprozesses in Kapitel 7 sind die Besonderheiten von begleitenden Evaluationen entsprechend zu berücksichtigen.

9. Reevaluation

Ist ein System einmal einer Evaluation unterzogen worden, so ist es unrealistisch anzunehmen, daß es deswegen fehlerfrei ist oder keinen weiteren Änderungen unterliegt. Durch die sich ändernde Umwelt wird ein System andere Anforderungen erfüllen müssen. Diese schlagen sich natürlich als Änderung der Software nieder.

Es stellt sich somit die Frage, wie diese Software-Änderungen eines evaluierten Systems zu behandeln sind. Hält man sich den finanziellen und zeitlichen Aufwand vor Augen, den die Evaluation eines größeren Systems bedeutet, so ist es verständlich, daß man nicht gewillt ist diesen Aufwand bei jeder Änderung zu tragen.

Andererseits ist ebenfalls zu bedenken, daß mit einer Evaluation und dem damit vergebenen Zertifikat eine Aussage bzgl. des Erfüllungsgrades bestimmter Kriterien ausgesprochen wurde, auf die der Anwender sich verläßt. Die Evaluationsbehörde hat nun das Problem, daß sie einerseits auch ungeprüfte Änderungen zulassen muß, andererseits aber weiterhin eine Art "Garantie" für das Produkt übernehmen soll.

Es ist ohne weiteres einsehbar, daß es Änderungen geben kann, die eine komplette neue Evaluation nach sich ziehen. Als Beispiel sei hier die Umstrukturierung des inneren Kerns eines Betriebssystems angeführt. Aber ebenso wird es Änderungen geben, die nur eine Teilevaluation nach sich ziehen und bei denen der Zeitaufwand ohne weiteres im Stundenbereich liegen kann. Die Behebung eines Implementierungsfehlers in einer evaluierten Komponente kann hier als Beispiel dienen.

Es wird aber auch Änderungen geben, die keine Evaluation nach sich ziehen. Beim Ablauf einer Evaluation eines Systems werden als erstes jene Teile untersucht, die unmittelbar zur Erfüllung der Sicherheitsanforderungen notwendig sind. Hinzu kommen als zweites noch jene Teile, die von diesen sicherheitskritischen Teilen nicht genügend getrennt sind und dadurch bei eigenem Fehlverhalten die sicherheitskritischen Teile beeinflussen können. Werden also Änderungen am System durchgeführt, die diese angesprochenen Teile nicht betreffen, so besteht keine Notwendigkeit einer Reevaluation.

Hinsichtlich des Aufwandes spielt auch noch die Qualitätsstufe, nach der das System evaluiert wurde, eine Rolle. Es ist verständlich, daß eine Änderung an einem System, das z.B. nach Q6 evaluiert wurde, einen anderen Aufwand verursacht als bei einem System, welches nur die Qualitätsstufe Q2 erreicht hat. Es beeinflussen also eine Vielzahl von Faktoren den Aufwand, den eine Reevaluation verursacht.

Was jedoch ganz klar ausgedrückt werden muß ist die Tatsache, daß Änderungen gleich welcher Art am lauffähigen, als fix deklarierten Code eines evaluierten Systems durch den Betreiber oder Hersteller, die der Evaluationsbehörde nicht oder nur im nachhinein zur Kenntnis gebracht werden, die Gültigkeit des Zertifikates aufheben. Wie im Kapitel Zertifikat dargestellt, beinhaltet dieses eine Liste jener Teile, die nach der Evaluation nicht mehr verändert werden dürfen, da sie unmittelbar zur Erfüllung der Sicherheitsanforderungen beitragen. Dies bedeutet natürlich nicht, daß nicht andere Systemkonfigurationen generiert werden können, die aufgrund einer geänderten Hardware-Installation notwendig werden. Bezieht das Zertifikat sich jedoch auf eine spezielle Hardware-Konfiguration, dann verliert natürlich mit Änderung der Hardware-Konfiguration auch das Zertifikat seine Gültigkeit.

Die Philosophie, die hinter der Entscheidung eine Reevaluation durchzuführen steht, unterscheidet zwischen evaluierten und nicht evaluierten Komponenten. Dabei können diese Komponenten reine Software-Anteile sein, aber auch sonstige Dokumente, z.B. ein Spezifikationsdokument. Die evaluierten Software-Komponenten bestehen aus folgenden Teilen:

(T1) Teile, die direkt zur Erfüllung der Sicherheitsanforderungen notwendig sind. Diese sind identisch mit den Sicherheitsfunktionen, die die Sicherheitsanforderungen realisieren. Hinzu kommen zusätzliche Teile (T2), die von den Sicherheitsfunktionen als Dienste verwendet werden, also z.B. eine Sortierroutine oder eine Suchroutine. Dazu kommen jetzt noch solche Software-Komponenten (T3), die auf Grund der Konstruktion des Systems nicht genügend von den Sicherheitsfunktionen getrennt werden können.

Ein Einfluß auf die Reevaluation besteht bei den höheren Qualitätsstufen auch noch durch die Werkzeuge (T4), die zur Erstellung des Systems Anwendung gefunden haben. Wird z.B. der Codegeneratorteil eines Compilers verändert, der für ein System Verwendung fand, das nach der Stufe Q6 evaluiert wurde, so erhält eine Neuübersetzung des Systems mit diesem Compiler nicht automatisch die Qualität Q6.

Es lassen sich daraus folgende Regeln bezüglich der Reevaluation ableiten:

- R1) Änderungen und/oder Erweiterungen an T1 erzwingen generell eine Reevaluation durch die Evaluationsstellen.
- R2) Änderungen und/oder Erweiterungen an T2 und T3 werden der Evaluationsbehörde zusammen mit den für die Qualitätsstufe notwendigen Unterlagen übersandt. Die Evaluationsbehörde entscheidet daraufhin, ob eine Reevaluation notwendig wird oder nicht.

- R3) Änderungen und/oder Erweiterungen an T4 werden der Evaluationsbehörde zusammen mit erläuternden Unterlagen übersandt. Dem Hersteller wird mitgeteilt, ob Einspruch gegen die Verwendung der geänderten Teile T4 besteht.
- R4) Änderungen und/oder Erweiterungen an nicht evaluierten Teilen haben keinen Einfluß auf das Zertifikat.

Im folgenden werden einige Beispiele aufgezeigt, die Hinweise geben, wann und mit welcher Zielrichtung eine Reevaluation zu erfolgen hat und wie dabei die vorher aufgestellten Regeln angewendet werden.

Beispiel 1:

Behebung eines Implementierungsfehlers in einem Compiler, der Anwendung für ein System findet, das nach Q6 evaluiert wurde.

Evaluation: Fehlerbehebung hat keine negative Auswirkung auf die Korrektheit der erzeugten Maschinenbefehle.

Evaluator: Hersteller; der Evaluationsbehörde zur Kenntnis und Freigabe.

Zertifikat: Keine Auswirkung auf Zertifikat. Eintrag in die Änderungsliste des Anhangs mit Hinweis auf neue Compilerversion.

Regel: R3, keine Reevaluation.

Beispiel 2:

Behebung eines Implementierungsfehlers im Mechanismus einer Grundfunktion.

Evaluation: Keine unerwünschten Nebeneffekte auf sonstige evaluierte Komponenten. Keinen negativen Einfluß auf die Wirksamkeit des Mechanismus.

Evaluator: Evaluationsstelle; Evaluation kann vor Ort beim Hersteller erfolgen, zur Kenntnis Evaluationsbehörde mit Freigabe.

Zertifikat: Keine Auswirkung auf Zertifikat. Eintrag in die Änderungsliste des Anhangs mit Hinweis auf behobenen Fehler und geänderte Funktionseinheiten.

Regel: R1, Reevaluation notwendig, Aufwand abhängig von Qualitätsstufe, Komplexität und Struktur des Systems.

Beispiel 3:

Erweiterung der Fähigkeiten einer Grundfunktion mit Einführung eines neuen Mechanismus.

Evaluation: Erweiterung wird entsprechend der dokumentierten Qualitätsstufe im Zertifikat geprüft unter Beachtung von Nebeneffekten auf andere evaluierte Komponenten.

Evaluator: Evaluationsstelle; Evaluation kann vor Ort beim Hersteller erfolgen, zur Kenntnis Evaluationsbehörde mit Freigabe.

Zertifikat: Neuerstellung mit jetzt gültigen erfüllten Sicherheitsanforderungen und erreichter Qualitätsstufe. Änderungsliste beinhaltet Hinweis auf Erstzertifikat. Listen in den Anhängen des Zertifikates erhalten Kennzeichen über neu evaluierte Teilkomponenten.

Regel: R1, Reevaluation aller betroffenen Teile. Aufwand abhängig von Qualitätsstufe, Komplexität und Struktur des Systems.

Beispiel 4:

Ersetzung eines Mechanismus, der keine Sicherheitsanforderungen erfüllt, durch einen lauffeitoptimierten mit gleichen Schnittstellen im privilegierten Teil eines Betriebssystems, das nach Q2 evaluiert ist.

Evaluation: Keine unerwünschten Nebeneffekte auf evaluierte Komponenten.

Evaluator: Hersteller; Evaluationsbehörde erhält Unterlagen und Tests

Zertifikat: Keine Auswirkung auf Zertifikat. Eintrag in die Änderungsliste mit Hinweis auf neue Komponente. Die Tests durch Hersteller wurden als ausreichend empfunden.

Regel: R2, keine Reevaluation, nur Sichtprüfung, falls Unterlagen und Tests des Herstellers der Qualitätsstufe Q2 angemessen sind.

Beispiel 5:

Erweiterung der Funktionalität nicht evaluierter Teile (z.B. Kommandointerpreter) eines nach Q4 evaluierten Systems.

Evaluation: Kein Einfluß auf Mechanismus, der evaluierte von nicht evaluierten Teilen trennt.

Evaluator: Hersteller; Evaluationsbehörde wird in Kenntnis gesetzt.

Zertifikat: Keine Auswirkung auf Zertifikat.

Regel: R4, Evaluationsbehörde weiß, daß Abgrenzungsmechanismus bei Q4 ausreichend stark ist. Somit können Fehler in den geänderten Teilen keinen Einfluß auf die Qualität der sicherheitskritischen Teile haben.

Hinsichtlich der Auswirkungen einer Reevaluation auf das Zertifikat können also zwei Fälle unterschieden werden:

- a) das Zertifikat wird als gesamtes ungültig, es wird ein neues erstellt,
- b) das Zertifikat behält seine Gültigkeit und erhält Einträge in den Änderungslisten zu den Anhängen. Dort werden die Änderungen erläutert. .

10. Evaluation von IT-Systemen, die bereits evaluierte Komponenten enthalten

Ziel der IT-Sicherheitskriterien ist es, ein möglichst weites Spektrum von IT-Systemen abdecken zu können. So ist es einerseits möglich, Systeme mit sehr speziellen Einsatzmöglichkeiten zu evaluieren, andererseits sollen auch komplexe Systeme, die aus mehreren Komponenten bestehen, evaluierbar sein. Dabei kann es dann vorkommen, daß einzelne Komponenten eines solchen komplexen Systems bereits evaluiert worden sind.

Um die Evaluation solcher Systeme zu vereinfachen, sollten die Ergebnisse der Evaluationen der Einzelkomponenten mit in den Evaluationsprozeß einbezogen werden. Um dies zu ermöglichen, sollte der Auftraggeber der Evaluationsstelle ein zusätzliches Dokument vorlegen, in dem genau beschrieben ist, welche der Sicherheitsanforderungen an das Gesamtsystem von den einzelnen, bereits evaluierten Komponenten abgedeckt werden sollen, und wie die Separierung der einzelnen Komponenten untereinander gewährleistet wird. Aufbau, Detaillierungsgrad und Form dieses Dokumentes hängen von der angestrebten Qualitätsstufe ab und sollten der Darlegung der Sicherheitsanforderungen an das Gesamtsystem bzw. der Darlegung der Spezifikation entsprechen.

Die Evaluationsstelle prüft dann, ob die so abgeleiteten Sicherheitsanforderungen an die Einzelkomponenten eine Teilmenge der bei der Evaluation dieser Einzelkomponente geprüften Sicherheitsanforderungen sind, und ob die Einzelkomponente in eine Qualitätsstufe evaluiert wurde, die gleich oder besser ist, als die für das Gesamtsystem angestrebte Qualitätsstufe. Ist dies der Fall, so braucht die Einzelkomponente im Rahmen der Evaluation des Gesamtsystems nicht weiter betrachtet zu werden. Zur Bewertung muß lediglich entsprechend der angestrebten Qualitätsstufe geprüft werden, ob die Komponente im Gesamtsystem die ihr zugeordneten Sicherheitsanforderungen abdeckt und nicht in irgendeiner Weise im Gesamtsystem umgehbar oder täuschbar ist. Ein weiterer Punkt der untersucht werden muß ist, ob die Einzelkomponente im Gesamtsystem mit ausreichender Qualität von den nicht zu evaluierenden Systemteilen getrennt ist.

Beispiel:

Gegeben sei ein Netzwerk, bestehend aus einer Reihe von Einzelrechnern, die in die Qualitätsstufe Q2 evaluiert wurden, aus speziellen Filterrechnern der Qualitätsstufe Q6, sowie aus File-Servern der Qualitätsstufe Q4.

Die Sicherheitsanforderungen verlangen folgendes:

- Identifikation und Authentisierung von Benutzern.
- Daten müssen in Dateien zusammengefaßt werden können.
- Benutzern und Dateien muß ein Attribut zugeordnet werden können, dessen Wertebereich eine Hierarchie bildet. Diese Attribut muß dazu verwendet werden, die Axiome des Bell-LaPadula-Modells zu realisieren.

Diese Sicherheitsanforderungen seien wie folgt auf die einzelnen Komponenten aufgeteilt:

- Die Identifikation und Authentisierung werde von den Einzelrechnern durchgeführt.
- Die Auswertung der Attribute und die Einhaltung der Bell-LaPadula-Axiome werde von den Filterkomponenten erzwungen.
- Die Dateiverwaltung sowie die Speicherung von Attributen und Authentisierungsinformationen werde von den File-Servern durchgeführt.

Somit kann das Gesamtsystem maximal die Qualitätsstufe Q2 erreichen, da eine der Sicherheitsanforderungen von einer Komponente realisiert wird, die nach Q2 evaluiert wurde. Um eine höhere Qualitätsstufe für das Gesamtsystem zu erreichen, muß entweder die Einzelkomponente im Rahmen einer Reevaluation in eine höhere Qualitätsstufe evaluiert werden, oder die von dieser Komponente realisierte Sicherheitsanforderung (Identifikation und Authentisierung von Benutzern) muß von einer anderen, höher bewerteten Komponente realisiert werden (z.B. durch die Filterkomponente). Dabei muß allerdings die von dieser Komponente nun zusätzlich zu erfüllende Sicherheitsanforderung eine Teilmenge der Sicherheitsanforderungen an diese Einzelkomponente bei deren Evaluation sein. Dann ist eine höhere Bewertung des Gesamtsystems möglich, wenn die Evaluation ergibt, daß die benötigten Sicherheitsfunktionen der Einzelkomponente im Gesamtsystem nicht umgehbar oder täuschbar sind.

11. Werkzeuge und Methoden

Allgemeine Bemerkungen

Wie in den höheren Qualitätsstufen dargestellt, werden dort immer stärkere Anforderungen an den Herstellungsvorgang gestellt und ebenso an die Darstellung der Sicherheitsanforderungen und der Spezifikation. Die Vielzahl der in diesen Bereichen anwendbaren Methoden und der dazugehörigen Werkzeuge stellt auf längere Sicht die Evaluationsbehörde und andere Evaluationsstellen vor ein Problem. Sie können längerfristig nicht Personal auf eigene Kosten ausbilden lassen, um bei jeder Evaluation mit den bei der Konstruktion verwendeten Werkzeugen umgehen zu können und die Methodik zu beherrschen.

Dies liegt auch im Interesse der Hersteller, da bei den höheren Qualitätsstufen auch eine bestimmte Vertrautheit nötig ist und diese nun einmal nicht in kurzer Zeit zu erwerben ist. Die Evaluationen würden sich also sehr lange Zeit hinziehen. Es besteht ebenso die Gefahr, daß durch mangelnde Vertrautheit Systeme falsch beurteilt werden. Dies ist nun auch nicht im Sinne der Evaluationsbehörde. Sie wird daher gezwungen sein, eine Liste der Werkzeuge und Methoden zu führen, die sie für höhere Qualitätsstufen zuläßt.

Beispielhafter Aufbau der Methoden und Werkzeugliste:

- Methoden oder Werkzeugname,
- Kurzbeschreibung und Anwendungsbereich,
- falls standardisiert: Standardnummer,
sonst: Hersteller, Vertreiber,
- zugelassene Versionen,
- Verwendung für folgende Qualitätsstufen zugelassen (Liste),
- wird in Zukunft (ab Datum) nicht mehr akzeptiert,
- wird mindestens bis (Datum) akzeptiert,
- sonstige Hinweise.

12. Abbildung auf andere Kriterienkataloge

Es ist bekannt, daß andere Nationen sich ebenfalls Gedanken machen, ob sie einen eigenen Kriterienkatalog zur Bewertung von IT-Systemen entwickeln sollen, oder ob sie die Kriterien des amerikanischen Verteidigungsministeriums übernehmen sollen. Beispielsweise in Großbritannien und Kanada wurden bereits eigene Kriterien veröffentlicht, die jedoch noch nicht offiziell herausgegeben worden sind. Deshalb soll im folgenden nur die Abbildbarkeit auf den Katalog der Amerikaner behandelt werden.

Das amerikanische Verteidigungsministerium hat im Zeitraum von 1980-1983 Untersuchungen finanziert, die als Ziel die Erstellung eines Kriterienkatalogs zur Bewertung der Vertrauenswürdigkeit von DV-Systemen hatten. Dieses Dokument, genannt "Trusted Computer System Evaluation Criteria", besser bekannt unter dem Namen "Orange Book", erschien in seiner ersten Version am 15.08.1983. In ihm werden vier Gruppen (D, C, B und A) mit insgesamt sieben Klassen (D, C1, C2, B1, B2, B3 und A1) definiert. Für jede dieser Klassen werden zu erfüllende Kriterien für die vier Bereiche "Security Policy", "Accountability", "Assurance", und "Documentation" aufgestellt. Die Kriterien der vier Bereiche sind von Klasse zu Klasse detaillierter, so daß die sieben Klassen eine Hierarchie bilden, wobei D die niedrigste Klasse ist und A1 die höchste Klasse repräsentiert. Funktionalität und Qualität sind damit gekoppelt. Dies führt zwar zu einer überschaubaren Zahl von Klassen, jedoch hat sich gezeigt, daß es eine Vielzahl von relevanten Systemen gibt, die nicht in diese Klasseneinteilung hineinpassen und somit nach diesem Kriterienkatalog nicht evaluierbar sind.

Deswegen wurde für die IT-Sicherheitskriterien ein Ansatz gewählt, bei dem die Kriterien für Funktionalität und Qualität getrennt sind. Für die entsprechende Klasse des "Orange Books" muß also einerseits die äquivalente Funktionalitätsklasse und andererseits die äquivalente Qualitätsstufe herausgesucht werden. Die ersten Funktionalitätsklassen der IT-Sicherheitskriterien sind so formuliert worden, daß sie weitestgehend die Funktionalität abdecken, wie sie das "Orange Book" in seinen Klassen C1 bis A1 fordert. Die Qualitätsstufen sind vollkommen unabhängig vom "Orange Book" entstanden und beinhalten eine Vielzahl von Kriterien, die einen Einfluß auf die Qualität eines Software-Produktes haben, die jedoch im "Orange Book" nicht vorhanden sind. Daraus folgt, daß ein System, welches nach den nationalen IT-Sicherheitskriterien bewertet wurde, bei gleicher Funktionalität und entsprechender Qualität (siehe Tabelle 1) sicher die äquivalente Klasse des "Orange Books" erfüllt, daß jedoch der rückwärtige Schluß nicht möglich ist. Ein nach dem "Orange Book" evaluiertes System erfüllt immer eine entsprechende, falls notwendig zu definierende Funktionalitätsklasse, aber nicht automatisch eine Qualitätsstufe. Hierzu müssen noch zusätzliche Kriterien erfüllt sein. Speziell in den niedrigeren Qualitätsstufen sollte dies nicht zu großen Problemen führen, wenn der Hersteller

kooperativ ist. Wie die Abbildung in beiden Richtungen im Detail aussieht bedarf noch einer genauen Abstimmung mit den Amerikanern.

Im "Orange Book" werden die sicherheitsrelevanten Teile eines Systems als "Trusted Computing Base (TCB)" bezeichnet. Die TCB umfaßt alle die Teile des Systems, die für die Einhaltung der Sicherheitspolitik und den Schutz der Objekte des Systems verantwortlich sind. Sie besteht aus den sicherheitsrelevanten Teilen der Software, der Hardware und der Firmware. Im Interesse der Verständlichkeit, Nachvollziehbarkeit und Wartbarkeit muß die TCB so klein und überschaubar wie möglich sein.

Um diese Forderung zu erfüllen, verlangt das "Orange Book" die Realisierung der TCB nach dem "Referenzmonitor Konzept". Der Referenzmonitor validiert jeden Benutzerzugriff auf Programme oder Daten des Systems aufgrund einer auf den Benutzer bezogenen Zugriffsliste. Der Referenzmonitor muß drei Designanforderungen erfüllen:

1. Der Referenzmonitor muß gegen unbefugten Zugriff geschützt sein.
2. Der Referenzmonitor darf nicht umgehbar sein.
3. Der Referenzmonitor muß korrekt arbeiten.

Da die IT-Sicherheitskriterien in vielen Punkten allgemeiner formuliert sind als das "Orange Book", sind die Begriffe "Trusted Computing Base" und "Referenzmonitor Konzept" nicht in den IT-Sicherheitskriterien verwendet worden. Jedoch läßt sich auch hier eine Abbildung zwischen den beiden Kriterienkatalogen herstellen.

In den IT-Sicherheitskriterien wird die TCB gebildet durch die Systemteile,

1. die Sicherheitsfunktionen erbringen,
2. die für die Sicherheitsfunktionen notwendige Systemdienste erbringen,
3. die nicht ausreichend von 1. und 2. getrennt sind und
4. die Abgrenzungsmechanismen realisieren.

Der Begriff Referenzmonitor wurde in den IT-Sicherheitskriterien nicht verwendet, weil er streng genommen nur die Grundfunktionen Rechteverwaltung und Rechteprüfung abdeckt.

Die Forderung des "Orange Book" nach einem Referenzmonitor wird in den IT-Sicherheitskriterien abgedeckt durch die Sicherheitsfunktionen der Grundfunktion Rechteverwaltung und Rechteprüfung sowie der Stärke der Mechanismen mit denen diese Sicherheitsfunktionen realisiert sind. Die Referenzmonitor-Eigenschaften werden dagegen sehr wohl gefordert. Dabei ist die Forderung des "Orange Book" "small enough to be analysed" in den IT-Sicherheitskriterien abhängig von der angestrebten Qualitätsstufe, von der Systemstruktur und der Komplexität des IT-Systems. Um die Anforderungen höherer Qualitätsstufen zu erfüllen, müssen diese

Systemteile so entworfen und implementiert sein, daß ihre korrekte Funktionalität und ihre Unumgehbarkeit geprüft und nachvollzogen werden kann.

IT-Sicherheitskriterien		"Orange Book" Klasse
Q0	----->	D
F1, Q2	----->	C1
F2, Q2	----->	C2
F3, Q3	----->	B1
F4, Q4	----->	B2
F5, Q5	----->	B3
F5, Q6	----->	A1
Q7		Beyond A1

Tabelle 1: Abbildung zwischen den zwei Kriterienkatalogen

Erläuterungen:

Wie im ersten Eintrag sichtbar ist die Einstufung nach Q0 unabhängig von der Funktionalität, dies entspricht genau der Philosophie, wie sie das "Orange Book" mit der Klasse D vertritt. In diese Klasse gelangen alle Systeme, die keine höhere Qualitätsstufe erreichten. Die weiteren Einträge zeigen eine Eigenart des "Orange Book", daß nämlich zwischen C1 und C2 eingestuft Systemen kein Qualitätsunterschied besteht, d.h. die Kriterien aus dem Bereich "Assurance" sind gleich. Im Gegensatz dazu besteht der Unterschied zwischen einem nach B3 oder A1 evaluiertem System im wesentlichen im Bereich "Assurance", die Funktionalität, d.h. die Sicherheitsanforderungen sind weitgehend identisch. Die in den IT-Sicherheitskriterien definierte Stufe Q1 ist für eine einfache relativ kurzfristige Überprüfung eines Systems vorgesehen. Der Hersteller wird nur sehr wenig in diese Evaluation eingebunden. Ein potentieller Anwender eines Systems erhält relativ schnell eine Aussage über die minimale Qualität eines Systems. Auf Grund des Ablaufs dieser Evaluation lassen sich auch schon erste Aussagen machen, ob eine Evaluation in eine höhere Qualitätsstufe sinnvoll erscheint. Dies alles soll dazu dienen, die Evaluationsstellen zu entlasten, da eine Evaluation in eine höhere Qualitätsstufe einen nicht unerheblichen organisatorischen Vorlauf bedeutet, der nicht umsonst geleistet werden soll. Die Qualitätsstufe Q7 beschreibt Kriterien, die im "Orange Book" nicht vorhanden sind, es wird dort nur der Hinweis auf eine in der Zukunft zu definierende Stufe gegeben, die im Augenblick zusammenfassend als "Beyond A1" bezeichnet wird.

Glossar

Das vorliegende - gegenüber den IT-Sicherheitskriterien aktualisierte - Glossar erläutert die Bedeutung der Begriffe, so wie sie in diesem Handbuch verstanden werden.

Authentisierung: Nachweis der angegebenen Identität.

Bedrohung: Umstand oder Ereignis, das die Vertraulichkeit, Integrität und Verfügbarkeit der auf einem IT-System verarbeiteten und gespeicherten Daten und/oder die Verfügbarkeit des IT-Systems selbst gefährdet.

Bell-LaPadula-Modell: Formales regelbasiertes Sicherheitsmodell (vorwiegend für Sicherheitsanforderungen im Bereich der "Vertraulichkeit von Daten").

Benutzer: Person, die mit dem IT-System in Verbindung steht und dessen Dienste und Funktionen in Anspruch nimmt.

Betriebsqualität: Maß für die Einhaltung der Sicherheitsanforderungen während des Betriebs eines IT-Systems, insbesondere in Ausnahmesituationen wie z.B. Fehler, Wartung. In anderem Zusammenhang auch: Maß für die Einhaltung aller funktionaler Anforderungen während des Betriebs eines IT-Systems, insbesondere in Ausnahmesituationen wie z.B. Fehler, Wartung.

Beweissicherung: Protokollierung der Ausübung bzw. der versuchten Ausübung von Rechten, um das Umgehen bzw. außer Kraft setzen von Sicherheitsfunktionen nachträglich nachweisen zu können.

Capability: Schlüssel, der dem Besitzer des Schlüssels den Zugriff zu einem Objekt des IT-Systems erlaubt. Der Schlüssel besteht aus einem eindeutigen Bezeichner und den möglichen Zugriffsrechten zu dem Objekt.

Daten: Alles, was mittels eines IT-Systems gespeichert, verarbeitet und ausgeführt werden kann.

Datenübertragung: Transport von Daten zwischen Rechnern, wobei der Übertragungsweg im allgemeinen nicht durch die Funktionen der Rechteprüfung und Rechteverwaltung gesichert ist.

Debugger: Software-Werkzeug zur Fehlersuche.

Designspezifikation: Eine Spezifikation, die das Design eines IT-Systems oder einer IT-Systemkomponente beschreibt. Typischer Inhalt: Kontrollfluß, Datenstrukturen, Datenzugriffe, Ein-/Ausgabeformate, verwendete Algorithmen und Schnittstellenbeschreibungen.

Evaluation: Prüfung und Bewertung eines IT-Systems anhand der IT-Sicherheitskriterien.

Evaluationsbehörde: Zentralstelle für Sicherheit in der Informationstechnik (ZSI). Diese Behörde führt Evaluationen durch und zertifiziert evaluierte Produkte, die den Anforderungen der IT-Sicherheitskriterien entsprechen.

Evaluationsbericht: Das Dokument, in dem das Ergebnis der Prüfung des IT-Systems und die daraus resultierende Bewertung nach Einzelaspekten aufgegliedert niedergelegt ist.

Evaluationsstelle: Eine von der Evaluationsbehörde autorisierte Stelle, die selbständig Evaluationen durchführen, jedoch keine Zertifikate vergeben kann. Die Zertifikatvergabe erfolgt durch die Evaluationsbehörde.

Formale Verifikation: Nachweis der Korrektheit von Programmen mit formalen Mitteln, wie z.B. wp-Kalkül.

Formaler Beweis: Strenger Beweis im mathematischen Sinne, i.a. auf Prädikatenlogik beruhend.

Formales Modell: Ein formales Modell besteht aus Mengen von abstrakten Objekten mit darauf definierten Operationen, für die bestimmte Gesetzmäßigkeiten (Axiome) gelten. Grundgerüst für ein formales Modell ist zum Beispiel die Prädikatenlogik. Ein Modell entsteht aus der Realität durch Abstrahieren (und damit Vereinfachen) und ist einer mathematischen Behandlung zugänglich.

(formales) Sicherheitsmodell: (formales) Modell für die Sicherheitsanforderungen bzw. Teile davon.

Funktionalitätsklasse: Gruppierung, die bestimmte Mindestanforderungen bezüglich der Funktionalität der Sicherheitsfunktionen an ein IT-System stellt.

Funktionseinheit: Modul, Prozedur, Übersetzungseinheit oder Komponente der Software eines IT-Systems.

Grundfunktionen: Abstrakte Beschreibung der Sicherheitsanforderungen an ein IT-System. Sie können zur Gruppierung von Sicherheitsanforderungen verwendet werden.

Identifikation: Bestimmung der Identität eines Subjekts bzw. Objekts.

Integrität: Eigenschaft von Daten, die gleichbedeutend mit deren Unverfälschtheit und Korrektheit ist.

IT-System: System der Informationstechnik

Kanal, verdeckter: Kommunikationsweg, der einen den Sicherheitsanforderungen zuwiderlaufenden Informationsfluß ermöglicht. Die Bandbreite eines verdeckten Kanals ist ein Maß für das mögliche Volumen dieses Informationsflusses im nachrichtentechnischen bzw. informationstheoretischen Sinn.

Konfigurierung: Wahl einer der für ein IT-System möglichen Ausprägungen (hard- und software-seitig) zur Anpassung an die Bedürfnisse des Betreibers.

Mechanismus: Beschreibung einer Vorgehensweise (Lösungsprinzip), wie eine oder mehrere Sicherheitsanforderungen, die an ein IT-System gestellt werden, von diesem erfüllt werden.

Nebeneffekt: Unbeabsichtigte, nicht spezifizierte Nebenwirkung einer Funktion, die unter Umständen auch eine Verletzung der Sicherheitsanforderungen bewirken bzw. ermöglichen kann.

Objekt: Objekte spielen die passive Rolle in der Rechteverwaltung bzw. Rechteprüfung, d.h. auf sie wird zugegriffen. Z.B. Dateien, Inhaltsverzeichnisse, Geräte.

Penetration: Umgehung der Sicherheitsfunktionen eines IT-Systems.

Penetrationstest: Test mit dem Ziel, das System auf die Möglichkeit der Penetration hin zu untersuchen.

Qualität: Maß für die Güte mit der bestimmte Anforderungen an ein IT-System erfüllt werden (im Englischen: assurance). Nach DIN 55350: Gesamtheit von Eigenschaften und Merkmalen eines Produktes oder einer Tätigkeit, die sich auf die Eignung zur Erfüllung gegebener Erfordernisse beziehen.

Qualitätsstufen: Hierarchische Unterteilung bezüglich der Qualitäten eines IT-Systems, die die Sicherheit betreffen. Bei der Evaluation erfolgt die Bewertung dieser Qualitäten des IT-Systems. Anhand dieser Bewertung erfolgt eine Einstufung in eine der Qualitätsstufen Q0 bis Q7 (siehe Kapitel 6.2 der IT-Sicherheitskriterien).

Rechteprüfung: Überprüfung durch das System, ob ein bestimmtes Subjekt die Berechtigung hat, in der beabsichtigten Art auf das gewünschte Objekt zuzugreifen. Durch die Rechteprüfung soll die unbefugte Ausübung von Rechten verhindert werden.

Rechteverwaltung: Verwaltung der Rechtebeziehungen zwischen Subjekten und Objekten, z.B. in Form der Verwaltung einer Zugriffskontrollliste, durch das System.

Risiko: Wahrscheinlichkeit dafür, daß durch eine Verwundbarkeit eines IT-Systems eine Bedrohung für dieses IT-System wirksam wird und ein Schaden eintritt.

Rolle: Eine Rolle ist eine Gruppierung von Rechten, die einem Subjekt oder dessen Repräsentanten im System zugewiesen worden sind. Z.B. die Rolle des Systemverwalters.

Schwachstelle: Schwäche im IT-System, die zur Umgehung oder Täuschung der Sicherheitsfunktionen ausgenutzt werden kann.

Sicherheitsanforderungen: Eine Menge von Forderungen und Regeln, die festlegen, inwieweit die Vertraulichkeit, Integrität und Verfügbarkeit der Daten auf einem IT-System und/oder die Verfügbarkeit des IT-Systems gewährleistet werden soll.

Sicherheitsfunktionen: Funktionen im IT-System, die die Sicherheitsanforderungen verwirklichen.

Sicherheitskritisches Ereignis: Ein Ereignis, durch das die Sicherheitsfunktionen eines IT-Systems umgangen oder außer Kraft gesetzt werden können.

Spezifikation: Ein Dokument, welches die Anforderungen an das System oder an Teile des Systems, die Architektur, das Verhalten oder andere Eigenschaften vollständig, genau und nachvollziehbar beschreibt.

Subjekt: Subjekte spielen die aktive Rolle in der Rechteverwaltung bzw. Rechteprüfung, d.h. sie üben Rechte auf Objekte aus. Z.B. Personen, Prozesse.

Systemverwalter: Rolle in der Rechteverwaltung, i.a. mit außergewöhnlichen Rechten versehen.

Trojanisches Pferd: Ein Programm, das vordergründig eine nützliche Aufgabe verrichtet, versteckt jedoch weitere Aktionen durchführt, wie z.B. sich die Privilegien bzw. Rechte des Aufrufers zunutze zu machen, um Sicherheitsfunktionen zu unterlaufen.

Verfügbarkeit: Wahrscheinlichkeit dafür, daß Daten, die auf einem IT-System gespeichert und verarbeitet werden, zu einem vorgegebenen Zeitpunkt zugreifbar sind oder daß das IT-System zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand ist. In anderem Zusammenhang auch: Wahrscheinlichkeit dafür, daß ein System zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand angetroffen wird.

Wiederaufbereitung: Aufbereitung wiederverwendbarer Betriebsmittel, wie z.B. Haupt- oder Plattenspeicher, mit dem Ziel, einen den Sicherheitsanforderungen widersprechenden Informationsfluß zwischen je zwei Nutzungen zu verhindern.