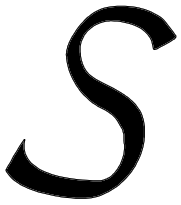


Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)

Vorläufige Form der harmonisierten Methodik

September 1993

Generaldirektion XIII

Telekommunikation, Informationsmarkt und Nutzung der Forschungsergebnisse

Nach umfassender internationaler Überprüfung wird Version 1.0 des ITSEM zur Anwendung im Rahmen der Regelwerke für die Evaluation und die Zertifizierung für einen vorläufigen Zeitraum von zwei Jahren ab Publikationsdatum veröffentlicht. Am Ende dieses Zeitraums soll das ITSEM anhand der gewonnenen praktischen Erfahrungen überarbeitet und fortgeschrieben werden. Darüber hinaus sollen auch Aspekte berücksichtigt werden, die sich aus der weiteren internationalen Harmonisierung ergeben.

Bibliographische Angaben sind am Ende der Veröffentlichung zu finden.

Luxemburg: Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, 1994

ISBN 92-826-7078-2

Printed in Italy

Inhalt

Teil 0 Einleitung

Teil 1 IT-Sicherheitsrahmen

Teil 2 Regelwerke für die Zertifizierung

Teil 3 Grundsätze, Konzepte und Prinzipien

Leerseite

Teil 0 Einleitung

Inhalt

Kapitel 0.1 Einleitung

Hintergrund

0.1.1 Im Mai 1990 veröffentlichten Frankreich, Deutschland, die Niederlande und das Vereinigte Königreich ausgehend von den in den einzelnen Ländern bereits geleisteten Vorarbeiten die Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik [ITSEC]. Nach umfassender internationaler Überprüfung sind zwei weitere Versionen der ITSEC erarbeitet worden, von denen die aktuelle Version 1.2 Grundlage dieses Handbuchs ist.

0.1.2 Ein wichtiger Grund, weshalb der Wunsch aufkam, diese international harmonisierten Kriterien zu erarbeiten, bestand darin, daß eine solche Harmonisierung eine der Voraussetzungen für die gegenseitige internationale Anerkennung der Zertifikate ist, in denen die Ergebnisse der IT-Sicherheitsevaluationen zusammengefaßt werden und die ordnungsgemäße Durchführung dieser Evaluationen bestätigt wird. Sie ist auch eine Voraussetzung für die gemeinsame Anerkennung der Tatsache, daß die bei der Umsetzung dieser harmonisierten Kriterien verwendeten Methoden ihrerseits harmonisiert werden sollten. Aus diesem Grund setzten die vier Länder nach Fertigstellung der ITSEC ihre Zusammenarbeit fort, um ein gemeinsames Konzept für die Durchführung von IT-Sicherheitsevaluationen zu beschließen, zumindest in dem Umfang, in dem dies zur Herstellung der erforderlichen Vertrauensbasis, die eine gegenseitige Anerkennung erleichtert, notwendig ist.

0.1.3 Im Zusammenhang mit der Entwicklung von Methoden für die Bewertung der Sicherheit von IT-Systemen ist bereits vieles geleistet und einiges veröffentlicht worden. Dazu gehören im Vereinigten Königreich das für den Bereich der Regierungsbehörden vorgesehene "CESG Memorandum Number 2" [CESG2] und die "Green Book"-Reihe des Department of Trade and Industry, einschließlich des "V23-Evaluation and Certification Manual" [DTI23], für kommerzielle IT-Sicherheitsprodukte. In Deutschland veröffentlichte die Zentralstelle für Sicherheit in der Informationstechnik ein eigenes IT-Evaluationshandbuch [GISA1].

0.1.4 Die Grundidee bestand darin, die in jedem der vier Länder vorhandenen Sicherheitsevaluationsmethoden so weit zu harmonisieren, daß die nationalen Evaluationsmethoden auf einheitlichen Grundsätzen aufbauen. Man war ursprünglich der Ansicht, die Arbeit solle auf die Harmonisierung vorhandener Methoden beschränkt werden. Es hat sich jedoch die Notwendigkeit ergeben, die bereits geleistete Arbeit fortzuführen und zur Erfüllung der gesetzten Ziele eine Reihe neuer Konzepte zu entwickeln.

Allgemeiner Geltungsbereich

0.1.5 Das vorliegende Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) stützt sich auf Version 1.2 der ITSEC und erläutert, in welcher Art und Weise ein Evaluationsgegenstand (EVG) nach diesen Kriterien bewertet werden soll. Das eigentliche Ziel des Handbuchs besteht darin, als Ergänzung zu den ITSEC einen harmonisierten Katalog von Evaluationsmethoden anzubieten.

0.1.6 Das ITSEM ist ein Fachkompendium, das vor allem für Personen gedacht ist, die mit Evaluationen befaßt sind (in erster Linie Evaluatoren, aber auch Antragsteller und Zertifizierer), es ist aber auch für Hersteller, Entwickler, Systemakkreditierer und Anwender von Interesse. Die darin enthaltene detaillierte Beschreibung von Evaluationsmethoden und -prozeduren reicht aus, um die technische Gleichwertigkeit von in verschiedenen Betriebsumgebungen durchgeführten Evaluationen nachzuweisen. Das Handbuch wird kostenlos abgegeben. ITSEM bezieht sich sowohl auf Evaluationen im Bereich der Wirtschaft als auch im Behördenbereich.

0.1.7 Mit Blick auf eine gegenseitige Anerkennung ist es unumgänglich, daß manche Teile des ITSEM für Evaluatoren Vorschriftencharakter haben. Der überwiegende Teil des Handbuchs dient jedoch zur Erläuterung oder ist als Orientierungshilfe gedacht.

0.1.8 Damit die verbindlichen und die erläuternden Evaluationsmethoden in einen Zusammenhang gebracht werden können, muß das ITSEM auch einige grundsätzliche Angaben über Zertifizierungen und ihren Ablauf enthalten.

0.1.9 In dem Handbuch wird besonders herausgestellt, wie wichtig die Unabhängigkeit der Evaluation von jedem wirtschaftlichen Druck seitens eines Antragstellers oder Entwicklers eines EVG ist. Dabei wird jedoch eine Evaluation, die von einer anderen Abteilung der antragstellenden oder entwickelnden Organisation durchgeführt wird ('first party evaluation'), nicht ausgeschlossen, sofern die Anforderungen des nationalen Regelwerks erfüllt sind.

0.1.10 Das ITSEM ist unter der Prämisse geschrieben worden, daß auf die Evaluation die Zertifizierung folgt. Der Fall, daß auf eine Evaluation eine Erklärung des Herstellers folgt, wird durch das Handbuch nicht abgedeckt; dennoch kann sich auch in diesem Fall der Gebrauch des ITSEM als durchaus hilfreich erweisen.

Struktur und Inhalt

0.1.11 Der Rest des Handbuchs besteht aus sechs Teilen, von denen einer mit Anhängen versehen ist. Jeder Teil ist mit Blick auf die darin angesprochene Zielgruppe erstellt worden. Manche Themen werden in mehreren Teilen angesprochen, jedoch mit unterschiedlichem Detaillierungsgrad.

0.1.12 Teil 1 des ITSEM beschreibt einen IT-Sicherheitsrahmen, der als Hintergrund und konzeptionelle Grundlage für die IT-Sicherheit, die Evaluation, die Zertifizierung und die Systemakkreditierung dient. Dieser Teil ist allgemein gehalten. Er ist für Leser aus dem Bereich des Managements gedacht.

0.1.13 Teil 2 des ITSEM liefert Basisinformationen über die Schaffung und Unterhaltung eines Regelwerks für die Evaluation und die Zertifizierung und beschreibt die allgemeinen Merkmale und den organisatorischen Ablauf des Zertifizierungsprozesses. Er ist für alle diejenigen von Interesse, die sich einen Einblick in den Zertifizierungsprozeß verschaffen möchten.

0.1.14 Teil 3 des ITSEM erläutert die den ITSEC zugrundeliegenden Evaluationsgrundsätze. Er beschreibt die Grundprinzipien, die von den Evaluatoren bei der Durchführung von Evaluationen zu beachten sind. Er enthält weitere Erläuterungen und klärende Aussagen zu den ITSEC-Konzepten und soll damit zum besseren Verständnis der einer Evaluation zugrundeliegenden technischen Aspekten beitragen.

0.1.15 Teil 4 des ITSEM ist für alle diejenigen, die direkt mit Evaluationen befaßt sind, der wichtigste Teil. Der gesamte verbindliche Text befindet sich in diesem Teil. Er gibt einen Überblick über die Art und Weise, wie eine Evaluation durchzuführen ist, und beschreibt sie aus der Sicht des einzubringenden Beitrags, des Prozesses und des zu erzielenden Ergebnisses.

0.1.16 Teil 5 des ITSEM bringt verschiedene Anwendungsbeispiele der ITSEC, aus denen zu ersehen ist, wie die ITSEC bei der Evaluation von Systemen und Produkten eingesetzt werden kann.

0.1.17 Teil 6 des ITSEM enthält evaluationsspezifische Hinweise für Antragsteller, Hersteller, Entwickler, Systemakkreditierer und Anwender. Er befaßt sich insbesondere mit der Erstellung des für eine Evaluation zu erbringenden Beitrags und der Verwendung der erzielten Ergebnisse.

Numerierung und Textkonventionen

0.1.18 Jeder Absatz eines Teils ist durch Kombination der Nummer des entsprechenden Teils, Kapitels und Absatzes innerhalb des Kapitels eindeutig gekennzeichnet. Ein erstmals in einem Teil verwendeter Glossarbegriff ist fett gedruckt. Kursive Schrift wird zur Hervorhebung oder für Zitate verwendet. In Teil 4 des ITSEM sind die Textteile mit Vorschriftencharakter durch Schattierung und Fettdruck ganzer Sätze oder Absätze hervorgehoben.

Hinweis: In der vorliegenden deutschen Übersetzung des ITSEM ist auf die in der englischen Version benutzte Schattierung von Textpassagen verzichtet worden.

Weitere Entwicklungen

0.1.19 Version 1.2 der ITSEC befindet sich zur Zeit in der Erprobungsphase. Während dieser Phase sind Verbesserungsvorschläge zu den ITSEC anhand der praktischen Erfahrungen zu erwarten. Das ITSEM greift auch auf andere Dokumente ([CESG2], [DTI23], [GISA1]) zurück, die bereits ausführlich diskutiert und in der Praxis für nationale Regelwerke herangezogen worden sind; es besteht die Ansicht, daß die Ideen und Konzepte sorgfältig gegeneinander abgewogen worden sind und daß die für das Handbuch gewählte Struktur eine größtmögliche Konsistenz gewährleistet und eine möglichst einfache Handhabung erlaubt.

0.1.20 In der vorliegenden Fassung des ITSEM kommen wichtige Änderungen aufgrund einer umfassenden internationalen Überprüfung zum Tragen. Der Prüfprozeß wurde von der Kommission der Europäischen Gemeinschaften unterstützt, die im September 1992 eine internationale Arbeitstagung veranstaltete, auf der die Version 0.2 diskutiert wurde. Ergänzend zu dieser Veranstaltung wurden schriftliche Kommentare und Beiträge prüfender Fachexperten herangezogen, die die Verfasser bei der Ausarbeitung der Version 1.0 weitestgehend berücksichtigt haben. Die Verfasser des ITSEM sind sich darüber im klaren, daß es in manchen Bereichen des ITSEM noch immer an ausführlicheren Leitlinien mangelt, jedoch werden weitere Informationen zu diesen Bereichen gegebenenfalls in späteren Versionen berücksichtigt, da sowohl das ITSEM als auch die ITSEC dem jeweiligen Erkenntnisstand entsprechend fortgeschrieben werden.

Kapitel 0.2 Hintergrundinformationen

Kontaktstellen

0.2.1 Kommentare und Vorschläge sind erwünscht und unter Angabe des Vermerks "ITSEM-Kommentare" an eine der folgenden Anschriften zu richten:

Commission of the European Communities
DIRECTORATE GENERAL XIII: Telecommmunications, Information Market and Exploitation of Research
DIRECTORATE B: Advanced Communications Technologies and Services
Rue de la Loi 200
B-1049 BRUSSELS
Belgien

In Frankreich:

Service Central de la Sécurité des Systèmes d'Information
18 Rue du Docteur Zamenhof
F-92131 ISSY LES MOULINEAUX

In Deutschland:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
D-53133 BONN

In den Niederlanden:

Netherlands National Comsec Agency
Bezuidenhoutseweg 67
P.O. Box 20061
NL-2500 EB THE HAGUE

National Security Service
P.O.Box 20010
NL-2500 EA THE HAGUE

In Großbritannien:

Head of the Certification Body
UK IT Security Evaluation and Certification Scheme
Certification Body
PO Box 152
CHELTENHAM
Glos GL52 5UF

Glossar und Literaturverzeichnis

0.2.2 Das Glossar enthält Definitionen von Fachbegriffen, die in einer auf das vorliegende Handbuch zugeschnittenen Bedeutung verwendet werden. Im Handbuch vorkommende Fachbegriffe, die nicht nachstehend definiert sind, werden im gesamten Text der Begriffsbestimmung im ITSEC-Glossar entsprechend verwendet. Sollten sie weder hier noch in den ITSEC definiert sein, werden sie in ihrer allgemein anerkannten Bedeutung gebraucht.

Abkürzungen

0.2.3	ANSI	-	American National Standards Institute
0.2.4	CAD	-	Computer Aided Design
0.2.5	CASE	-	Computer Aided Software Engineering
0.2.6	CB	-	Certification Body - Zertifizierungsstelle
0.2.7	CRC	-	Cyclic Redundancy Check
0.2.8	DAC	-	Discretionary Access Control
0.2.9	ETR	-	Evaluation Technical Report - Technischer Evaluationsbericht
	EVG	-	Evaluationsgegenstand, siehe TOE
0.2.10	EWP	-	Evaluation Work Programme - Evaluationsarbeitsprogramm
0.2.11	FMEA	-	Failure Mode and Effects Analysis
0.2.12	FMSP	-	Formal Model of Security Policy
0.2.13	I&A	-	Identification and Authentication - Identifikation und Authentisierung
0.2.14	IPSE	-	Integrated Project Support Environment
0.2.15	ISO	-	International Organisation for Standardisation - Internationale Standardisierungsorganisation
0.2.16	ITSEC	-	Information Technology Security Evaluation Criteria - Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik
0.2.17	ITSEF	-	Information Technology Security Evaluation Facility - Akkreditierte Evaluationsstelle für die Bewertung der Sicherheit von Systemen der Informationstechnik
0.2.18	ITSEM	-	Information Technology Security Evaluation Manual - Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik
0.2.19	MAC	-	Mandatory Access Control
0.2.20	MARION	-	Méthode d'Analyse de Risques Informatiques et d'Optimisation par Niveau
0.2.21	MELISA	-	Méthode d'Evaluation de la Vulnérabilité Résiduelle des Systèmes

0.2.22	MMI	-	Man Machine Interface
0.2.23	PCB	-	Printed Circuit Board
0.2.24	PDL	-	Program Description Language
0.2.25	PID	-	Personal Identification Device
0.2.26	PIPSE	-	Populated Integrated Project Support Environment
0.2.27	SSADM	-	Structured Systems Analysis and Design Methodology
0.2.28	SEISP	-	System Electronic Information Security Policy
0.2.29	SEF	-	Security Enforcing Function - Sicherheitsspezifische Funktionen
0.2.30	SoM	-	Strength of Mechanisms - Stärke der Mechanismen
0.2.31	SPM	-	Security Policy Model - Sicherheitsmodell
0.2.32	SSP	-	System Security Policy - Systemsicherheitspolitik
0.2.33	TCB	-	Trusted Computing Base
0.2.34	TOE	-	Target of Evaluation - Evaluationsgegenstand (siehe EVG)
0.2.35	T&T	-	Technique and Tool - Evaluationstechniken und Evaluationswerkzeuge

Glossar

0.2.36 **Wert**: Informationen oder Ressourcen, die durch die technischen und nichttechnischen Gegenmaßnahmen eines EVG zu schützen sind.

0.2.37 **Protokoll**: Die von einem EVG als Antwort auf protokollpflichtige Operationen generierten Aufzeichnungen, die als Grundlage für die Protokollauswertung dienen.

0.2.38 **Authentisierung**: Die Verifizierung einer behaupteten Identität.

0.2.39 **Analyse des Zusammenwirkens**: Die Ermittlung, ob die Gesamtheit sicherheitsspezifischer Funktionen zusammen mit der Beschreibung ihres Zusammenwirkens entsprechend den Angaben des Architekturentwurfs die Gesamtheit der Sicherheitsziele erfüllt, d.h. alle in den Sicherheitsvorgaben aufgeführten Bedrohungen abdeckt.

0.2.40 **Zertifikat/Zertifizierungsreport**: Das von einer Zertifizierungsstelle als formale Erklärung ausge-stellte öffentliche Dokument, in dem die Ergebnisse der Evaluation und die ordnungsgemäße Anwen- dung der Evaluationskriterien, -methoden und -prozeduren bestätigt werden; hierzu gehören auch aus-reichende Detailangaben über die Evaluation ausgehend vom Technischen Evaluationsbericht (ETR).

0.2.41 **Zertifizierungsstelle**: Eine nationale Stelle, in vielen Fällen die für IT-Sicherheit zuständige nationale Behörde, die für die Verwaltung der ITSEC-Evaluationen in dem jeweiligen Land verantwortlich ist.

0.2.42 **Konstruktionsschwachstelle**: Schwachstellen, die irgendeine während der Konstruktion eingebrachte Eigenschaft des EVG ausnutzen.

0.2.43 **Korrekte Verfeinerung**: Die Verfeinerung einer auf einem bestimmten Abstraktionsniveau beschriebenen Funktion wird als korrekt bezeichnet, wenn die Gesamtheit der auf dem niedrigeren Abstraktionsniveau beschriebenen Wirkungen mindestens alle auf dem höheren Abstraktionsniveau beschriebenen Wirkungen aufweist.

0.2.44 **Gegenmaßnahme**: Eine technische oder nichttechnische Sicherheitsmaßnahme, die zur Erfüllung des Sicherheitsziels bzw. der Sicherheitsziele eines EVG beiträgt.

0.2.45 **Evaluationsbeitrag**: ein Gegenstand oder eine Ressource, der/die den Evaluatoren für die Evaluation zur Verfügung zu stellen ist.

0.2.46 **Fehler**: Eine Nichterfüllung der Korrektheitskriterien.

0.2.47 **Technischer Evaluationsbericht (ETR)**: Ein von einer ITSEF erstellter und der Zertifizierungsstelle vorgelegter Bericht, der die Feststellungen einer Evaluation präzisiert und Grundlage der Zertifizierung eines EVG ist.

0.2.48 **Evaluationsarbeitsplan (EWP)**: Eine Beschreibung der Art und Weise, wie der Arbeitsablauf bei einer Evaluation organisiert wird, d.h. eine Beschreibung der Arbeitspakete, die bei der Evaluation anfallen, und in welcher Beziehung sie zueinander stehen.

0.2.49 **Ausnutzbare Schwachstelle**: Eine Schwachstelle, die in der Praxis zur Überwindung eines Sicherheitsziels eines EVG benutzt werden kann.

0.2.50 **Auswirkungsanalyse**: Eine vom Antragsteller durchgeführte Maßnahme, mit der festgestellt werden soll, ob bei einem geänderten EVG eine Reevaluation erforderlich ist.

0.2.51 **Unvoreingenommenheit**: Vorurteilsfreiheit gegenüber der Erzielung eines bestimmten Ergebnisses.

0.2.52 **Akkreditierte Evaluationsstelle für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEF)**: Eine nach Maßgabe bestimmter anerkannter Regeln (z.B. [EN45]) akkreditierte Stelle, die von der Zertifizierungsstelle ermächtigt worden ist, ITSEC-Sicherheitsevaluationen durchzuführen.

0.2.53 **Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)**: Ein technisches Dokument, dessen detaillierte Angaben über Evaluationsmethoden und -prozeduren für eine gegenseitige Anerkennung ausreichen.

0.2.54 **Nationales Regelwerk**: Ein Katalog nationaler Regeln und Vorschriften für die Evaluation und Zertifizierung nach Maßgabe der ITSEC und des ITSEM.

0.2.55 **Objekt**: Eine passive Einheit, die Informationen enthält oder empfängt.

0.2.56 **Objektivität**: Die Eigenschaft eines Tests, aufgrund derer das Ergebnis mit einem Minimum an subjektivem Urteil oder subjektiver Meinung erzielt wird.

0.2.57 **Operationelle Schwachstelle**: Schwachstellen, die Schwächen nichttechnischer Gegenmaßnahmen ausnutzen, um die Sicherheit des EVG zu verletzen.

0.2.58 **Potentielle Schwachstelle**: Eine mutmaßliche Schwachstelle, die zur Überwindung eines Sicherheitsziels eines EVG benutzt werden kann, deren Ausnutzbarkeit oder Existenz aber noch nicht nachgewiesen worden ist.

0.2.59 **Mängelbericht**: Ein von den Evaluatoren erstellter und an die Zertifizierungsstelle gerichteter Kurzbericht, in dem ein Fehler oder eine potentielle oder tatsächliche Schwachstelle eines EVG erläutert wird.

0.2.60 **Reevaluation**: Die Evaluation eines früher evaluierten EVG nach erfolgter Vornahme von Änderungen.

0.2.61 **Wiederverwendung**: Die Heranziehung früherer Evaluationsergebnisse, wenn eine oder mehrere zuvor evaluierte Komponenten in ein System oder Produkt eingefügt werden.

0.2.62 **Wiederholbarkeit**: Eine erneute Evaluation desselben EVG anhand derselben Sicherheitsvorgaben und durch dieselbe ITSEF führt zu der gleichen Gesamtentscheidung des Evaluators wie bei der Erstevaluation (z.B. E0 oder E5).

0.2.63 **Darstellung**: Die Spezifikation eines EVG in einer bestimmten Phase des Entwicklungsprozesses (der Anforderungen, des Architekturentwurfs, einer Feinentwurfsstufe, der Implementierung).

0.2.64 **Reproduzierbarkeit**: Die Evaluation desselben EVG anhand derselben Sicherheitsvorgaben durch eine andere ITSEF führt zu der gleichen Gesamtentscheidung des Evaluators wie bei der Erstevaluation (z.B. E0 oder E5).

0.2.65 **Subjekt**: Eine aktive Einheit, normalerweise in Form einer Person, eines Prozesses oder eines Geräts [TCSEC].

0.2.66 **Analyse der Eignung**: Die Ermittlung, ob die in den Sicherheitsvorgaben beschriebenen sicherheitsspezifischen Funktionen als Gegenmaßnahmen für die in den Sicherheitsvorgaben definierte(n) Bedrohung(en) dienen können. (Eignung wird nur auf dieser Stufe bewertet).

0.2.67 **Schwachstelle**: Eine Sicherheitsschwäche in einem EVG (z.B. aufgrund von Fehlern in der Analyse, im Entwurf, bei der Implementierung oder beim Betrieb).

Literaturverzeichnis

0.2.68 Auf folgende Bücher und Abhandlungen wird im Text verwiesen:

BDSS Risk Quantification Problems and Bayesian Decision Support System Solutions, Will Ozier, Information Age, Vol. 11, No. 4, October 1989.

BOE Characteristics of Software Quality - TRW North Holland, B.W. Boehm, Software Engineering Economics - Prentice Hall, 1975.

CESG2 Handbook of Security Evaluation, CESG Memorandum No. 2, Communications-Electronics Security Group, United Kingdom, November 1989.

CRAMM CCTA Risk Analysis and Management Methodology, Guidance on CRAMM for Management, Version 2.0, CCTA, February 1991.

DTI23 Evaluation and Certification Manual, V23 Department of Trade and Industry, United Kingdom, Version 3.0, February 1989.

ECMA A Reference Model for Frameworks of Computer-Assisted Software Engineering Environments, ECMA TR/55.

EN45 Allgemeine Kriterien zum Betreiben von Prüflaboratorien, EN 45001.

GASSER Building a Secure Computer System, Morrie Gasser, Van Nostrand Reinhold.

GISA1 IT-Evaluationshandbuch, ZSI, 1990.

GISA2 IT-Sicherheitshandbuch, BSI 7105, Version 1.0, März 1992.

GUI25 General Requirements for the Technical Competence of Testing Laboratories, International Standards Organisation, ISO Guide 25, 1982.

ISO65A Software for Computers in the Application of Industrial Safety Related Systems, ISO/IEC JTC1/SC27 N381, November 1991.

ITSEC Information Technology Security Evaluation Criteria - Harmonised Criteria of France, Germany, the Netherlands and the United Kingdom, Version 1.2, June 1991.

Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik - Harmonisierte Kriterien von Frankreich, Deutschland, den Niederlanden und dem Vereinigten Königreich, Version 1.2, Juni 1991.

LINDE Operating System Penetration, R Linde, Proceedings of the AFIPS, NCC, S. 361-368, 1975.

MCC Factors in Software Quality, J A McCall, General Electric n. 77C1502, June 1977.

MS1629A Procedures for performing a failure mode, effects and criticality analysis, MIL-STD-1629A, US DoD, November 1980.

NIS35 Interpretation of Accreditation Requirements for IT Test Laboratories for Software and Communications Testing Services, NAMAS Information Sheet NIS35, NAMAS Executive, National Physics Laboratory, United Kingdom, November 1990.

OSI OSI Basic Reference Model, Part 2 - Security Architecture, ISO 7498 (1988(E)).

PCTE Portable Common Tool Environment Abstract Specification (December 1990; ECMA 149).

PCTE+ Portable Common Tool Environment (Extended) Definition Team Final Report (14 December 1992).

SRMM Shared Resource Matrix Methology: An Approach to Identifying Storage and Timing Channels. R A Kemmerer, ACM Transactions on Computer Systems, Vol. 1, No. 3, August 1983.

TCSEC Trusted Computer Systems Evaluation Criteria, DoD 5200.28-STD, Department of Defense, United States of America, December 1985.

TNI Trusted Network Interpretation of the TCSEC, National Computer Security Center, United States of America, NCSC-TG-005, Version 1, 31 July 1987.

TDI Trusted Database Interpretation of the TCSEC, National Computer Security Center, United States of America, NCSC-TG-021, April 1991.

Leerseite

Teil 1 IT-Sicherheitsrahmen

Inhalt

Abbildungen

Kapitel 1.1 Einleitung

Werte, Bedrohungen, Risiken, Vertrauen und Gegenmaßnahmen

1.1.1 Die Informationstechnik (IT) hat sich zu einem wesentlichen Faktor der erfolgreichen Abwicklung von Geschäften und der staatlichen Aufgaben entwickelt und gewinnt auch für Privatpersonen, die vom Einsatz der Informationstechnik betroffen sind, zunehmend an Bedeutung. Informationen sind etwas, das gesammelt und geschützt werden muß, damit die eigenen Geschäfte oder die persönlichen Angelegenheiten vorangetrieben werden können; sie sind daher als **Wert** zu betrachten. Die Bedeutung dieser Werte drückt sich für gewöhnlich in dem Folgeschaden aus, der beim Eintreten einer Bedrohung entstehen kann. Schäden können entweder unmittelbar oder mittelbar, durch Offenlegen, unbefugte Modifikation, Vernichten oder Mißbrauch von Informationen entstehen. Das Risiko steigt mit der Größe des zu erwartenden Schadens und der Wahrscheinlich eines Eintretens der Bedrohung.

1.1.2 Die Informationen in IT-Systemen müssen vor Bedrohungen geschützt werden, die schädliche Auswirkungen auf Werte mit sich bringen. Bedrohungen können absichtlich (z.B. Angriffe) oder unabsichtlich (z.B. Fehler oder Ausfälle) sein.

1.1.3 Zur Risikominimierung werden spezifische **Gegenmaßnahmen** ausgewählt. Diese Gegenmaßnahmen sind entweder materieller, personeller, organisatorischer oder technischer Art. Zu den *technischen Gegenmaßnahmen* oder *IT-Gegenmaßnahmen* gehören die sicherheitsspezifischen Funktionen und Mechanismen des IT-Systems; zu den *nichttechnischen Gegenmaßnahmen* oder *Nicht-IT-Gegenmaßnahmen* gehören die materiellen, personellen und organisatorischen Gegenmaßnahmen. Die ITSEC-Evaluation befaßt sich hauptsächlich mit technischen Gegenmaßnahmen.

1.1.4 Oberstes Sicherheitsziel eines IT-Systems ist die Reduzierung der mit ihm verbundenen Risiken auf ein für die betroffene Organisation akzeptierbares Niveau. Dies kann durch die Sicherheitsfunktionen und -eigenschaften des IT-Systems erreicht werden.

1.1.5 Das Vertrauen, das in die von dem IT-System gebotene Sicherheit gesetzt werden kann, wird als Vertrauenswürdigkeit bezeichnet. Je größer die Vertrauenswürdigkeit, desto größer das Vertrauen in die Fähigkeit des Systems, seine Werte gegen eine Bedrohung unter Berücksichtigung eines akzeptierbaren Restrisikos zu schützen.

1.1.6 Je höher die ITSEC-Evaluationsstufe und die Stärke der Mechanismen, desto größer das Vertrauen, das der Anwender den in das IT-System oder -Produkt eingebauten Gegenmaßnahmen entgegenbringen kann. Die von einem Anwender geforderte Evaluationsstufe hängt vom akzeptierbaren Ausmaß des bekannten Restrisikos ab und kann nur mit Hilfe einer Bedrohungs- und Risikoanalyse für einen bestimmten Fall bestimmt werden. Sicherheit und Kosten sind gegeneinander abzuwägen. Produkte oder Systeme mit höheren Evaluationsstufen werden für gewöhnlich teurer sein, da die Kosten für Entwicklung und Evaluation mit zunehmender Evaluationsstufe steigen dürften. Angaben darüber, wie eine Evaluationsstufe in Abhängigkeit von umgebungsrelevanten Parametern bestimmt wird, sind beispielsweise in [GISA2] zu finden. Gezielte Ratschläge können bei den in Teil 2 des ITSEM genannten nationalen Organisationen eingeholt werden.

In den IT-Sicherheitsrahmen einbezogene Prozesse

1.1.7 Es gibt verschiedene Prozesse, die zum Gesamtziel der IT-Sicherheit beitragen. Sie werden in Abbildung 1.1.1 dargestellt.

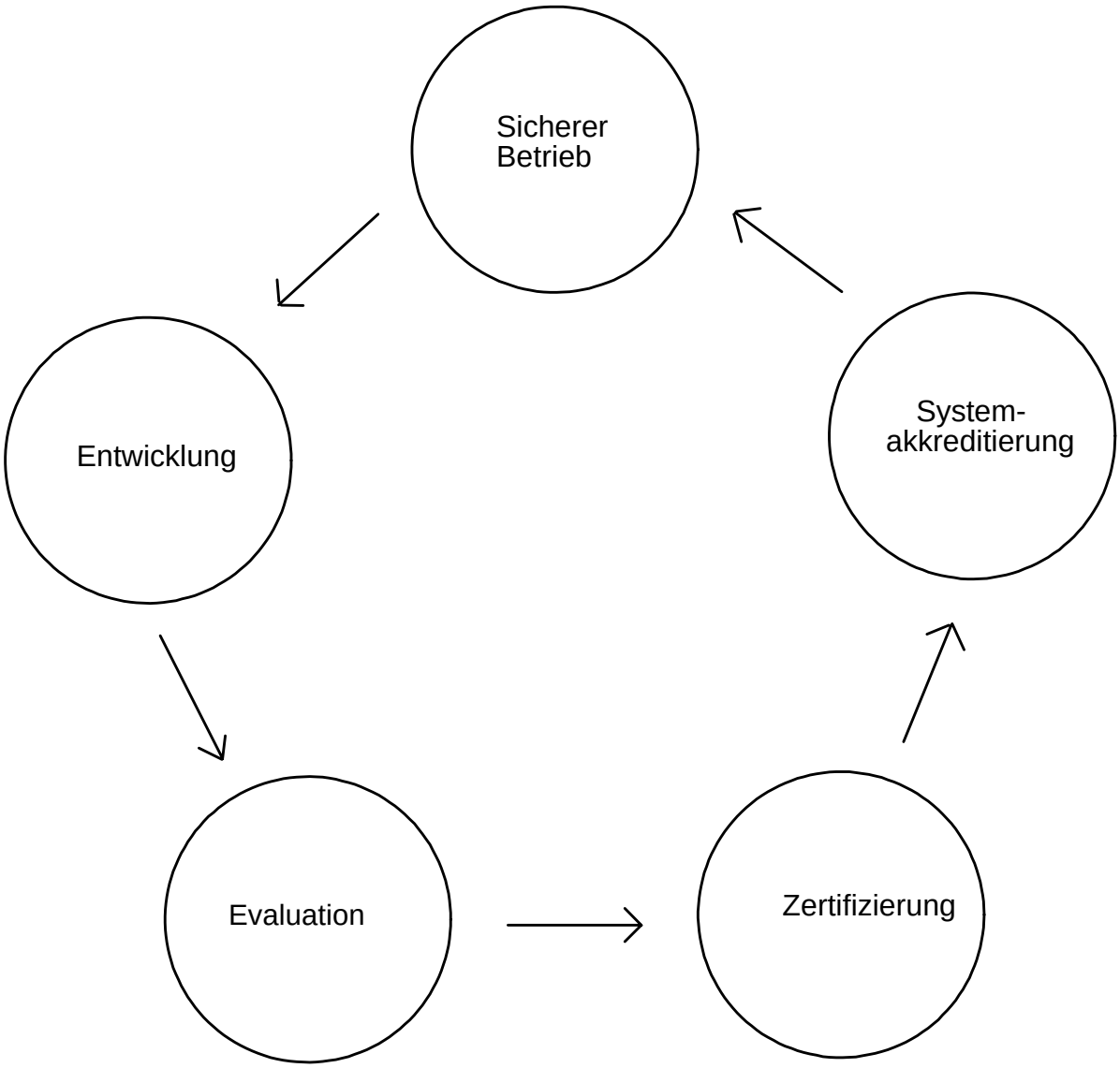


Abbildung 1.1.1 In den IT-Sicherheitsrahmen einbezogene Prozesse

1.1.8 Diese Abbildung zeigt in idealster Form den Zusammenhang in den die IT-Sicherheitsevaluation und -zertifizierung eingebettet ist. Die Pfeile in der Abbildung deuten an, daß aus dem jeweiligen Prozeß ein Eingabe in den nächsten erfolgt. Die Prozesse können teilweise ineinandergreifen. Die Prozeßfolge kann iterativ und kontinuierlich fortlaufend sein.

1.1.9 Der Bau eines IT-Systems oder -produkts erfolgt im Rahmen des Entwicklungsprozesses. Im Verlauf des Evaluationsprozesses wird dieses anhand vorgegebener Sicherheitsevaluationskriterien geprüft. Durch den Zertifizierungsprozeß wird bestätigt, daß die Ergebnisse einer Evaluation gültig und die Evaluationskriterien korrekt angewandt worden sind. Durch den Systemakkreditierungsprozeß soll dann bestätigt werden, daß der Einsatz eines IT-Systems in einer bestimmten Betriebsumgebung und für einen bestimmten Zweck akzeptiert werden kann. Im Rahmen des Prozesses 'Sicherer Betrieb' wird ein akkreditiertes System anhand anerkannter Prozeduren in Betrieb genommen, wobei es sein kann, daß aufgrund von Veränderungen in der Betriebsumgebung Änderungen erforderlich werden, die eine Vorgabe in den Entwicklungsprozeß darstellen.

1.1.10 Der Begriff Akkreditierung wird in zwei unterschiedlichen Begriffszusammenhängen verwendet. Die Akkreditierung einer Evaluationsstelle für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEF) ist das Verfahren zur Anerkennung der **Unvoreingenommenheit** und der technischen Kompetenz dieser Stelle für die Durchführung von Evaluationen. Die Akkreditierung eines IT-Systems (nach der Definition in der Einleitung zu den ITSEC) ist ein Verfahren, durch das ein IT-System für den Betrieb in einer bestimmten Betriebsumgebung zugelassen wird. Die Systemakkreditierung befaßt sich sowohl mit IT- als auch mit Nicht-IT-Gegenmaßnahmen, wohingegen das ITSEM in erster Linie IT-Gegenmaßnahmen betrifft. Die Systemakkreditierung fällt nicht in den Anwendungsbereich von ITSEC/ITSEM.

Evaluationszusammenhang

1.1.11 Im Zusammenhang mit Evaluationen sind drei Aspekte zu nennen:

a) Kriterien;

b) Methodik;

c) **nationale Regelwerke**.

1.1.12 Die Kriterien sind der Maßstab, anhand dessen die Sicherheit eines IT-Systems oder -Produkts bei seiner Evaluation, Entwicklung und Beschaffung bestimmt wird. Die Kriterien geben an, was evaluiert werden muß. In der Methodik wird empfohlen, wie die Evaluation anhand der Kriterien durchzuführen ist. Die nationalen Regelwerke schreiben Regeln für den Ablauf des Evaluations-, Zertifizierungs- und Laborakkreditierungsprozesses hinsichtlich Rolle, Prozeduren, Rechte und Pflichten vor. Die Kriterien sind in den ITSEC zu finden und die zugehörige Methodik im ITSEM, wobei der Detaillierungsgrad so gewählt wurde, daß eine gegenseitige Anerkennung der nationalen Regelwerke erleichtert wird. Aspekte der nationalen Regelwerke werden in Teil 2 des ITSEM und in der in den einzelnen Ländern vorliegenden Dokumentation zu diesen Regelwerken behandelt.

Kapitel 1.2 Evaluations- und Zertifizierungsprozeß

Grundsätzliches

1.2.1 Der im vorliegenden Kapitel beschriebene Evaluationsprozeß dient als Rahmen für die Beschreibung der organisatorischen und verfahrenstechnischen Aspekte der Durchführung einer Evaluation. Es gibt viele Fragen im Umfeld einer Evaluation, die in den verschiedenen Ländern aus Gründen wie etwa der sachlichen Zuständigkeit oder der nationalen Sicherheit unterschiedlich gehandhabt werden. Die Vorschriften des nationalen Regelwerks haben in jedem der Länder Vorrang. Auf die die nationalen Regelwerke betreffenden Fragen wird in Teil 2 des Handbuchs eingegangen.

1.2.2 Wenn Evaluationen auf kommerzieller Basis betrieben werden, unterliegen sie nach den ITSEC den wirtschaftlichen Gegebenheiten des IT-Marktes. Sie müssen wirtschaftlich tragbar sein, d.h. erschwinglich und zeitgerecht. Dieses Ziel muß gegen die Nutzvorteile der Evaluation abgewogen werden. Die dem Evaluations- und Zertifizierungsprozeß zugrundeliegenden Prinzipien werden in Teil 3 des Handbuchs dargelegt.

1.2.3 Bei dieser Form der Evaluation

a) können Antragsteller die Ziele für den Evaluationsprozeß vorgeben;

b) können auf Ersuchen des Antragstellers Ressourcen der ITSEF bereitgestellt werden, und;

c) wird die Pflege von **Zertifikaten**/**Zertifizierungsreports** durch eine **Reevaluation** ohne weiteres unterstützt.

Beteiligte Parteien

1.2.4 Zu den unmittelbar am Evaluationsprozeß beteiligten Parteien gehören

a) der Antragsteller einer Evaluation;

b) die Entwickler eines IT-Produkts oder -Systems;

c) die akkreditierte Evaluationsstelle für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEF);

d) die **Zertifizierungsstelle**.

1.2.5 Ebenfalls mit Evaluationen und Zertifizierungen befaßt sind Anwender und Systemakkreditierer. Sie befassen sich hauptsächlich mit Fragen der Beschaffung und des sicheren Betriebs.

1.2.6 Aus Abbildung 1.2.1 ist zu ersehen, daß alle Beteiligten die Evaluation und die Zertifizierung aus unterschiedlichem Blickwinkel je nach der ihnen zugewiesenen Rolle betrachten.

1.2.7 Das ITSEM enthält erläuternde Informationen und Hinweise für Antragsteller, Entwickler, ITSEFs, Systemakkreditierer und Zertifizierungsstellen; außerdem sind in Teil 4 des Handbuchs zusätzliche evaluatorspezifische Informationen mit Vorschriftencharakter zu finden.

1.2.8 Der Antragsteller einer Evaluation ist derjenige, der die Evaluation veranlaßt und bezahlt. Im Falle einer Systemevaluation dürften Antragsteller und Systemakkreditierer ein und dieselbe Organisation sein.

1.2.9 Die ITSEFs führen die Evaluation durch, normalerweise auf kommerzieller Basis. Die Evaluation schließt nach dem ITSEM und den ITSEC eine eingehende Prüfung eines EVG ein, wobei nach **Schwachstellen** gesucht und gleichzeitig ermittelt wird, inwieweit die Sicherheitsvorgaben des EVG durch seine Implementierung abgedeckt sind.

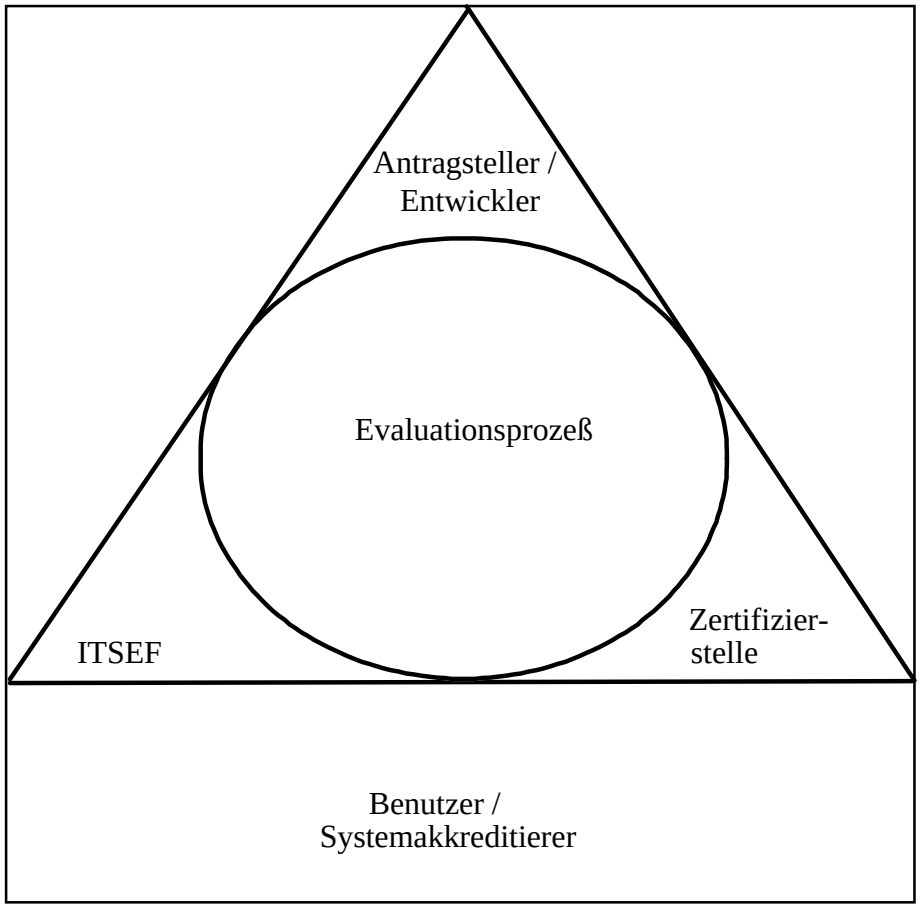


Abbildung 1.2.1 An einer Evaluation oder einer Zertifizierung beteiligte oder damit befaßte Stellen

1.2.10 Als besonders wichtig wird erachtet, daß die ITSEFs keinem wirtschaftlichen oder sonstigen Druck seitens des Antragstellers oder Entwicklers eines EVG ausgesetzt ist. Dies schließt jedoch nicht die Möglichkeit einer Eigenevaluation bzw. Evaluation im Sinne einer von einer anderen Abteilung der antragstellenden oder entwickelnden Organisation durchgeführten Evaluation ('first party evaluation') aus, sofern die Anforderungen des nationalen Regelwerks erfüllt sind.

1.2.11 Aller Voraussicht nach wird eine Evaluation auf der Grundlage einer mit dem Antragsteller oder Entwickler getroffenen Geheimhaltungsvereinbarung durchgeführt. Eine ITSEF unterliegt der geschäftsüblichen Schweigepflicht.

1.2.12 Ein weiterer wichtiger Punkt ist die Unvoreingenommenheit der ITSEF gegenüber durchgeführten Evaluationen. Nationale Regelwerke können einer ITSEF zu erfüllende Anforderungen vorschreiben, die zu erfüllen sind.

1.2.13 Die Zertifizierungsstelle prüft, ob die Ergebnisse einer Evaluation Gültigkeit haben und ob die Evaluationskriterien korrekt angewandt worden sind. Damit soll die Einheitlichkeit und Korrektheit von Evaluationsprozessen nach Maßgabe des ITSEM und der ITSEC und die Konsistenz und Kompatibilität der Evaluationsergebnisse gewährleistet werden. Die Zertifizierungsstelle erstellt und vergibt das Zertifikat/den Zertifizierungsreport für diejenigen EVG, die nach ihren Feststellungen den Sicherheitsvorgaben entsprechen und damit die Anforderungen von Kapitel 5 der ITSEC erfüllen.

1.2.14 Das Zertifikat/der Zertifizierungsreport wird veröffentlicht. Angaben zu Format und Inhalt sind in Teil 2 des ITSEM zu finden.

Phasen des Evaluationsprozesses

1.2.15 Der Evaluationsprozeß ist in drei Phasen unterteilt:

a) Phase I Vorbereitung;

b) Phase II Durchführung;

c) Phase III Abschluß.

1.2.16 Der Prozeß wird hier anhand einer typischen Evaluation umrissen. In der Praxis gibt es eine Reihe von Alternativen, insbesondere wenn die Evaluation parallel zum Entwicklungsprozeß erfolgt. Die drei Phasen werden in Teil 4 des ITSEM ausführlicher beschrieben.

1.2.17 Zu Phase I gehört eine erste Kontaktaufnahme zwischen dem Antragsteller und der ITSEF, eine etwaige Durchführbarkeitsanalyse und die Vorbereitung auf die Evaluation. Die Durchführbarkeitsanalyse ist optional, wird jedoch insbesondere Antragstellern und Entwicklern ohne vorherige Erfahrungen mit Evaluationen empfohlen. Die Durchführbarkeitsanalyse soll bestätigen, daß der Antragsteller und der Entwickler auf die Durchführung einer Evaluation gut vorbereitet sind, und beinhaltet zumindest eine Durchsicht der Sicherheitsvorgaben. Wenn der Erfolg einer Evaluation gesichert erscheint, werden eine Liste der erforderlichen **Evaluationsbeiträge**, ein Plan für ihre Auslieferung und ein **Evaluationsarbeitsplan** (EWP) erstellt. Es empfiehlt sich, Kontakt mit der Zertifizierungsstelle aufzunehmen und einen zwischen dem Antragsteller, dem Entwickler, der ITSEF und der Zertifizierungsstelle abgesprochenen Ablaufplan festzulegen.

1.2.18 Für gewöhnlich wird zwischen dem Antragsteller und einer ITSEF in Phase 1 ein Vertrag geschlossen. Dieser Vertrag berücksichtigt nationale Vorschriften und schließt üblicherweise eine Geheimhaltungsvereinbarung ein.

1.2.19 Der Evaluationsarbeitsplan (EWP) für einen bestimmten EVG stützt sich auf die Evaluationsbeiträge, den dazugehörigen Lieferplan und auf die Kriterien in den ITSEC. Die erforderliche Arbeit wird in Evaluationsaktivitäten unterteilt, die von Evaluatoren nach einem festen Zeitplan durchzuführen sind. Die Aufgabe der Erstellung des Evaluationsarbeitsplans (EWP) entspricht in etwa der Aufgabe der Planung innerhalb des Lebenszykluses der Software-Entwicklung. Für die Anwendung der Kriterien ist in den ITSEC keine feste Reihenfolge vorgeschrieben, jedoch sind einige Abfolgen besser geeignet und effizienter als andere. Einzelheiten zu dieser Frage sind in Teil 4 des ITSEM zu finden.

1.2.20 Phase II ist der wichtigste Teil des Evaluationsprozesses. Die Evaluatoren führen die nach den ITSEC vorgesehenen Evaluatoraufgaben aus. Dazu gehören auch Penetrationstests anhand der Liste **potentieller Schwachstellen** und sonstige Tests. Der technische Evaluationsbericht (ETR) wird in dieser Phase erstellt.

1.2.21 In Phase III übergibt die ITSEF das Endergebnis des Evaluationsprozesses, den technischen Evaluationsbericht (ETR), an den Antragsteller/Entwickler und an die Zertifizierungsstelle als Basisbeitrag zum Zertifizierungsprozeß. Aufgrund einer Verpflichtung zur Vertraulichkeit kann eine andere Vorgehensweise erforderlich sein. Da der ETR sensitive Informationen enthält, ist er kein öffentliches Dokument und unterliegt den Vorschriften des nationalen Regelwerks. Es könnte sich für die ITSEF auch die Notwendigkeit ergeben, der Zertifizierungsstelle im Zusammenhang mit dem ETR fachliche Unterstützung zukommen zu lassen.

1.2.22 Auf die Zertifizierung wird in Teil 2 des ITSEM eingegangen.

Behandlung von Mängeln

1.2.23 Stößt die ITSEF während einer Evaluation auf Mängel, werden diese für gewöhnlich zwischen dem Antragsteller, dem Entwickler und der ITSEF besprochen. In schwierigen Fällen soll die Zertifizierungsstelle zu Rate gezogen werden. Können Mängel nicht beseitigt werden, kann der Antragsteller sich für den Verzicht auf die Evaluation entscheiden. Die Vorschriften des nationalen Regelwerks kommen in allen Fällen zur Anwendung.

Begleitende und nachfolgende Evaluation

1.2.24 Eine Evaluation kann nach beendeter Entwicklung des EVG durchgeführt werden, das heißt als *nachfolgende Evaluation*, oder parallel zur Entwicklung des EVG, das heißt als *begleitende* Evaluation.

1.2.25 Der Hauptunterschied zwischen begleitenden und nachfolgenden Evaluationen besteht in der Verfügbarkeit der diversen **Darstellungen** des EVG, die als Evaluationsbeiträge vorgelegt werden. Bei einer nachfolgenden Evaluation stehen sämtliche in den ITSEC geforderten Evaluationsbeiträge von den Sicherheitsvorgaben bis zum betriebsbereiten EVG in der Regel direkt ab Beginn der Evaluation zur Verfügung. Bei einer begleitenden Evaluation werden die Evaluationsbeiträge vom Antragsteller/Entwickler dem Fortgang der Entwicklung entsprechend vorgelegt. Begleitende Evaluationen geben dem Antragsteller/Entwickler die Möglichkeit, auf entdeckte Mängel rasch zu reagieren.

1.2.26 Der Unterschied zwischen den beiden Evaluationsarten hat keine technischen Auswirkungen, sondern betrifft den organisatorischen Ablauf einer Evaluation, d.h. den Evaluationsarbeitsplan (EWP). Bei der begleitenden Evaluation müssen Abfolge und Zeithorizont der Evaluationsaktivitäten auf die Auslieferung der Evaluationsbeiträge abgestimmt werden. Penetrations- und sonstige Tests können erst nach Vorlage des betriebsbereiten EVG durchgeführt werden. Die möglichen Folgen von Verzögerungen und Wiederholungen müssen mit berücksichtigt werden.

Produkt- und Systemevaluation

1.2.27 Nach den ITSEC ist ein Produkt *ein IT-Software- und/oder Hardware-Paket, das eine bestimmte Funktionalität bietet, die zur Verwendung für oder zum Einbau in eine Vielzahl von Systemen entworfen wurde,* und ein System ist *eine spezifische IT-Installation mit einem bestimmten Zweck und einer bestimmten Betriebsumgebung.*

1.2.28 Produkt- und Systemevaluationen sind annähernd gleich; beide können begleitend oder nachfolgend sein. Der Hauptunterschied besteht in den Sicherheitsvorgaben. Bei einem System ist die Betriebsumgebung bekannt, und die Bedrohungen oder Sicherheitsziele sind real und können im einzelnen spezifiziert werden. Bei einem Produkt müssen die Bedrohungen oder die Sicherheitsziele durch Vorwegnahme des Zwecks und der Umgebung, für den bzw. in der das Produkt eingesetzt werden soll, angenommen werden und können nur in generischer Form ausgedrückt werden.

Reevaluation und Wiederverwendung von Evaluationsergebnissen

1.2.29 Wird ein Produkt oder ein System evaluiert oder zertifiziert, gilt das Zertifikat/der Zertifizierungsreport nur für die evaluierte Version und Konfiguration. Sicherheitsanforderungen und evaluierte Produkte oder Systemen sind aller Wahrscheinlichkeit nach Veränderungen unterworfen. Das Zertifikat/der Zertifizierungsreport hat unter Umständen für das veränderte Produkt oder System keine Gültigkeit, so daß eine Reevaluation erforderlich werden kann. Genauere Einzelheiten darüber sind in Teil 6, Anhang 6.D zu finden.

1.2.30 Im Verlauf des Reevaluationsprozesses kann sich die **Wiederverwendung** von Ergebnissen der früheren Evaluation des EVG als wünschenswert erweisen. Dieser Punkt wird in Teil 4, Kapitel 4.6 und in Teil 6, Anhang 6.F behandelt.

Teil 2 Regelwerke für die Zertifizierung

Inhalt

Kapitel 2.1 Einleitung

2.1.1 In den ITSEC, Version 1.2 heißt es in Absatz 1.31 unter Bezugnahme auf den Zertifizierungsprozeß: *Damit die Kriterien einen praktischen Wert haben, müssen sie durch Vorschriften für die Durchführung und Überwachung von unabhängigen Evaluationen, die durch qualifizierte und anerkannte nationale Zeritfizierungsstellen durchgeführt werden, ergänzt werden. Diese Stellen werden Zertifikate vergeben, in denen die Bewertung der Sicherheit des EVG bestätigt wird, welche er auf Grund einer ordnungsgemäß durchgeführten Evaluation erreicht hat*.

2.1.2 Aufgrund der Tatsache, daß derartige Regelwerke eine konsequente und korrekte Anwendung der im ITSEM dargelegte Methodik bei der Bewertung eines EVG anhand der ITSEC gewährleisten, sind sie eine Voraussetzung für die gegenseitige Anerkennung der von den einzelnen Zertifizierungsstellen vergebenen Zertifikate auf internationaler Ebene.

2.1.3 Unter der Voraussetzung, daß sämtliche Regelwerke die Übereinstimmung der Evaluationen mit dem ITSEM bei der Durchführung der in den ITSEC vorgesehenen Aufgaben des Evaluators gewährleisten, sollte davon ausgegangen werden können, daß das Ergebnis einer auf der Grundlage des einen Regelwerks durchgeführten Evaluation dasselbe ist wie das auf der Grundlage eines anderen Regelwerks erzielte Ergebnis.

Kapitel 2.2 Normen

2.2.1 Als allgemeine Orientierungshilfe für die Akkreditierung und den Betrieb von Prüflabors sind internationale und europäische Normen (ISO Guide 25 [GUI25] und EN45001 [EN45]) erarbeitet worden. Diese Normen schaffen einen Handlungsrahmen für die objektive Prüfung von Produkten aller Art, nicht nur aus dem IT-Bereich. Soweit es um die IT-Sicherheitsevaluation und -zertifizierung geht, ist die Einhaltung dieser Normen ein erstrebenswertes Ziel, insbesondere weil damit die Anerkennung einer Vereinbarung über die gegenseitige Anerkennung durch das European Committee for IT Testing and Certification (ECITC) erleichtert würde.

2.2.2 Es gibt allerdings für die IT-Sicherheit besonders typische Faktoren, aufgrund derer die buchstabengetreue Einhaltung derartiger Normen möglicherweise nicht wünschenswert oder schwer zu erreichen ist. Daher werden zur Zeit in verschiedenen Ländern Auslegungen von EN45001 für den Bereich der IT-Sicherheitsevaluation ausgearbeitet, die dem Geiste dieser Normen entsprechend Bestandteil der nationalen Vorschriften für Evaluationen, Zertifizierungen sowie für die Akkreditierung und Lizensierung von Evaluationsstellen werden sollen. Trotz dieser Auslegungen gibt es bei IT-Sicherheitsevaluationen einige Punkte, die eine Zertifizierungsstelle beobachten muß, will sie zu vergleichbaren Evaluationsergebnisse kommen.

Kapitel 2.3 Errichtung von ITSEFs

2.3.1 Besonders wichtig ist, daß Evaluationen von Evaluationsstellen mit Erfahrung in der IT-Sicherheit und der ITSEC-/ITSEM-Methodik durchgeführt werden. Diese Evaluationsstellen sollen sich daher um Einhaltung der Vorgaben von EN45001 und der entsprechenden Auslegungen für die IT-Sicherheit bemühen. Ein formales Akkreditierungsverfahren nach dieser Norm ist jedoch nicht zwingend vorgeschrieben. Dies hat dazu geführt, daß in einigen Ländern Lizenzierungsvorschriften für ITSEFs mit weitergehenden Anforderungen (insbesondere für den IT-Sicherheitsbereich) für eine Akkreditierung nach EN45001 festgelegt worden sind. Da diese erweiterten Anforderungen nicht in den Rahmen des ITSEM fallen, wird auf sie nicht näher eingegangen. Allerdings sind diese Aspekte entweder für die gegenseitige Anerkennung nicht relevant, oder es wird davon ausgegangen, daß sie in vertraglichen Vereinbarungen über eine gegenseitige Anerkennung geregelt werden.

2.3.2 Einige nationale Vorschriftenkataloge für Akkreditierungen oder Lizenzierungungen sind bereits in Kraft und unterliegen den obengenannten Anforderungen. Beteiligte, die an weiteren Auskünften, insbesondere über diese erweiterten Anforderungen, interessiert sind, sollten sich an die zuständige nationale Behörde wenden (siehe Kapitel 2.7).

Kapitel 2.4 Evaluation und Zertifizierung: Ziele und Nutzen

2.4.1 Hauptziel einer Zertifizierung ist die Erteilung einer unabhängigen Bestätigung, daß eine Evaluation nach den anerkannten Kriterien, Methoden und Verfahren ordnungsgemäß durchgeführt worden ist, und daß das Ergebnis der Evaluation mit den vorgelegten Fakten übereinstimmt. Im Falle eines von einer einzigen Zertifizierungsstelle aus überwachten Regelwerks hilft dies wiederum, eine Vertrauens-basis dafür herzustellen, daß die verschiedenen, diesem Regelwerk unterliegenden Evaluationsstellen denselben Anforderungen genügen, und daß die von zwei beliebigen Evaluationsstellen erzielten Ergebnisse gleichermaßen zuverlässig sind. Die wichtigsten Aspekte für diese Vertrauensbasis lassen sich in vier Grundprinzipien zusammenfassen:

a) **Unvoreingenommenheit**: Sämtliche Evaluationen müssen frei von Vorurteilen sein.

b) **Objektivität**: Die Eigenschaft eines Tests, aufgrund derer das Ergebnis mit einem Minimum an subjektivem Urteil oder subjektiver Meinung erzielt wird.

c) **Wiederholbarkeit**: Eine erneute Evaluation desselben EVG anhand derselben Sicherheitsvorgaben und durch dieselbe ITSEF führt zu der gleichen Gesamtentscheidung des Evaluators wie bei der Erstevaluation.

d) **Reproduzierbarkeit**: Die Evaluation desselben EVG anhand derselben Sicherheitsvorgaben durch eine andere ITSEF führt zu der gleichen Gesamtentscheidung des Evaluators wie bei der Erstevaluation.

2.4.2 In Verbindung mit dem Evaluations- und Zertifizierungsverfahren ergeben sich eine Reihe von Nutzwirkungen, die den verschiedenen Beteiligten mit Sicherheit Vorteile bringen. Einige davon sind nachstehend aufgeführt:

a) Der Hersteller/Entwickler/Antragsteller profitiert von einer Evaluation und Zertifizierung insoweit, als

- dem Kunden bewußt wird, daß eine erfolgreiche Evaluation durch einen unabhängigen Dritten die in bezug auf das Produkt gemachten Angaben bestätigt;
- ein entsprechendes Zertifikat den Zugang zu speziellen Märkten ermöglicht und die Akzeptanz fördert;
- zertifizierte Produkte als Bausteine für zertifizierte Systeme benutzt werden können;
- die Zertifizierung auch eine Aussage über die Qualität eines Produkts oder Systems und seine Entwicklung beinhaltet.

b) Die Anwender/Systemakkreditierer profitieren von einer Evaluation und Zertifizierung insoweit, als

- sie darauf vertrauen können, daß eine Bewertung durch einen Dritten die Angaben eines Herstellers in puncto Sicherheit bestätigt;
- ein Zertifikat eine nützliche Grundlage für Vergleiche zwischen verschiedenen Produkten liefert;
- sie gezeigt bekommen, wie sie dafür sorgen können, daß die sichere Konfiguration eines zertifizierten EVG nicht gefährdet wird.

c) Die Evaluatoren profitieren von einer Evaluation und Zertifizierung insoweit, als

- sie Nutzen aus der Erweiterung ihres Kundenkreises ziehen;
- die unabhängige Beaufsichtigung durch die Zertifizierungsstelle den Evaluatoren als Maßstab für die ordnungsgemäße Erfüllung ihrer Pflichten dient.

d) Für die Regelwerke für Zertifizierungen ergeben sich Vorteile in Form von

- Möglichkeiten des Vergleichs, der Entwicklung und der Pflege internationaler Normen;
- einer Bewertung interner Normen anhand eines Katalogs internationaler Kriterien;
- einer Ermutigung von Antragstellern, die Absatzmöglichkeiten für ihre Produkte zu erweitern.

Kapitel 2.5 Das Regelwerk für die Zertifizierung

2.5.1 Zu den Hauptzielen einer Zertifizierungsstelle gehören erstens die Schaffung der notwendigen Voraussetzungen für die Gewährleistung der Unverfälschtheit und Konsistenz der Arbeit aller ITSEFs innerhalb eines Regelwerks und der Gültigkeit, Wiederholbarkeit und Reproduzierbarkeit der von ihnen gezogenen Schlußfolgerungen, und zweitens bei Einzelevaluationen die Erteilung einer unabhängigen Bestätigung, daß diese nach anerkannten Kriterien, Methoden und Verfahren durchgeführt worden sind. Um diese Ziele verwirklichen zu können, muß die Zertifizierungsstelle (unter anderem) folgende Aufgaben übernehmen:

a) Sie genehmigt die Beteiligung von ITSEFs an dem Regelwerk und sorgt so für die Erfüllung der Anforderungen des fraglichen Regelwerks;

b) sie überwacht die Arbeit der ITSEFs und die Befolgung und Anwendung der ITSEC und des ITSEM durch diese Beteiligte und gibt, soweit erforderlich, zusätzliche Hinweise heraus;

c) sie überwacht jede von einer ITSEF durchgeführte Evaluation;

d) sie überprüft sämtliche Evaluationsreports, um die Folgen der Ergebnisse für die Sicherheit abzuschätzen, und um sicherzustellen, daß sie mit den ITSEC und dem ITSEM übereinstimmen;

e) sie erstellt Zertifizierungsreports;

f) sie veröffentlicht Zertifikate und Zertifizierungsreports.

2.5.2 Alle diese Aktivitäten werden auf der Grundlage eines Regelwerks für die Zertifizierung durchgeführt. Die besonders wichtige Konsistenz der Normen (und somit auch die Gültigkeit und Zuverlässigkeit der Ergebnisse) zwischen unterschiedlichen ITSEFs kann nur im Rahmen eines derartigen Regelwerks erreicht werden. Diese Konsistenz ist nicht nur aus der Sicht des Einzelkunden und seines Vertrauens in eine Evaluation (und somit auch in das evaluierte Produkt oder System) so besonders wichtig, sondern auch weil sie eine Voraussetzung für eine gegenseitige Anerkennung auf internationaler Ebene ist.

2.5.3 Zu den übrigen Aufgaben eines Regelwerks für die Zertifizierung gehören folgende: Die Bestimmung der verschiedenen Arten von Produkten und Systemen, die evaluiert werden können, die Ausgabe von Zertifikaten und Zertifizierungsreports und ihre spätere Pflege (einschließlich Schutz vor Mißbrauch), die Herausgabe von Unterlagen über das Regelwerk und seine Funktionsweise sowie weitere Aspekte der routinemäßigen Verwaltung des Regelwerks.

2.5.4 Für einzelne Regelwerke speziell festgelegte nationale Anforderungen fallen nicht in den Rahmen des ITSEM. Weitere Auskünfte über die einzelnen **nationalen Regelwerke** erteilt die zuständige Behörde, die in Kapitel 2.7 unter den dort aufgeführten Kontaktstellen zu finden ist.

Kapitel 2.6 Inhalt von Produktzertifikaten/Zertifizierungsreports

2.6.1 Zertifikate und Zertifizierungsreports werden der Öffentlichkeit zugänglich gemacht.

2.6.2 Zertifikate und Zertifizierungsreports sollen zumindest folgendes enthalten:

a) **Einleitung**:

- Vorbereitungsmaterial entsprechend der im nationalen Regelwerk geübten Praxis.

b) **Zusammenfassung**:

- die Identität der ITSEF;
- die Kennung des Evaluationsgegenstands (EVG) einschließlich Ausgaben-/Release-Nummer;
- die von der Zertifizierungsstelle zugewiesene Evaluationskennung;
- eine Zusammenfassung der wichtigsten Schlußfolgerungen der Evaluation;
- die Identität des Entwicklers (ggf. einschließlich Unterauftragnehmer);
- die Identität des Antragstellers;
- die konkret erreichte Evaluationsstufe.

c) **Produktübersicht**:

- eine Beschreibung der evaluierten Konfigurationen;
- Hardware-Beschreibung;
- Firmware-Beschreibung;
- Software-Beschreibung;
- Dokumentationsbeschreibung.

d) **Die Evaluation**:

- eine kurze Beschreibung der Sicherheitsvorgaben, einschließlich einer Beschreibung der Sicherheitseigenschaften des Evaluationsgegenstands;
- Verweis auf den **technischen Evaluationsbericht (ETR)**;
- die Identität der akkreditierten Evaluationsstelle für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEF);
- Zusammenfassung der wichtigsten Schlußfolgerungen der Evaluation.

e) **Zertifizierung**:

- Geltungsumfang des Zertifikats (z.B. irgendwelche Einschränkungen im Hinblick auf die Anwendung des EVG).

Kapitel 2.7 Liste der Kontaktstellen

2.7.1 Nachstehend folgt eine Liste der Kontaktstellen, die Auskünfte über Evaluationen und Zertifizierungen geben können:

In Frankreich:

Service Central de la Sécurité des Systèmes d'Information
18 Rue du Docteur Zamenhof
F-92131 ISSY LES MOULINEAUX

In Deutschland:

Akkreditierstelle:

Bundesamt für Sicherheit in der Informationstechnik
Referat II 4
Postfach 20 03 63
D-53133 BONN

Zertifizierungsstelle:

Bundesamt für Sicherheit in der Informationstechnik
Referat II 3
Postfach 20 03 63
D-53133 BONN

In den Niederlanden:

National Security Service
P.O.Box 20010
NL-2500 EA THE HAGUE

Netherlands National Comsec Agency
Bezuidenhoutseweg 67
P.O. Box 20061
NL-2500 EB THE HAGUE

In Großbritannien:

Head of the Certification Body
UK IT Security Evaluation and Certification Scheme
Certification Body
P.O. Box 152
CHELTENHAM
Glos GL52 5UF

Leerseite

Teil 3 Grundsätze, Konzepte und Prinzipien

Inhalt

Abbildungen

Kapitel 3.1 Einleitung

3.1.1 Dieser Teil beschreibt die den ITSEC zugrundeliegenden Evaluationsgrundsätze und führt in die Grundprinzipien der Evaluationsarbeit ein. Er stellt im Evaluationsprozeß verwendete Konzepte und Begriffe vor. Er liefert die fachliche Grundlage für die nationalen Regelwerke für die Evaluation und die Zertifizierung (ITSEM, Teil 2) und den Evaluationsprozeß (ITSEM, Teil 4). Die Prinzipien werden im ITSEM, Teil 4, ausführlich behandelt und umgesetzt.

.

Kapitel 3.2 Allgemeine Evaluationsgrundsätze

Vertrauen und Vertrauenswürdigkeit

3.2.1 Hauptziel einer Evaluation ist die Schaffung von Vertrauen, daß der EVG die eigenen Sicherheitsvorgaben erfüllt. Die Evaluation schafft auch ein bestimmtes Maß an Vertrauen in das Nichtvorhandensein **ausnutzbarer Schwachstellen**. Der Nutzen der in den Sicherheitsvorgaben enthaltenen Sicherheitsziele wird während der Evaluation nicht bewertet, da sie von der speziellen Anwendung des EVG abhängen.

3.2.2 Das durch eine Evaluation geschaffene Maß an Vertrauen hängt von der Evaluationsstufe und von der Stärke der Mechanismen ab. Je höher die Evaluationsstufe, desto größer die gelieferte und genutzte Menge an relevanten Informationen, der erforderliche Evaluationsaufwand und die daraus resultierende Vertrauenswürdigkeit. Somit kann eine Evaluation als einzelne, aber komplexe Bewertung betrachtet werden, die mit einem durch die Evaluationsstufe charakterisierten Grad an Genauigkeit durchgeführt wird. Folglich soll die Evaluationsstufe und die Stärke der Mechanismen umso höher sein, je mehr man sich auf die von einem EVG bereitgestellten **Gegenmaßnahmen** stützen muß, z.B. um ein hohes Risiko auf ein akzeptierbares Maß zu reduzieren. Es besteht eine größere Wahrscheinlichkeit, daß sich der EVG wie erwartet verhält und den Bedrohungen angemessen entgegenwirkt.

3.2.3 Vertrauen in die Sicherheit eines Produkts oder Systems entwickelt sich sowohl aus der Prüfung des Produkts oder Systems und seiner **Darstellungen** als auch aus der Kenntnis seines Entwicklungs-prozesses.

3.2.4 Den größten Beitrag zur Vertrauenswürdigkeit liefert die Prüfung von Darstellungen des Produkts oder Systems selbst. Ein anhand einer Qualitätsnorm wie etwa ISO 9001 akkreditierter Entwickler ist wahrscheinlich eher in der Lage, angemessene Darstellungen zu erstellen, jedoch kann eine solche Akkreditierung auf keinen Fall irgendeinen Teil der Evaluation ersetzen.

Wiederholbarkeit, Reproduzierbarkeit, Unvoreingenommenheit und Objektivität

3.2.5 Im Zusammenhang mit der Evaluation und Zertifizierung der IT-Sicherheit werden wie im wissenschaftlichen Bereich und bei Tests *Wiederholbarkeit*, *Reproduzierbarkeit*, *Unvoreingenommenheit* und *Objektivität* als wichtige Prinzipien betrachtet.

3.2.6 Eine Evaluation ist wiederholbar, wenn die erneute Evaluation desselben EVG anhand derselben Sicherheitsvorgaben durch dieselbe ITSEF zu der gleichen Gesamtentscheidung des Evaluators wie bei der Erstevaluation führt.

3.2.7 Ein Evaluationsergebnis ist reproduzierbar, wenn die Evaluation desselben EVG anhand derselben Sicherheitsvorgaben durch eine andere ITSEF zu der gleichen Gesamtentscheidung des Evaluators wie bei der Erstevaluation führt.

3.2.8 Eine Evaluation wird unvoreingenommen durchgeführt, wenn sie nicht durch irgendein bestimmtes Ergebnis beeinflußt wird.

3.2.9 Eine Evaluation wird objektiv durchgeführt, wenn das Ergebnis auf tatsächlichen Fakten, unbeeinflußt von den Gefühlen oder Ansichten der Evaluatoren, beruht.

3.2.10 Diese vier Prinzipien werden von einer Zertifizierungsstelle im Rahmen eines nationalen Regelwerks durchgesetzt. Die Zertifizierungsstelle sorgt insbesondere dafür, daß die Wiederholbarkeit und Reproduzierbarkeit der Prüfergebnisse auf das Evaluationsergebnis als Ganzes ausgedehnt wird.

Verständnis

3.2.11 Die Evaluationskriterien beschreiben den vom Antragsteller einer Evaluation bzw. dem Entwickler zu führenden Nachweis und die vom Evaluator zu prüfenden Punkte. Die Evaluation basiert auf den vom Antragsteller/Entwickler gelieferten Informationen. Die durch eine Evaluation erzielte Vertrauenswürdigkeit hängt von der Kenntnis des EVG und seines Verhaltens ab. Je sachbezogener und vollständiger die Informationen über den EVG sind, desto verständlicher wird der EVG. Das Ergebnis ist ein größeres Vertrauen in die Fähigkeit des EVG, die eigenen Sicherheitsvorgaben zu erfüllen. Ihren Niederschlag finden diese Fakten in den für Antragsteller/Entwickler geltenden ITSEC-Anforderungen hinsichtlich der Bereitstellung von **Evaluationsbeiträgen** zur Konstruktionsphase als Spezifikationen des EVG auf unterschiedlichen Abstraktionsstufen.

3.2.12 Eine Evaluation besteht aus einer Kombination von Beobachtung, Theorie und Experiment. Sich mit dem EVG vertraut zu machen, ist die erste Voraussetzung für gute Evaluationsarbeit. Dies geschieht durch Bewerten der Sicherheitsvorgaben und der anderen, die Korrektheitskriterien betreffenden, Evaluationsbeiträge. Anhand ihrer Kenntnis des EVG und seiner Sicherheitsvorgaben können die Evaluatoren diesen mit Blick auf die Wirksamkeitskriterien untersuchen, d.h., ob der EVG in irgendeiner Weise gegen die Anforderungen der Sicherheitsvorgaben verstoßen kann oder ob er anfällig gegen zu erwartende Bedrohungen ist.

3.2.13 Im allgemeinen sind EVG viel zu komplex, als daß allein durch Tests nachgewiesen werden kann, ob sie die Sicherheitsvorgaben erfüllen. Erschöpfende Tests sind nicht möglich. Daher wird die Vertrauensbasis für die Evaluation von den Evaluatoren dadurch geschaffen, daß sie sich durch Auswerten der vorhandenen Dokumentation über seine Konstruktion und seinen Betrieb sowie durch Tests mit dem EVG vertraut machen. Gewisse Zweifel hinsichtlich der Übereinstimmung des EVG mit den Sicherheitsvorgaben werden immer bestehen bleiben. Volle Vertrauenswürdigkeit wird es nie geben, dafür aber den Nachweis einer erhöhten Wahrscheinlichkeit, daß der EVG die für ihn geltenden Sicherheitsvorgaben erfüllt. Im allgemeinen ist es wünschenswert, die verbleibende Unsicherheit auf ein Mindestmaß zu reduzieren. Je höher die Evaluationsstufe, desto besser muß der Evaluator sich mit dem EVG auskennen.

Prinzipien der Modularisierung und der Software-Entwicklung

3.2.14 Die Modularisierung und andere Prinzipien der Software-Entwicklung wie etwa die Datenabschottung usw. sind in der Regel eine gute Ausgangsbasis für die Unterstützung und Begrenzung der erforderlichen Evaluationsarbeit. Sie tragen zur Feststellung **potentieller Schwachstellen** bei. Eine gut dokumentierte Entwicklung unter Verwendung klar definierter Begriffe hilft dem Evaluator, den EVG zu verstehen. Programmiersprachen mit klar definierter Syntax und Semantik sind ein Beispiel, das für die Implementierungsphase von Belang ist. Entwicklung auf der Grundlage einer soliden Software-Entwicklungspraxis erleichtert die Arbeit der Evaluatoren.

Evaluationsprozeß

3.2.15 Es soll eine klar definierte Evaluationsmethode verwendet werden, die von allen Beteiligten verstanden wird. Die einzelnen Evaluationsprozesse für bestimmte EVG werden anhand der Kriterien in den ITSEC, der Evaluationsgrundsätze und der Evaluationsprinzipien, des **nationalen Regelwerks** und der in Teil 4 des ITSEM beschriebenen Evaluationsprozesse erarbeitet (siehe Abbildung 3.2.1). Der Evaluationsprozeß soll aus Gründen der Vereinfachung und wegen der größeren Effizienz der Überwachung und Gegenüberstellung der Ergebnisse standardisiert werden. In der Praxis wird die Evaluationsmethode im **Evaluationsarbeitsplan** (EWP) und im Rahmen der Durchführung der aufgezeigten Evaluatoraktivitäten umgesetzt. Aufgrund der enormen Vielfalt möglicher Sicherheits-vorgaben und EVG ist eine detaillierte Beschreibung nicht möglich. Die Erarbeitung der Evaluationsmethode ist in Teil 4 des ITSEM sowie in nationalen Regelwerken beschrieben.

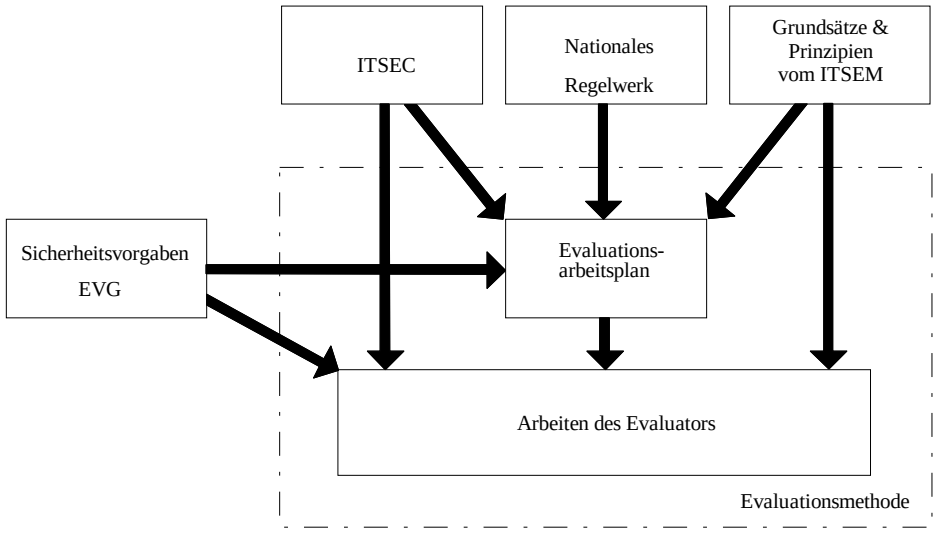


Abbildung 3.2.1 Ableitung des Evaluationsprozesses

3.2.16 Die konkrete Darlegung der Evaluationsmethode anhand eines bestimmten Evaluationsprozesses wird beeinflußt durch

a) Evaluationsattribute (begleitende oder nachfolgende Evaluation);

b) EVG-Attribute (System oder Produkt).

3.2.17 Diese Attribute sind in Teil 1 des ITSEM (1.2.24 - 1.2.28) beschrieben.

Kapitel 3.3 Sicherheits- und Evaluationskonzepte

3.3.1 Im vorliegenden Kapitel werden zusätzlich zu den in Teil 1 des ITSEM eingeführten Konzepten als Orientierungshilfe für die Auslegung bestimmter Evaluatoraktivitäten eine Reihe von ITSEC-Konzepten und ITSEC-Begriffen genauer erläutert. Zu diesen Konzepten und Begriffen gehören folgende:

a) Sicherheitsziele, **Werte** und Bedrohungen;

b) Korrektheit und Wirksamkeit;

c) Komponenten, Funktionen und Mechanismen;

d) sicherheitsspezifische, sicherheitsrelevante und nicht sicherheitsrelevante Funktionen und Komponenten;

e) Trennung der Funktionalität;

f) Verfeinerung, **Fehler** und Fehlerbehebung;

g) Konstruktionsschwachstellen und **operationelle Schwachstellen**;

h) Stärke der Mechanismen;

i) ausnutzbare Schwachstellen;

j) Penetrationstests.

3.3.2 Es ist darauf hinzuweisen, daß nationale Regelwerke eine weitergehende Auslegung dieser und anderer Begriffe vorsehen können.

Sicherheitsziele, Werte und Bedrohungen

3.3.3 In den Sicherheitsvorgaben sind die Sicherheitsziele des EVG festgeschrieben, wobei jedes Ziel (es muß mindestens ein Sicherheitsziel vorhanden sein) auf Bedrohungen und Werten bezogen wird. Ein Beispiel eines Ziels könnte wie folgt aussehen:

a) Der EVG muß die Preisgabe sensitiver Informationen an Mitarbeiter mit unzureichender Berechtigung für den Zugriff auf Informationen verhindern.

b) Der EVG muß sicherstellen, daß mit der Überkreuzprüfung von Kundendaten befaßte Aufsichtspersonen ihre Amtsbefugnisse beispielsweise nicht zu betrügerischen Zwecken mißbrauchen.

3.3.4 In den Sicherheitsvorgaben sind die Bedrohungen aufgelistet, denen der EVG ausgesetzt ist, und die Werte, die er schützen muß. Nach den ITSEC müssen Bedrohungen und Werte so identifiziert werden, daß der Evaluator prüfen kann, ob die Sicherheitsziele und die einzelnen Listen der Bedrohungen und Werte konsistent sind.

3.3.5 In den Sicherheitsvorgaben werden außerdem die Gegenmaßnahmen aufgezeigt, die zum Schutz der Werte vor den Bedrohungen und damit zur Erfüllung der Sicherheitsziele implementiert werden müssen. Wenn die Gegenmaßnahmen mit technischen Mitteln durchgesetzt werden müssen, d.h. innerhalb des Computersystems selbst, werden sie als sicherheitsspezifische Funktionen bezeichnet. Diese Funktionen spezifizieren die Sicherheitsfunktionalität des EVG (anstelle der Mechanismen, die zur Implementierung der Sicherheitsfunktionen verwendet werden). In den ITSEC wird empfohlen, diese Funktionen unter den in Kapital 2 der ITSEC genannten generischen Oberbegriffen oder durch Verwendung einer vordefinierten Funktionalitätsklasse zu beschreiben. In den Sicherheitsvorgaben werden außerdem die spezifischen Ziele jeder Gegenmaßnahme präzisiert, z.B., der EVG verwendet zur Feststellung und Verifizierung einer behaupteten Identität eine Identifikations- und **Authentisierung**sfunktion.

3.3.6 Spezifische Bedrohungen und Werte sind in den Sicherheitsvorgaben für ein Produkt schwerer zu spezifizieren als für ein System. Somit kann ein Anwender mit Hilfe der Produktbeschreibung herausfinden, wie seine tatsächlichen Werte durch Verwendung der in dem Produkt vorhandenen Gegenmaßnahmen gegen die tatsächlichen Bedrohungen geschützt werden können. Die Produktbeschreibung wird daher wahrscheinlich eher detaillierte Angaben über Sicherheitsziele als über bekannte Bedrohungen und Werte enthalten.

Korrektheit und Wirksamkeit

3.3.7 Von grundlegender Bedeutung für die Kriterien in den ITSEC ist die Trennung zwischen Funktionalität und Vertrauenswürdigkeit und die weitere Aufteilung in Vertrauen in die Korrektheit der sicherheitsspezifischen Funktionen und Vertrauen in die Wirksamkeit dieser Funktionen.

3.3.8 Während einer Evaluation müssen zwei entscheidende Fragen beantwortet werden:

a) Beweisen die Evaluationsbeiträge, daß der EVG die Sicherheitsvorgaben korrekt implementiert? (Korrektheit)

b) Sind die im EVG implementierten Sicherheitsmaßnahmen gegen die identifizierten Bedrohungen wirksam und sind sie frei von ausnutzbaren Schwachstellen? (Wirksamkeit)

3.3.9 Die Korrektheit beschäftigt sich mit zwei Hauptfragen:

a) Beinhalten die Sicherheitsvorgaben eine geeignete Beschreibung der sicherheitsspezifischen Funktionen und liefern die Evaluationsbeiträge den Beweis, daß diese Funktionen im EVG korrekt implementiert sind?

b) Ist ein disziplinierter Entwicklungsansatz verfolgt worden, so daß ein ausreichendes Maß an Vertrauen in die **korrekte Verfeinerung** der Anforderungen geschaffen werden kann?

3.3.10 Die Wirksamkeit soll als eine Checkliste betrachtet werden, die verschiedene Aspekte enthält, aufgrund derer ein EVG eine Evaluation nicht bestehen kann. Sie beschäftigt sich mit folgenden Fragen:

a) Sind die sicherheitsspezifischen Funktionen in der Lage, die spezifizierten Werte vor den in den Sicherheitsvorgaben aufgeführten Bedrohungen zu schützen? (Eignung der Funktionalität)

b) Ist der Entwurf so gestaltet, daß bei korrekter Implementierung der einzelnen sicherheitsspezifischen Funktionen der EVG in seiner Gesamtheit gemessen an seinen Sicherheitsvorgaben sicher ist? (Zusammenwirken der Funktionalität)

c) Besitzt der EVG als Ganzes und in seiner Betriebsumgebung irgendwelche ausnutzbaren Schwachstellen? (Schwachstellenbewertungen, Stärke der Mechanismen und Benutzerfreund-lichkeit)

Komponenten, Funktionen und Mechanismen

3.3.11 Der EVG besteht aus einzelnen Komponenten. Die Komponenten bestehen ihrerseits aus Komponenten, wobei die vom Entwickler auf der niedrigsten Entwurfsebene ausgewiesenen Komponenten Basiskomponenten genannt werden, z.B. Kompilierungseinheiten.

3.3.12 Eine Komponente kann mehr als eine Funktion implementieren. Im Falle einer Basiskomponente werden die Teile, die die Implementierung jeder derartigen Funktion enthalten, als Funktionseinheit bezeichnet. Es ist wichtig, daß die in den Sicherheitsvorgaben ausgewiesenen Sicherheitsfunktionen auf Komponenten aller in die Evaluation einbezogenen Abstraktionsstufen abgebildet werden können.

3.3.13 Die Logik oder der Algorithmus zur Implementierung einer Funktion wird Mechanismus genannt. Evaluationsaspekte zur Frage der Mechanismen sind in Teil 6, Anhang 6.C zu finden.

Sicherheitsspezifische, sicherheitsrelevante und nicht sicherheitsrelevante Funktionen und Komponenten

3.3.14 Die Begriffe sicherheitsspezifisch, sicherheitsrelevant und nicht sicherheitsrelevant schließen zwar einander aus, sind aber umfassend, d.h., jeder Aspekt der EVG-Funktionalität kann genau einer dieser drei Kategorien zugewiesen werden. Diese drei Attribute können für Funktionen und Komponenten verwendet werden.

3.3.15 Funktionen sind nicht sicherheitsrelevant, wenn die Erfüllung der Sicherheitsziele nicht von ihnen abhängt. Sicherheitsspezifische Funktionen sind alle Funktionen des EVG, die direkt zum Erreichen der Sicherheitsziele beitragen. Sicherheitsrelevante Funktionen tragen zum sicheren Funktionieren des EVG bei und leisten häufig nicht nur Dienste für die sicherheitsspezifischen Funktionen, sondern auch für nicht sicherheitsbezogene Funktionen. Für gewöhnlich hängen sicherheitsspezifische Funktionen vom korrekten Betrieb der sicherheitsrelevanten Funktionen ab.

3.3.16 Wenn mindestens eine der in einer Komponente implementierten Funktionen sicherheitsspezifisch ist, dann ist auch die Komponente sicherheitsspezifisch. Wenn keine der Funktionen sicherheitsspezifisch oder sicherheitsrelevant ist, dann ist die Komponente selbst auch nicht sicherheitsrelevant.

Trennung der Funktionalität

3.3.17 Eine Trennung kann nachgewiesen werden, indem (mit entsprechender Genauigkeit) dargelegt wird, daß unabhängig davon, welches Verhalten die nicht sicherheitsspezifischen Komponenten aufzeigen, die Sicherheitsziele eingehalten werden, sofern die sicherheitsspezifischen Funktionen korrekt funktionieren.

3.3.18 Die Trennung zwischen sicherheitsspezifischen, sicherheitsrelevanten und nicht sicherheitsrelevanten Funktionen ist eine Frage der Architektur, die nicht allein von Sicherheitsüberlegungen bestimmt wird. Durch das Referenzmonitorkonzept ist bekannt, wie Vertraulichkeitsanforderungen zur Unter-stützung der Funktionalität getrennt werden können. Dieses Konzept kann jedoch nicht mit Erfolg auf den Bereich der Integrität und der Verfügbarkeit ausgedehnt werden.

Verfeinerung, Fehler und Fehlerbehebung

3.3.19 In den Kriterien in den ITSEC ist keine bestimmte Entwicklungsmethode vorgeschrieben, doch es wird davon ausgegangen, daß die Entwicklung eines EVG mehrere Verfeinerungs- und Integrationsstufen umfaßt. Am Ende des Entwicklungsprozesses liegen Darstellungen des EVG auf verschiedenen Abstraktionsstufen vor. Die Sicherheitsvorgaben befinden sich auf der höchsten Abstraktionsstufe. Der betriebsbereite EVG in Form eines ausführbaren Codes oder eines elektronischen Schaltungsaufbaus ist die konkreteste und detaillierteste Darstellung. In den Korrektheitskriterien der ITSEC bezeichnen die Begriffe *Sicherheitsvorgaben*, *Architekturentwurf*, *Feinentwurf* und *Implementierung* unterschiedliche Abstraktionsstufen. Der Feinentwurf zum Beispiel ist weniger abstrakt und detaillierter als der Architekturentwurf. Daher wird der Feinentwurf als Verfeinerung des Architekturentwurfs bezeichnet.

3.3.20 Eine in den Sicherheitsvorgaben beschriebene Funktion kommt auf unterschiedlichen Abstraktions- oder Detailstufen, einschließlich ihrer Implementierung im EVG, vor. Die Beschreibung dieser Funktion auf einer gegebenen Abstraktionsstufe in dieser Hierarchie wird als korrekte Verfeinerung bezeichnet, wenn die Gesamtheit der auf dieser (niedrigeren) Abstraktionsstufe beschriebenen Wirkungen die auf der vorhergehenden (höheren) Abstraktionsstufe beschriebenen Wirkungen aufweist.

3.3.21 Eine Nichterfüllung der Korrektheitskriterien wird als Fehler bezeichnet. Eine typische Ursache ist eine Inkonsistenz bezüglich der Verfeinerung. Man könnte es auch als Problem der Abbildbarkeit oder eine Inkonsistenz zwischen zwei Darstellungen des EVG betrachten. Zweck der ITSEC-Korrektheitskriterien ist, Hilfestellung beim Nachweis der Tatsache zu geben, daß jede den Evaluatoren gelieferte Darstellung eine korrekte Verfeinerung der entsprechenden Darstellung auf der höheren Stufe ist. Die ITSEC-Korrektheitskriterien für die Konstruktion versuchen, den Beweis zu erbringen, daß der EVG eine korrekte Verfeinerung der Sicherheitsvorgaben ist. Die Abbildung zwischen Sicherheitsvorgaben und EVG wird durch Abbildungen innerhalb der Zwischenstufen, wie in Abbildung 3.3.1 dargestellt, erreicht.

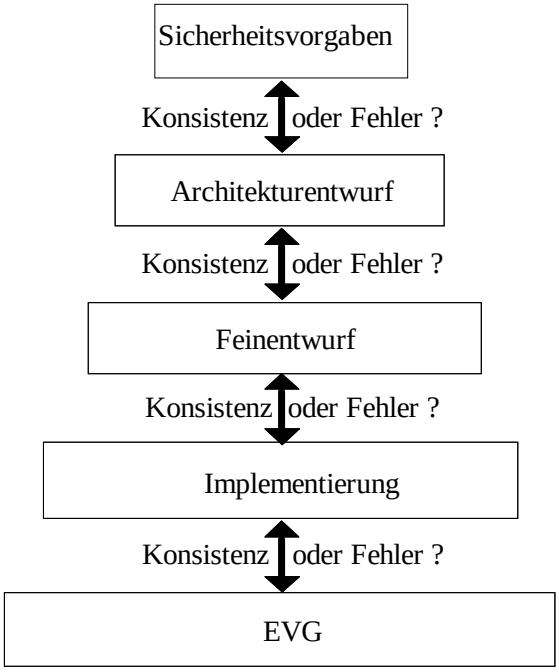


Abbildung 3.3.1 Darstellungen des EVG und Korrektheit

3.3.22 Ein Fehler wird dadurch korrigiert, daß mindestens eine der Darstellungen modifiziert wird. Nehmen wir beispielsweise an, auf einer Entwurfsstufe gäbe es eine Darstellung einer Identifikations- und Authentisierungsfunktion. Im Entwurf wird genau spefiziert, was im Falle eines Überlaufens der Tabellen mit den Anwender-ID und Paßwörtern zu unternehmen ist. Wenn auf der nächsttieferen Entwurfsstufe bei einem Überlaufen der Tabellen etwas anderes unternommen wird, ist dies ein Fehler, da eine auf einer Stufe spezifizierte Wirkung auf der nächsten nicht vorhanden ist. Aus diesem Grund

a) wird entweder der Entwurf auf der ersten Stufe dahingehend modifiziert, daß die auf der nächsten Stufe konkret veranlaßten Maßnahmen spezifiziert werden. Das kann Auswirkungen auf höhere Entwurfsstufen wie etwa den Architekturentwurf und vielleicht auch die Sicherheitsvorgaben haben; oder

b) wird der Entwurf auf der nächsten Stufe dahingehend modifiziert, daß die auf der ersten Stufe vorgeschriebene Maßnahme spezifiziert wird. Dies wirkt sich normalerweise auf die unterhalb der nächsten Stufe liegenden Entwurfs- und Implementierungsstufen aus.

3.3.23 Eine andere typische Ursache für einen Fehler ist die Vorlage unzureichender Nachweise durch den Antragsteller/Entwickler. Unentdeckt gebliebene Fehler könnten zu potentiellen Schwachstellen führen. Typographische Fehler in der Dokumentation des Antragstellers/Entwicklers werden normalerweise nicht als Fehler nach den ITSEC eingestuft.

Konstruktionsschwachstellen und operationelle Schwachstellen

3.3.24 Eine **Schwachstelle** ist eine Sicherheitsschwäche in einem EVG, die von einem Angreifer dazu benutzt werden kann, eine Bedrohung auszuüben und einen Wert zu gefährden oder eine Gegenmaßnahme zu überwinden. Es gibt Konstruktionsschwachstellen und operationelle Schwachstellen. **Konstruktionsschwachstellen** nutzen irgendeine Eigenschaft des EVG aus, die während seiner Konstruktion eingebracht wurde, z.B. die Unfähigkeit, einen Pufferspeicher zu löschen. Operationelle Schwachstellen nutzen Schwächen in nichttechnischen Gegenmaßnahmen aus, um die Sicherheit des EVG zu verletzen, z.B. die Preisgabe des eigenen Paßworts an einen Dritten.

3.3.25 Eine Verfeinerung führt oft zu einer weiteren Differenzierung auf der niedrigeren Abstraktionsstufe. Die Wirkungen auf der niedrigeren Stufe sind eine "Obermenge" der Wirkungen auf der höheren Stufe. Die zusätzlichen Details sind Quellen potentieller Konstruktionsschwachstellen. So wird beispielsweise durch die Einbringung einer Sperrvariablen, die auf der höheren Abstraktionsstufe nicht vorhanden ist, eine potentielle Schwachstelle eingeführt. Ist die Kontrolle des Informationsflusses ein Sicherheitsziel innerhalb der Sicherheitsvorgaben und kann die Sperrvariable zum Anlegen eines verdeckten Kanals benutzt werden, kann die Schwachstelle auswertbar sein.

3.3.26 Potentielle Schwachstellen aufgrund von Verfeinerungen werden von den Evaluatoren bei der Durchführung der Korrektheitsbewertung identifiziert. Die Bewertung der Konstruktionsschwachstelle entscheidet darüber, ob solche Schwachstellen auswertbar sind oder nicht.

3.3.27 Operationelle Schwachstellen betreffen den Grenzbereich zwischen IT- und Nicht-IT-Gegenmaßnahmen, z.B. Betriebsprozeduren, die sich mit der materiellen Sicherheit, nichtelektronischen Formen der Schlüsselverwaltung und der Ausgabe von Sicherheitsplaketten befassen. Nicht-IT-Maßnahmen sind für die Evaluatoren von Belang,

a) wenn sie als Teil der Betriebsdokumentation erscheinen, oder

b) wenn die Sicherheitsvorgaben auf der Grundlage einer System-Sicherheitspolitik formuliert sind (siehe ITSEC Absatz 2.8 - 2.15) oder als Teil der Produktbeschreibung erscheinen (siehe ITSEC Absatz 2.16 - 2.17).

3.3.28 Die Nicht-IT-Gegenmaßnahmen, von denen die Sicherheit des EVG abhängt, werden als Behauptungen ausgewiesen, die die Betriebsumgebung des EVG betreffen. Zum Beispiel kann behauptet werden, daß nur Firmenangehörigen Zugang zu dem System gewährt wird und daß es Sache der Nicht-IT-Gegenmaßnahmen ist zu gewährleisten, daß diese Behauptung eingehalten wird. Die Evaluatoren gehen von der Annahme aus, daß diese Behauptung stimmt. Wenn die Kombination aus IT- und Nicht-IT-Gegenmaßnahmen in den Rahmen der Evaluation fällt, sollen die Evaluatoren ermitteln, ob die Kombination irgendwelche potentiellen Schwachstellen enthält.

Stärke der Mechanismen

3.3.29 Die ITSEC-Definitionen für die drei Bewertungen der Stärke der Mechanismen - *niedrig*, *mittel* und *hoch* - sind ein grober Maßstab, um die Bedürfnisse auf Anwenderseite zum Ausdruck zu bringen. Die Definitionen bieten keine detaillierten Möglichkeiten der Bewertung während der Evaluation. Man muß zwischen dem erforderlichen Arbeitsaufwand zur Entdeckung einer Schwachstelle, zur Festlegung einer Beschreibung für eine Schwachstelle (z.B. man liest darüber in einer Zeitschrift) und schließlich zur Ausnutzung einer Schwachstelle aufgrund einer Beschreibung unterscheiden. Die Betonung bei der Bewertung liegt auf dem erforderlichen Arbeitsaufwand zur Ausnutzung einer Schwachstelle.

3.3.30 Der Evaluator stützt sich bei der Bewertung der Stärke der Mechanismen auf die Aspekte Fachkenntnisse, Gelegenheit und Ressourcen. Praktischer in der Anwendung sind die vier Parameter Fachkenntnisse, geheime Absprache, Zeit und Ausstattung.

3.3.31 Die Bewertung soll für alle denkbaren und vertretbaren Kombinationen der Werte für die einzelnen Parameter durchgeführt werden. Dies kann durch Verwendung von Tabellen oder mit Hilfe eines Regelkatalogs geschehen. Einzelheiten zu der Bewertung der Stärke der Mechanismen sind in Teil 6, Anhang 6.C zu finden.

3.3.32 Kryptographische Mechanismen werden von ITSEFs nicht bewertet (siehe ITSEC Absatz 3.23).

Ausnutzbare Schwachstellen

3.3.33 Es kann viele Wege geben, eine bestimmte Gegenmaßnahme zu überwinden, wobei einige leichter als andere sein können. Für gewöhnlich gibt es mehr als eine Gegenmaßnahme, die ein Angreifer überwinden muß, um den EVG erfolgreich angreifen zu können. Der Entwickler stellt sich die möglichen Arten eines Angriffs auf einen EVG vor und wählt entsprechende Gegenmaßnahmen aus. Ausgehend von der Analyse des Entwicklers nehmen die Evaluatoren eine unabhängige Prüfung des EVG aus der Sicht eines Angreifers vor, um herauszufinden, wie ein Sicherheitsziel gefährdet werden kann.

3.3.34 Durch ein erfolgreiches Eindringen wird eine ausnutzbare Schwachstelle oder eine Nichterfüllung der erforderlichen Stärke der Mechanismen aufgedeckt. Ist ein Angriff erfolgreich, ist die Schwachstelle auswertbar. Im Interesse einer kostenwirksamen Evaluation braucht die Auswertbarkeit von Schwachstellen nicht durch Tests nachgewiesen zu werden, wenn die theoretischen Argumente ausreichen. Die Entwicklung von Angriffsszenarien und die Durchführung von Penetrationstests erfolgt im Rahmen der Schwachstellenbewertung bei der Evaluation.

Penetrationstests

3.3.35 Sobald die Evaluatoren die Liste potentieller Schwachstellen zusammengestellt und mit der vom Entwickler vorgelegten Liste verglichen haben (ITSEC Absatz 3.12), schließen sie die unabhängige Analyse durch Penetrationstests ab, mit denen sie überprüfen, ob die potentiellen Schwachstellen auswertbar sind.

3.3.36 Penetrationstests unterscheiden sich von Funktionstests, mit denen der Nachweis erbracht werden soll, daß der EVG der eigenen Spezifikation entspricht.

Kapitel 3.4 Prinzipien der Durchführung von Evaluationen

Theorie und Experiment

3.4.1 Theorien über den EVG und sein Verhalten können den Evaluatoren helfen, sich klar zu machen, wie der EVG die eigenen Sicherheitsvorgaben erfüllt. Evaluatoren sollen ihre eigenen Theorien über die EVG während der Analyse der Evaluationsbeiträge entwickeln und aufzeichnen. Diese Theorien sollen entweder übernommen und bestätigt oder durch Prüfen anderer Informationen über den EVG oder auf experimentellem Weg durch Penetrations- und sonstige Tests verworfen werden.

3.4.2 In der Wissenschaft stützt sich ein Experiment auf eine Hypothese, die dann geprüft wird. Solche Experimente können einer der nachfolgenden Kategorien zugeordnet werden:

a) Tests, mit denen nachgewiesen werden soll, ob das geprüfte System bestimmte Merkmale aufweist oder nicht;

b) Versuche, zwischen konkurrierenden Theorien über das Systemverhalten zu unterscheiden, indem Experimente konzipiert und durchgeführt werden, anhand derer die unterschiedlichen Theorien bestätigt oder widerlegt werden können.

3.4.3 Dieses Prinzip in bezug auf Experimente und Theorien kann auch in der Evaluationspraxis verwendet werden. Tests an EVG sollen nicht stichprobenweise durchgeführt werden, sondern ausgehend von dem Grundsatz, daß eine Theorie oder ein Verdacht überprüft werden muß. Für einen Evaluator bieten sich verschiedene Vorgehensweisen an. Anhand der Analyse der Sicherheitsvorgaben sollen Evaluatoren sich einen Einblick in die geforderten Sicherheitseigenschaften des EVG verschaffen und diese Informationen zur Entwicklung von Tests benutzen. Anhand der Analyse der anderen Evaluationsbeiträge sollen die Evaluatoren das Verhalten des EVG verstehen lernen und diese Informationen zur Entwicklung von Tests benutzen, mit denen die Auswertbarkeit potentieller Schwachstellen bestätigt oder widerlegt werden kann. Ein weiteres wichtiges Hilfsmittel für die Entwicklung von Tests ist die Kenntnis des Verhaltens ähnlicher Produkte und Systeme.

Systematische Verfeinerung

3.4.4 Die Komplexität eines EVG ist praktisch unbegrenzt. Die systematische Verfeinerung ist ein bekanntes Konzept zur Bewältigung dieses Problems während der Evaluation. Dieses Konzept findet seinen Niederschlag in verschiedenen ITSEC-Anforderungen an den Entwickler, in denen es um Evaluationsbeiträge und den Entwicklungsprozeß geht. Beispiele hierfür sind

a) die Aufteilung der Angabe der geforderten Sicherheitsfunktionalität in sicherheitsspezifische Funktionen in den Sicherheitsvorgaben;

b) die architekturmäßige Abtrennung der Sicherheitsfunktionalität von einer anderen Funktionalität;

c) die Verwendung eines abgestuften Konstruktionsprozesses;

d) die Verwendung strukturierter Entwicklungskonzepte;

e) die Verwendung von Programmiersprachen, die eine Modularisierung unterstützen.

3.4.5 Die Kriterien in den ITSEC folgen dem Prinzip der systematischen Verfeinerung während der Evaluation auch durch Trennung der Korrektheitsaspekte von den Wirksamkeitsaspekten und durch Unterscheidung zwischen unterschiedlichen Wirksamkeitsaspekten wie Eignung, Zusammenwirken usw.

Modellierung

3.4.6 Die Modellierung wird als Evaluationstechnik zur Untermauerung der Theorie und zum Nachweis des Verständnisses eingesetzt. Besonders relevant ist sie für höhere Evaluationsstufen. Bei der Entwicklung von Modellen stützt man sich häufig auf Erfahrung und Intuition. Sie werden unter Verwendung einer informellen, semiformalen und formalen Darstellungsform beschrieben. Vom Antragsteller/Entwickler vorgelegte Modelle sollen vom Evaluator als Verständnis- und Modellierungsgrundlage verwendet werden.

Abbildbarkeit

3.4.7 Auf höheren Evaluationsstufen soll die Erfüllung der Sicherheitsziele bis hinunter zum betriebsbereiten EVG für die Evaluatoren vollständig nachvollziehbar sein. Diese Abbildbarkeit kann nur dann vollständig sein, wenn sie alle Entwicklungsphasen abdeckt. Dies schließt die Anforderungs-, die Architekturentwurfs-, die Feinentwurfs- und die Implementierungsphase ein. Die Abbildbarkeit muß von den Sicherheitsvorgaben und den anderen Evaluationsbeiträgen, die verschiedene Darstellungen des EVG liefern, bewirkt werden. Dazu gehören auch Quellcode und ausführbarer Code, sofern dies für die betreffende Evaluationsstufe und den betreffenden EVG in Frage kommt.

Entscheidung des Evaluators

3.4.8 Aus der Sicht der Kriterien in den ITSEC besteht ein EVG eine Evaluation nur dann erfolgreich, wenn der Evaluator eine akzeptierende Entscheidung für alle Korrektheits- und Wirksamkeitskriterien der angestrebten Evaluationsstufe fällt. Dies bedeutet, daß in der Abschlußphase in dem EVG keine ausnutzbaren Schwachstellen übrigbleiben und die postulierte Mindeststärke der Mechanismen erfüllt worden ist. Er besteht die Evaluation nicht, wenn zum Schluß mindestens eines der Korrektheits-kriterien nicht erfüllt ist oder wenn in dem EVG eine ausnutzbare Schwachstelle übrigbleibt.

3.4.9 Ausgangsbasis für die von den Evaluatoren gefällte Entscheidung über ein Kriterium in den ITSEC ist der Nachweis, den der Antragsteller in den Evaluationsbeiträgen erbringt. Ergänzt wird dieser durch weitere Aufgaben des Evaluators gemäß den ITSEC, normalerweise durch eine Überkreuzprüfung oder irgendeine Art von Penetrationstest, um einen unabhängigen Nachweis der Erfüllung des Kriteriums erbringen und die Gültigkeit der Nachweise des Antragstellers/Entwicklers überprüfen zu können. Dieser Grundsatz der Unabhängigkeit gilt für alle Ergebnisse von Antragsteller-/Entwickler-analysen und -tests, beispielsweise die Bestätigung von Testergebnissen durch Stichprobenwieder-holung. Eine ablehnende Entscheidung wird erteilt, wenn vom Antragsteller/Entwickler kein Nach-weis, ein unvollständiger Nachweis (Grundsatz der Vollständigkeit) oder kein korrekter Nachweis für ein relevantes Kriterium erbracht wird.

Fehlerbehebung

3.4.10 Wenn während der Evaluation ein Fehler entdeckt wird, muß er behoben werden, da sonst die Evaluation am Ende eine ablehnende Entscheidung für eines der Korrektheitskriterien erbringt. Dasselbe gilt für ausnutzbare Schwachstellen.

3.4.11 Werden an früher evaluierten Evaluationsbeiträgen Korrekturen vorgenommen, verliert ein Teil der früheren Evaluationsarbeit seine Gültigkeit, so daß eine Wiederholung der Evaluationsarbeit notwendig wird.

Penetrationstests

3.4.12 Penetrationstests schaffen unabhängiges Vertrauen, daß ein bestimmter EVG keine ausnutzbaren Schwachstellen oder kritischen Mechanismen mit einer geringeren Stärke als angegeben enthält.

3.4.13 Penetrationstests bilden den Schlußpunkt des folgenden Prozesses:

a) Gewinnung eines Einblicks in den EVG und in die Sicherheitsvorgaben während der Durchführung der die Korrektheit betreffenden Evaluatoraufgaben;

b) Suche nach Schwachstellen und Entwicklung von Hypothesen über deren Ausnutzbarkeit während der Durchführung der die Wirksamkeit betreffenden Evaluatoraufgaben.

3.4.14 Penetrationstests werden bei sämtlichen Evaluationen durchgeführt und schließen für gewöhnlich die Tätigkeit des Evaluators ab. Evaluatoren legen Penetrationstests fest, spezifizieren sie, führen sie durch und zeichnen sie auf.

Checklisten

3.4.15 Bei Evaluationen verwendete Checklisten gewährleisten, daß kein relevanter Standardaspekt, wie z.B. wohlbekannte Schwachstellen bei einem bestimmten Produkt- oder Systemtyp, vergessen wird, bevor eine Entscheidung gefällt wird.

Review

3.4.16 Evaluationen setzen Denkfähigkeit und Urteilskraft voraus. Zur Verhinderung von Vorurteilen und Eingrenzung der Folgen von Fehlern sowie zur Sicherung der Gesamtqualität sollen die Evaluationsergebnisse innerhalb der ITSEF einem Reviewprozeß unterzogen werden. Die Anforderungen im Hinblick auf den Reviewprozeß und die Beteiligung der **Zertifizierungsstelle** können im nationalen Regelwerk präzisiert werden. An dem Review soll mindestens eine Person teilnehmen, die nicht an dem zu überprüfenden Ergebnis beteiligt gewesen ist.

3.4.17 Durch den Reviewprozeß bei einer Evaluation soll sichergestellt werden, daß die Ergebnisse der Evaluation mit den einschlägigen Kriterien, den Anforderungen des ITSEM und dem nationalen Regelwerk übereinstimmen.

Aufzeichnungen

3.4.18 Zum Nachweis der Evaluationsarbeit und der Evaluationsergebnisse sind umfassende Aufzeichnungen erforderlich. Wichtige Entscheidungen, Begründungen, Tests und deren Ergebnisse sollen dokumentiert werden, z.B. in Betriebstagebüchern oder Berichten. Die Dokumentierung zeitweise aufgetretener Probleme und ihre Lösung oder von den Evaluatoren unabhängig durchgeführte Aufgaben könnte sich als nützlich erweisen und als Bestätigung dienen. Die Vorschriften des nationalen Regelwerks für die Evaluation und die Zertifizierung können diesen Fall abdecken.

Ressourcen

3.4.19 Welche und wie viele Ressourcen für eine Evaluation benötigt werden, hängt in erster Linie von der Komplexität des EVG, seinen Sicherheitsvorgaben und der Evaluationsstufe ab. Zu den anderen Faktoren, die den erforderliche Aufwand an Ressourcen bestimmen, gehören die Kompetenz und die Erfahrung der Evaluatoren und der Einsatz unterstützender Werkzeuge. Die erforderlichen Aufgaben des Evaluators ergeben sich aus dem betreffenden Kriterienkatalog, der Struktur des EVG und den Evaluationsbeiträgen. Die Wirksamkeit ist Sache der ITSEF. Den Mindestbedarf an Ressourcen bestimmt das nationale Regelwerk, wobei von praktischen Erfahrungswerten ausgegangen werden soll.

Ressourcen für Penetrationstests

3.4.20 Die Suche nach ausnutzbaren Schwachstellen ist durch die je nach Evaluationsstufe verfügbare Informationsmenge sowie die Fachkenntnisse, Gelegenheiten und Ressourcen entsprechend der postulierten Mindeststärke der Mechanismen begrenzt.

Evaluationsarbeitsplan (EWP)

3.4.21 Ein Evaluationsarbeitsplan (EWP) enthält eine ausführliche Beschreibung der Aktivitäten des Evaluators, Voranschläge der benötigten Ressourcen und einen Zeitplan. Hinweise zur Erstellung eines Evaluationsarbeitsplans (EWP) sind in Teil 4 des ITSEM zu finden.

Wiederholbarkeit, Reproduzierbarkeit, Unvoreingenommenheit und Objektivität

3.4.22 Wiederholbarkeit, Reproduzierbarkeit, Unvoreingenommenheit und Objektivität sind förderliche Prinzipien für die Durchführung von Evaluationen. Sie sind eng miteinander verknüpft, insbesondere die Unvoreingenommenheit mit der Objektivität und die Reproduzierbarkeit mit der Wiederholbarkeit. Unvoreingenommenheit und Objektivität sind Voraussetzungen für Reproduzierbarkeit und Wiederholbarkeit. Dies wird in Abbildung 3.4.1 veranschaulicht.

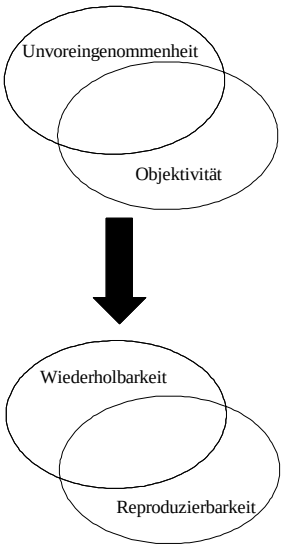


Abbildung 3.4.1 Die vier Grundprinzipien der Evaluation

3.4.23 Zur Unterstützung der vier Grundprinzipien können dokumentierte standardisierte Evaluationsprozeduren, -techniken und -werkzeuge eingesetzt werden (siehe Teil 4 des ITSEM). Wirksamkeitsaspekte wie etwa die Identifikation von Schwachstellen, die Stärke der Mechanismen und die Auswertbarkeit von Schwachstellen sind von besonderem Belang, da durch sie subjektive Faktoren wie Erfahrung und Intuition eingebracht werden. Der Subjektivität kann innerhalb des Evaluationsprozesses nicht vollständig entgegengewirkt werden. Es empfiehlt sich die Beteiligung eines Dritten wie etwa einer Zertifizierungsstelle zur unabhängigen Überwachung von Evaluationen, damit die Konsistenz und Vergleichbarkeit der Ergebnisse verschiedener ITSEFs gewährleistet ist (siehe Teil 2 des ITSEM).

Teil 4 Evaluationsprozeß

Inhalt

Abbildungen

Kapitel 4.1 Einleitung

Evaluationsmethoden

4.1.1 Der vorliegende Teil des ITSEM richtet sich speziell an Evaluatoren. Es werden die bei der Evaluation verwendeten Methoden beschrieben, sowohl hinsichtlich des organisatorischen Rahmens als auch hinsichtlich der Techniken, die zur Evaluation eines EVG anhand der ITSEC verwendet werden. Der Beitrag zur Evaluation, der Evaluationsprozeß und das Evaluationsergebnis werden ebenfalls beschrieben. Eine ausführliche Beschreibung, wie jede einzelne Evaluatoraufgabe durchzuführen ist, erfolgt nicht.

4.1.2 In einigen Abschnitten dieses Teils des ITSEM werden Aspekte der Evaluationsmethoden definiert, die verbindlich sind - diese Abschnitte sind im Text durch Fettdruck und Schattierung hervorgehoben. Zweck dieser Textteile mit Vorschriftencharakter ist es sicherzustellen, daß Evaluationen, die anhand der ITSEC und des ITSEM durchgeführt werden, auf einer gemeinsamen technischen Grundlage erfolgen.

Hinweis: In der vorliegenden deutschen Übersetzung des ITSEM ist auf die in der englischen Version benutzte Schattierung von Textpassagen verzichtet worden.

Struktur

4.1.3 Dieser Teil ist in verschiedene Kapitel unterteilt, wobei die vorliegenden einleitenden Bemerkungen Kapitel 4.1 darstellen.

4.1.4 Kapitel 4.2 gibt einen Überblick über den Evaluationsprozeß; es zeigt die Rolle der an der Evaluation Beteiligten auf und beschreibt die einzelnen Phasen, die das Verfahren durchläuft.

4.1.5 Kapitel 4.3 beschreibt die Maßnahmen zum Starten einer Evaluation und zur Beschaffung der **Evaluationsbeiträge.**

4.1.6 Kapitel 4.4 enthält eine detaillierte Beschreibung des Evaluationsprozesses aus der Sicht der Evaluatoren. Die Angaben sind so detailliert, wie dies zur Gewährleistung der technischen Gleichwertigkeit von Evaluationen erforderlich ist.

4.1.7 Kapitel 4.5 behandelt Techniken und Werkzeuge, die für Evaluatoren von Nutzen sind.

4.1.8 Kapitel 4.6 enthält für Evaluatoren bestimmte Hinweise über die Wiederverwendung von Evaluationsergebnissen.

4.1.9 Kapitel 4.7 befaßt sich mit den Ergebnissen, die eine Evaluation zu erbringen hat, d.h. den **technischen Evaluationsberichten** (ETRs).

Kapitel 4.2 Der Evaluationsprozeß

Einleitung

4.2.1 Das vorliegende Kapitel gibt einen Überblick über den Evaluationsprozeß, definiert die Rollen der am Verfahren Beteiligten sowie die Phasen und Stufen, die das Verfahren durchläuft.

4.2.2 Der in diesem Kapitel beschriebene Evaluationsprozeß ist als Rahmen anzusehen, der die während der Durchführung einer Evaluation zu befolgenden organisatorischen und verfahrenstechnischen Aspekte beschreibt.

Rollen

Überblick

4.2.3 Die Durchführung des in diesem Kapitel beschriebenen Evaluationsprozesses setzt voraus, daß folgende Stellen vorhanden sind:

a) ITSEF;

b) Antragsteller;

c) Entwickler;

d) **Zertifizierungsstelle**.

4.2.4 Die Rolle jeder dieser Stellen innerhalb des Evaluationsprozesses wird in den nachfolgenden Unterabschnitten behandelt. In Abbildung 4.2.1 sind diese Stellen und die verschiedenen Arten von Informationen dargestellt, die während des Evaluationsprozesses zwischen ihnen ausgetauscht werden können.

ITSEF

4.2.5 Die Aufgabe der ITSEF besteht darin, als unabhängige Stelle zu fungieren, bei der Evaluationen durch Dritte innerhalb des vom **nationalen Regelwerk** gesetzten Rahmens durchgeführt werden können. Die ITSEF leistet Hilfestellung bei den organisatorischen, administrativen und vertraglichen Aspekten von Evaluationen.

4.2.6 Aufgabe der Evaluatoren innerhalb der ITSEF ist die Durchführung einer detaillierten, unvoreingenommenen Prüfung eines EVG, um nach **Schwachstellen** zu suchen und um herauszufinden, in welchem Umfang die Sicherheitsvorgaben des EVG durch seine Implementierung gemäß den ITSEC erfüllt werden. Die Ergebnisse der Evaluation werden der Zertifizierungsstelle und dem Antragsteller vorgelegt.

4.2.7 **Die Evaluatoren führen die Evaluationsarbeiten gemäß den Anforderungen von ITSEC/ITSEM und den im nationalen Regelwerk festgelegten Vorgehensweisen und Vervahren durch. Bei der Durchführung dieser Arbeiten sind die Evaluatoren für folgendes verantwortlich:**

a) das Führen von Aufzeichnungen über sämtliche während der Evaluation durchgeführten Arbeiten;

b) die Erstellung von Evaluationsberichten;

c) die Wahrung der jeweils erforderlichen Vertraulichkeit in allen den Evaluationsprozeß betreffenden Fragen.

4.2.8 Evaluatoren unterstützen die Zertifizierungsstelle während des Zertifizierungsprozesses (siehe Unterabschnitt *Phase III - Abschluß* in diesem Kapitel).

4.2.9 Evaluatoren halten Verbindung zu anderen an der Evaluation Beteiligten, wozu der Antragsteller der Evaluation, der Entwickler des EVG und die Zertifizierungsstelle gehören.

4.2.10 Die Evaluatoren sollen sicherstellen, daß Antragsteller und Entwickler sich der ihnen nach dem nationalen Regelwerk auferlegten Verpflichtungen bewußt sind und diese vollständig verstehen. Insbesondere sollen die Evaluatoren sicherstellen, daß der Antragsteller in der Lage ist, alle notwendigen Beiträge zum Evaluationsprozeß (Evaluationsbeiträge) zu liefern. Die Evaluatoren sollen daher bei Beginn einer Evaluation klarstellen, was der Antragsteller bereitzustellen hat.

Antragsteller

4.2.11 Beim Antragsteller einer Evaluation handelt es sich in der Regel um den Vertreiber eines Produkts oder um den Anwender oder Anbieter eines Systems, der nachweisen will, daß der EVG die spezifizierten Sicherheitsvorgaben erfüllt.

4.2.12 Das Starten der Evaluation eines EVG durch eine ITSEF wird vom Antragsteller veranlaßt. Er definiert die Sicherheitsvorgaben, gibt die Evaluation in Auftrag und bekommt den ETR sowie im Falle einer akzeptierenden Entscheidung der Evaluation das **Zertifikat**/den **Zertifizierungsreport** ausgehändigt.

4.2.13 Die Rolle des Antragstellers wird in Teil 6 des ITSEM ausführlicher beschrieben.

Entwickler

4.2.14 Der Begriff Entwickler bezieht sich auf die Organisation (bzw. die Organisationen), die den EVG (oder Teilkomponenten des EVG) herstellt (bzw. herstellen). Der Entwickler soll (sofern er nicht der Antragsteller der Evaluation ist) bereit sein, mit dem Antragsteller zusammenzuarbeiten und bei der Evaluation Hilfestellung zu leisten, z.B. durch technische Unterstützung der ITSEF.

4.2.15 Die Rolle des Entwicklers wird in Teil 6 des ITSEM ausführlicher beschrieben.

Zertifizierungsstelle

4.2.16 Die Hauptziele einer Zertifizierungsstelle bestehen darin,

a) die Voraussetzungen dafür zu schaffen, daß die Arbeit aller einem bestimmten Regelwerk unterliegenden ITSEFs unverfälscht und konsistent ist und die von ihnen gezogenen Schlußfolgerungen gültig, nachvollziehbar und reproduzierbar sind;

b) eine unabhängige Bestätigung dafür zu geben, daß Evaluationen nach Maßgabe der genehmigten Kriterien, Methoden und Verfahren durchgeführt worden sind.

4.2.17 Die Rolle der Zertifizierungsstelle wird in Teil 2 des ITSEM ausführlicher beschrieben.

Phasen des Evaluationsprozesses

Überblick

4.2.18 Der Evaluationsprozeß kann in drei Phasen unterteilt werden: Vorbereitung, Durchführung und Abschluß. Die drei Phasen werden in den folgenden Unterabschnitten im einzelnen beschrieben.

Phase I - Vorbereitung

4.2.19 Der Antragsteller nimmt mit der laut nationalem Regelwerk zuständigen Stelle (Zertifizierungsstelle oder ITSEF) Kontakt auf und startet die Evaluation eines EVG. Es wird eine ITSEF ausgewählt, mit der der Antragsteller einen Vertrag für Phase I schließt. Der Antragsteller legt der ITSEF seine Sicherheitsvorgaben für den EVG (unter Umständen in Entwurfsform) vor und bestimmt die Zielrichtung der Evaluation.

4.2.20 Die ITSEF schätzt die Wahrscheinlichkeit einer erfolgreichen Evaluation ab und fordert beim Antragsteller relevante Informationen an. Wenn ihren Anforderungen Genüge getan ist, schließt sie mit dem Antragsteller einen Vertrag über die Durchführung der Evaluation. Ergänzend kann die ITSEF die Sicherheitsvorgaben überprüfen und dem Antragsteller zur Schaffung einer gesicherten Evaluationsbasis für unumgänglich erachtete Änderungen nahelegen.

4.2.21 Das nationale Regelwerk kann die ITSEF zur Erstellung eines **Evaluationsarbeitsplans** (EWP) oder einer Liste der Evaluationsbeiträge vor Beginn der Evaluation verpflichten. Der EWP dient zur Beschreibung der Arbeiten, die von der ITSEF während der Evaluation durchzuführen sind. Die Liste der Evaluationsbeiträge stellt eine Beschreibung dessen dar, was der Antragsteller der ITSEF während der Evaluation vorzulegen hat, einschließlich der Termine für die Vorlage der Evaluationsbeiträge. Die Zertifizierungsstelle überprüft den EWP, um sicherzustellen, daß die vorgeschlagenen Arbeiten angemessen sind. Der Vorteil solcher EWP und Listen von Evaluationsbeiträgen ist, daß Antragsteller und ITSEF sich von vornherein im klaren sind, welche Arbeiten erforderlich sind.

4.2.22 Zu Beginn der Evaluation stützt sich der EWP auf die der ITSEF zu diesem Zeitpunkt vorliegenden Informationen. Mit fortschreitender Evaluation ist davon auszugehen, daß den Evaluatoren weitergehende Informationen zur Verfügung stehen und der EWP fortentwickelt wird. Die Zertifizierungsstelle prüft die Änderungen des EWP, um sicherzustellen, daß die vorgeschlagenen Arbeiten angemessen sind.

4.2.23 Eine ITSEF kann Antragsteller und Entwickler bei der Erstellung der erforderlichen Evaluationsbeiträge beraten. Die Beratung kann durch eine andere als die mit der Durchführung der Evaluation betraute ITSEF erfolgen. **Falls eine Beratung durch eine ITSEF erfolgt, darf sie deren Unabhängigkeit bei irgendeiner Evaluation nicht beeinträchtigen.** Einzelheiten werden durch das nationale Regelwerk geregelt.

4.2.24 Während der Vorbereitungsphase sollen Antragsteller und ITSEF sich über die Notwendigkeit von Reevaluationsinformationen im ETR verständigen.

Phase II - Durchführung

4.2.25 Bis zum Beginn der Durchführungsphase soll zwischen Antragsteller und ITSEF ein Vertrag geschlossen sein, die erforderlichen Arbeiten sollen abgesprochen und die Sicherheitsvorgaben endgültig festgelegt sein.

4.2.26 Die Evaluatoren führen für jede jeweils relevante Phase bzw. jeden relevanten Aspekt der ITSEC die geforderten Evaluatoraufgaben aus. Die Evaluationsbeiträge werden dahingehend geprüft, ob alle Kriterien berücksichtigt sind. Darüber hinaus erstellen die Evaluatoren eine Liste der **potentiellen Schwachstellen**. Alle festgestellten Mängel werden mit den Zuständigen besprochen.

4.2.27 In der Durchführungsphase festgestellte Mängel sind zwei unterschiedlichen Gruppen zuzuordnen. Die erste Gruppe umfaßt Mängel, für die der Antragsteller eine für die ITSEF und die Zertifizierungsstelle annehmbare Lösung anbieten kann. Zwischen ITSEF und Antragsteller wird eine Frist vereinbart, innerhalb derer der Mangel der vereinbarten Lösung entsprechend behoben wird. Die zweite Gruppe umfaßt Mängel, die der Antragsteller nicht beheben kann oder will. ITSEF und Zertifizierungsstelle setzen den Antragsteller über die Konsequenzen in Kenntnis, die sich ergeben, wenn der Mangel nicht behoben wird. Der Antragsteller kann die Evaluation daraufhin entweder abbrechen oder die Konsequenzen für die Zertifizierung hinnehmen.

4.2.28 **Während einer Evaluation muß von der ITSEF ein ETR erstellt werden.** Der ETR ist zwar das Endprodukt der Evaluation, er stellt jedoch nicht das Endprodukt des Evaluations- und Zertifizierungsprozesses dar. Der endgültige Entwurf des ETR wird dem Antragsteller und der Zertifizierungsstelle zur Genehmigung vorgelegt.

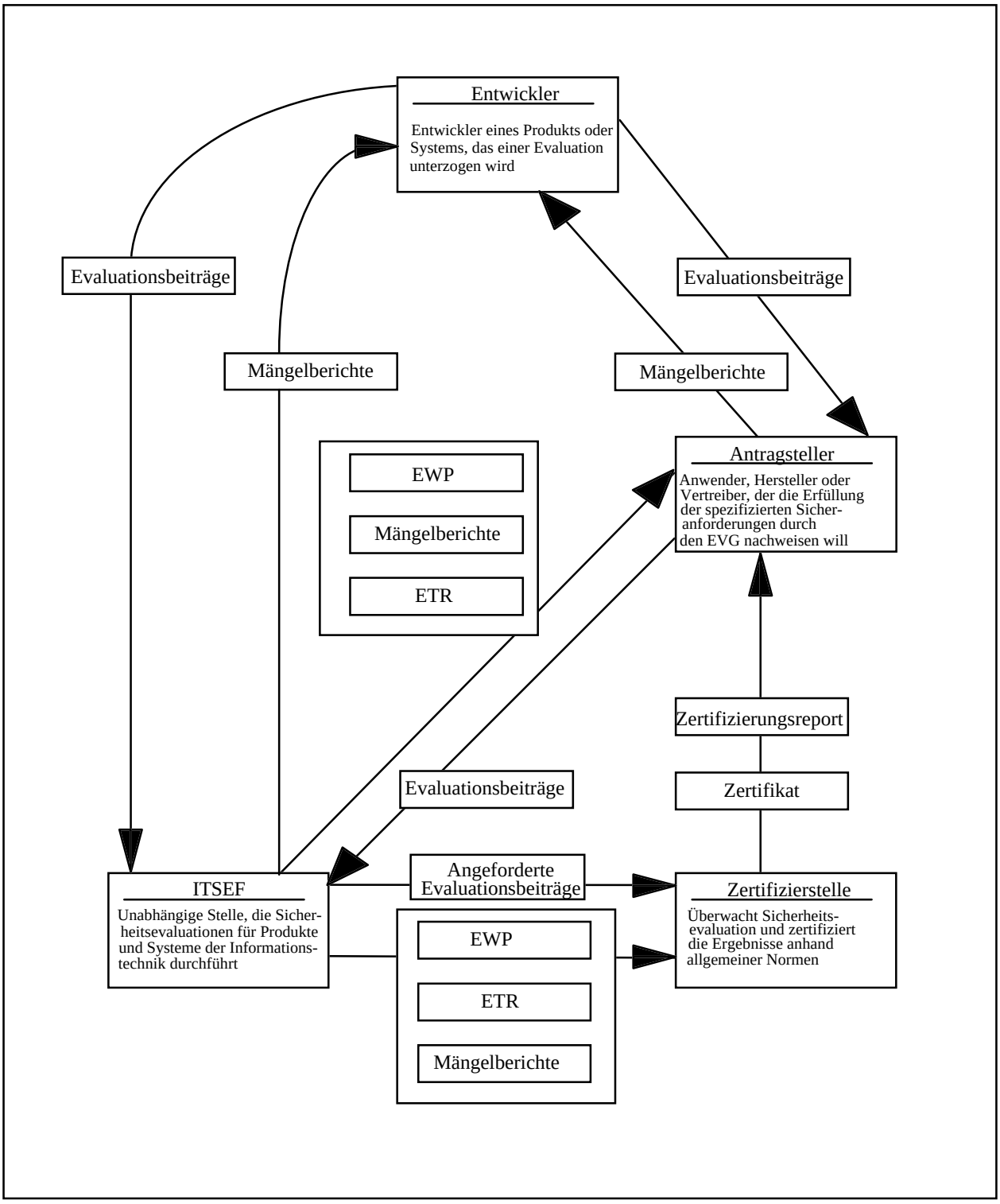
Phase III - Abschluß

4.2.29 In der Abschlußphase legt die ITSEF der Zertifizierungsstelle und dem Antragsteller die angenommene Fassung des ETR als Beleg für die Evaluationsergebnisse vor. Der ETR soll auch für künftige Evaluatoren im Falle einer Reevaluation des EVG verwendbar sein. Der gesamte ETR und jeder seiner Teile ist - ob in der Entwurfsform oder in der endgültigen Fassung - vertraulich zu behandeln.

4.2.30 Die Zertifizierungsstelle kann die ITSEF um technische Unterstützung ersuchen und in angemessener Form die Einsichtnahme in bestimmte technische Unterlagen und Ergebnisse zur Untermauerung der im ETR gezogenen Schlußfolgerungen verlangen. Dies bringt in der Regel keine zusätzlichen Evaluationsarbeiten für die ITSEF mit sich.

4.2.31 Während des Zertifizierungsprozesses überprüft die Zertifizierungsstelle den ETR, um herauszufinden, ob der EVG die Sicherheitsvorgaben erfüllt; dabei werden auch nicht in den Anwendungsbereich der Evaluation fallende Faktoren berücksichtigt. Im Verlauf dieses Prozesses kann sie die Zuordnung zu einer Evaluationsstufe veranlassen. Die von ihr gezogenen Schlußfolgerungen werden im Zertifikat/Zertifizierungsreport festgehalten.

4.2.32 I**n dieser Phase hat die abschließende Verfügung über die Evaluationsbeiträge zu erfolgen.**



Anmerkung: Ein Antragsteller kann auch Entwickler sein.

Abbildung 4.2.1 Beispiel für den Informationsfluß im Verlauf des Evaluationsprozesses

Kapitel 4.3 Beitrag zur Evaluation

Einleitung

4.3.1 Im vorliegenden Kapitel werden die Faktoren beschrieben, die von den Evaluatoren vor einer Evaluation und während des Startens einer Evaluation zu berücksichtigen sind. Dabei geht es auch um die Art der Hilfestellung, die Evaluatoren dem Antragsteller bei der Bereitstellung seines Beitrags leisten sollen, und was mit den Evaluationsbeiträgen geschieht, sobald sie sich in Händen der Evaluatoren befinden.

4.3.2 Es ist nicht Sinn dieses Kapitels, verbindlich vorzuschreiben, wie ein nationales Regelwerk aufgebaut sein soll; vielmehr sollen den Evaluatoren Informationen an die Hand gegeben werden, wie eine Evaluation im Normalfall gestartet wird und was mit den Evaluationsbeiträgen geschieht.

4.3.3 Es ist zu bedenken, daß es zwar keine verbindlichen Vorschriften gibt, eine Evaluation unter der Leitung der Zertifizierungsstelle zu starten, daß aber eine möglichst frühzeitige Beteiligung dieser Stelle empfehlenswert ist, damit die technischen und wirtschaftlichen Risiken der Evaluation so gering wie möglich gehalten werden können.

4.3.4 Die Bezeichnung *Evaluationsbeitrag* wird für alles (einschließlich des EVG selbst) verwendet, was den Evaluatoren zu Evaluationszwecken zur Verfügung zu stellen ist. Dazu gehören immaterielle Beiträge wie die Unterstützung der Evaluatoren und der Zugang zu Rechnern. Einzelheiten zu den Anforderungen von ITSEC/ITSEM an Evaluationsbeiträge sind Teil 6, Anhang 6.A zu entnehmen.

4.3.5 Zweck der Evaluationsbeiträge ist es, die Evaluatoren in die Lage zu versetzen, die Evaluation des EVG durchzuführen. Die verschiedenen Arten von Evaluationsbeiträgen erfüllen diesen Zweck auf unterschiedliche Weise und zwar wie folgt:

a) Evaluationsbeiträge können den Nachweis der Wirksamkeit oder Korrektheit erbringen, z.B. eine informelle Beschreibung der Entsprechung von Quellcode und Feinentwurf.

b) Evaluationsbeiträge können die Evaluatoren in die Lage versetzen, einen zusätzlichen Nachweis der Wirksamkeit oder Korrektheit zu führen, z.B. den Zugang zum entwickelten EVG.

c) Evaluationsbeiträge können die Effizienz der von den Evaluatoren durchgeführten Arbeiten insgesamt erhöhen, z.B. die technische Unterstützung durch den Entwickler.

Verantwortung für Evaluationsbeiträge

4.3.6 Die Verantwortung für die Bereitstellung aller geforderten Evaluationsbeiträge liegt beim Antragsteller. Die meisten Evaluationsbeiträge werden jedoch vom Entwickler erstellt und geliefert (sofern der Antragsteller nicht der Entwickler ist). Für die Evaluatoren ist das Vertragsverhältnis zwischen Antragsteller und Entwickler ohne Belang. Kunde der Evaluatoren ist der Antragsteller.

4.3.7 Die Betriebskosten und -risiken (z.B. Verluste oder Schäden durch Feuer, Wasser, Diebstahl usw.) für sämtliche Evaluationsbeiträge sind vom Antragsteller zu tragen, es sei denn, mit den Evaluatoren ist ausdrücklich etwas anderes vereinbart worden. Dabei ist zu beachten, daß bei manchen Evaluationsbeiträgen wie etwa neuen oder Sonderzwecken dienenden Gerätetypen der Wiederbeschaf-fungswert nicht so ohne weiteres ermittelt werden kann und diese somit ein Versicherungsrisiko darstellen können, das nicht an die Evaluatoren weitergegeben werden kann.

4.3.8 Den Evaluatoren wird empfohlen, eine Liste der Evaluationsbeiträge zu erstellen. Es handelt sich dabei um eine endgültige Liste der zu erwartenden Evaluationsbeiträge (z.B. als Verweis auf die Dokumentation des Antragstellers) mit Angabe der Termine, zu denen die Evaluationsbeiträge den Evaluatoren vorzuliegen haben. Auf die Liste der Evaluationsbeiträge kann im ETR verwiesen werden.

4.3.9 Es empfiehlt sich, dafür zu sorgen, daß die Ziele der Durchführung der Evaluation für die Evaluatoren klar verständlich sind und den anderen Beteiligten mitgeteilt werden. Den Evaluatoren wird daher empfohlen sicherzustellen, daß alle Beteiligten an der Evaluation sich über den Zweck und Umfang der Evaluation einig und ihrer jeweiligen Verantwortung bewußt sind.

4.3.10 Zu den Punkten, die mit einem Antragsteller abzusprechen sind, gehören u.a. folgende: Fragen der nationalen Geheimhaltung und kommerziellen Vertraulichkeit von Informationen; die Zugänglichkeit oder die Notwendigkeit spezieller Werkzeuge; eventuelle Einschränkungen beim Zugriff der Evaluatoren auf die Evaluationsbeiträge; frühere Evaluationsergebnisse; und die gewünschte Häufigkeit von Besprechungen über den Fortgang der Arbeiten.

4.3.11 Im Rahmen einer Einzelvereinbarung zwischen Antragsteller und ITSEF müssen gegebenenfalls folgende Details geklärt werden:

a) der Datenträger und das Format maschinenlesbarer Evaluationsbeiträge;

b) der Zeitplan für die Erstellung der Evaluationsbeiträge;

c) die Anzahl der vorzulegenden Ausfertigungen der Evaluationsbeiträge;

d) die Sachlage bei Evaluationsbeiträgen in Entwurfsform;

e) die Sachlage bei in Verbindung mit dem EVG zu verwendenden Produkten;

f) Vereinbarungen über die Besprechung der Entwicklungsumgebung mit dem Entwickler;

g) Zutritt zum Betriebs- und zum Entwicklungsort;

h) Art und Dauer der Entwicklerunterstützung, einschließlich Rechnerzugriff und von den Evaluatoren benötigte Räumlichkeiten.

4.3.12 In vielen Fällen müssen die Evaluatoren die Möglichkeit des Zugriffs auf Informationen haben, die von Unterauftragnehmern oder Dritten bereitgestellt werden. Der Antragsteller hat solche Fälle zu berücksichtigen.

4.3.13 Die Frage, ob die Evaluation begleitend oder nachfolgend erfolgt, hat Auswirkungen auf die Verfügbarkeit von Evaluationsbeiträgen und muß bei der Erstellung eines spezifischen EWP berücksichtigt werden (siehe Kapitel 4.4).

4.3.14 Die Frage, ob es bei der Evaluation um ein System oder ein Produkt geht, hat ebenfalls Auswirkungen auf die Bereitstellung von Evaluationsbeiträgen und somit auch auf die Erstellung eines spezifischen EWP. Beispielsweise kann ein Produkt zur Aufstellung und Prüfung bei der ITSEF bereitstehen, während ein System der ITSEF wahrscheinlich nicht in derselben Weise zur Verfügung gestellt werden kann.

Behandlung von Evaluationsbeiträgen

Vertraulichkeit

4.3.15 Während ihrer Arbeit haben die ITSEFs Zugang zu sensitiven Geschäftsinformationen ihrer Kunden und unter Umständen auch zu Informationen, die der nationalen Geheimhaltung unterliegen. Evaluationspartner müssen darauf vertrauen können, daß mit den an die ITSEFs weitergegebenen Informationen kein Mißbrauch getrieben wird.

4.3.16 Die allgemeinen Anforderungen im Hinblick auf die Vertraulichkeit sind durch das nationale Regelwerk zu regeln. Antragsteller und ITSEFs können zusätzliche Anforderungen vereinbaren, sofern diese im Einklang mit dem nationalen Regelwerk stehen.

4.3.17 Die an die Vertraulichkeit gestellten Anforderungen betreffen viele Aspekte der Evaluationsarbeit, einschließlich der Entgegennahme, Behandlung und Aufbewahrung der Evaluationsbeiträge und der abschließenden Verfügung über sie.

Evaluationsbeiträge in Entwurfsform

4.3.18 Evaluatoren benötigen stabile und offiziell freigegebene Versionen der Evaluationsbeiträge. Unter Umständen kann es für die Evaluatoren jedoch von Nutzen sein, auch Einblick in Entwurfsversionen bestimmter Evaluationsbeiträge zu bekommen wie etwa

a) Testunterlagen, die ihnen eine frühzeitige Bewertung von Tests und Testprozeduren ermöglichen;

b) Quellcode oder Hardware-Konstruktionszeichnungen, die ihnen die Möglichkeit geben, die Anwendung der Standards des Entwicklers zu bewerten.

4.3.19 Evaluationsbeiträge in Entwurfsform sind am ehesten dort zu finden, wo die Evaluation eines EVG parallel zu seiner Entwicklung erfolgt. Sie können jedoch auch bei der nachfolgenden Evaluation eines Produkts oder Systems vorkommen, wenn der Entwickler zusätzliche Arbeiten durchführen mußte, um einen von den Evaluatoren festgestellten Mangel zu beheben (z.B. einen **Fehler** in der Konstruktion) oder um einen Sicherheitsnachweis zu erbringen, der in der vorhandenen Dokumentation nicht erbracht wird (z.B. die Wirksamkeit betreffende Evaluationsbeiträge im Fall eines Produkts oder Systems, das ursprünglich nicht für die Erfüllung der ITSEC-Anforderungen entwickelt wurde).

Konfigurationskontrolle

4.3.20 **Die Evaluatoren müssen die Evaluationsbeiträge unter Kontrolle halten, damit die Zertifizierungsstelle die Relevanz der Evaluationsergebnisse für den (endgültig) betriebsbereiten EVG gewährleisten kann.** Die Evaluatoren sollen sich eines Qualitätssicherungssystems bedienen, das um Übereinstimmung mit [EN45] bemüht ist; so ist sichergestellt, daß die Evaluationsbeiträge den Wünschen des Antragstellers und dem nationalen Regelwerk entsprechend kontrolliert und behandelt werden können.

Abschließende Verfügung über die Evaluationsbeiträge

4.3.21 N**ach vollendeter Durchführung der Evaluation (am Ende der Abschlußphase) müssen die Evaluatoren eine abschließende Verfügung über sämtliche Evaluationsbeiträge treffen. Dies kann auf eine oder mehrere der folgenden Arten geschehen:**

a) Vernichtung der Evaluationsbeiträge;

b) Rückgabe der Evaluationsbeiträge;

c) Archivierung der Evaluationsbeiträge.

4.3.22 **Die Behandlung und Aufbewahrung archivierten Materials muß den Anforderungen des nationalen Regelwerks entsprechen.**

4.3.23 Die für die abschließende Verfügung über die Evaluationsbeiträge geltenden Regelungen sollen mit dem Antragsteller vor Beginn von Phase II (Durchführung) abgesprochen werden.

Reevaluation und Wiederverwendung von Evaluationsbeiträgen

Überblick

4.3.24 Dieser Abschnitt enthält für Evaluatoren bestimmte Hinweise über den geforderten Beitrag zu Evaluationen, die unter Heranziehung früherer Evaluationsergebnisse als Evaluationsbeitrag durchgeführt werden. In Kapitel 4.6 wird beschrieben, wie diese Evaluationen durchgeführt werden.

4.3.25 Eine **Reevaluation** des EVG kann im Falle einer Änderung des EVG oder der dazugehörigen Evaluationsbeiträge erfolgen. Beispiele für Änderungen sind u. a. die Erhöhung der angestrebten Evaluationsstufe oder die Hinzufügung sicherheitsspezifischer Funktionen zu den Sicherheitsvorgaben eines EVG. Der Antragsteller nimmt eine Auswirkungsanalyse vor und legt die entsprechende Maßnahmenfolge fest, damit die Ergebnisse einer früheren Evaluation den in Teil 6, Anhang 6.D enthaltenen Hinweisen entsprechend erneut bestätigt werden können.

4.3.26 Die **Wiederverwendung** von Evaluationsergebnissen stellt eine Möglichkeit der Verminderung des Evaluationsaufwands für die Evaluation eines EVG dar, der einen oder mehrere zuvor evaluierte EVG enthält. Die Ergebnisse der ursprünglichen Evaluation können im Zusammenhang mit der Evaluation des neuen EVG weiterhin gültig sein oder nicht.

4.3.27 Wenn die Evaluationsstufe(n) der zuvor evaluierten Komponente(n) auf einer höheren oder der gleichen Stufe wie die angestrebte Evaluationsstufe des EVG liegt/liegen, werden die früheren Korrektheitsergebnisse durch die Zertifikate/Zertifizierungsreports bestätigt.

4.3.28 Wenn ein zertifiziertes Produkt oder System als Komponente eines neuen EVG verwendet wird, ändern sich die Rahmenbedingungen seiner Verwendung. Somit bleibt zwar die Korrektheit der zertifizierten Komponente in bezug auf ihre ursprünglichen Sicherheitsvorgaben weiterhin gültig, jedoch muß ihre Wirksamkeit im bezug auf die neuen Sicherheitsvorgaben mit Blick auf die neuen Rahmenbedingungen erneut bestätigt werden.

4.3.29 Vom Antragsteller wird daher erwartet, daß er die Evaluationsbeiträge des neuen EVG für die angestrebte Evaluationsstufe zusammen mit den Zertifikaten/Zertifizierungsreports für etwaige zertifizierte Komponenten vorlegt.

4.3.30 Es kann jedoch sein, daß zur Unterstützung der Wirksamkeitsanalyse auch die korrektheitsspezifischen Evaluationsbeiträge für die Komponenten des EVG benötigt werden.

4.3.31 Aus den für den neuen EVG zum Nachweis der Wirksamkeit vorzulegenden Evaluationsbeiträgen muß die Wirksamkeit der bereits früher evaluierten Produkte in ihrer neuen Betriebsumgebung hervorgehen. Beispielsweise muß nachgewiesen werden, daß in den Sicherheitsvorgaben für den neuen EVG die zuvor evaluierten Produkte angemessen berücksichtigt worden sind. Desgleichen muß der Antragsteller auf das Zusammenwirken *aller* Komponenten des neuen EVG achten, selbst wenn für manche dieser Komponenten Zertifikate/Zertifizierungsreports aus der/den ursprünglichen Evaluation(en) vorliegen.

Verfügbarkeit von Evaluations- und Zertifizierungsergebnissen

4.3.32 Das Zertifikat/der Zertifizierungsreport oder der ETR (oder Teile davon) kann als Beitrag zur Reevaluation oder Wiederverwendung herangezogen werden. In der Praxis hängt der Umfang, in dem die Ergebnisse früherer Evaluationen verfügbar sind, davon ab, ob diese Evaluationen

a) von derselben ITSEF,

b) von einer anderen ITSEF nach den Vorschriften desselben nationalen Regelwerks oder

c) von einer ITSEF nach den Vorschriften eines anderen nationalen Regelwerks

durchgeführt worden sind.

4.3.33 Der ETR kann kommerziell sensitive oder der nationalen Geheimhaltung unterliegende Informationen enthalten, die dem breiten Publikum nicht zugänglich gemacht werden dürfen. Daher kann die Verfügbarkeit des ETR nur für die ITSEF garantiert werden, die innerhalb desselben nationalen Regelwerks tätig sind. Reevaluationsinformationen sind außerdem optional und nicht immer im ETR zu finden.

4.3.34 Das Zertifikat/der Zertifizierungsreport ist öffentlich zugänglich und enthält eine Zusammenfassung des EVG und seiner Evaluation (siehe Teil 2 des ITSEM). Daher haben Antragsteller jederzeit die Möglichkeit, den ITSEFs Zertifikate/Zertifizierungsreports zur Verfügung zu stellen.

4.3.35 Was die Frage der Verfügbarkeit von Evaluationsergebnissen betrifft, gelten in sämtlichen Fällen die Vorschriften der nationalen Regelwerke.

Kapitel 4.4 Durchführung der Evaluation

Einleitung

4.4.1 Im vorliegenden Kapitel wird der Evaluationsprozeß dargelegt, der für alle anhand von den ITSEC durchgeführten Evaluationen empfohlen wird; außerdem werden eine Reihe von verbindlichen Anforderungen festgelegt. Die verfahrenstechnischen Aspekte für den Ablauf dieses Verfahrens (z.B. die detaillierten Verfahrensregeln, die bei der Erstellung von **Mängelberichten** im gesamten Verlauf einer Evaluation einzuhalten sind) werden in diesem Kapitel nicht vorgeschrieben. Diese Aspekte sind in das Ermessen der nationalen Regelwerke gestellt.

4.4.2 Der Evaluationsprozeß soll mit den Grundsätzen und Grundprinzipien übereinstimmen, die in Teil 3 des ITSEM dargelegt werden. Dabei geht es darum, die Planung, Durchführung und Protokollierung der Evaluation in der Weise abzuwickeln, daß die Übereinstimmung mit den ITSEC und dem ITSEM ohne weiteres ersichtlich ist.

4.4.3 Die durchgeführten technischen Arbeiten werden in den restlichen Abschnitten mit den Überschriften *Arbeitspläne* und *Anwendung der ITSEC* sowie in Kapitel 4.5 behandelt.

Arbeitspläne

Überblick

4.4.4 **Damit ein EVG zertifiziert werden kann, muß seine Evaluation in Übereinstimmung mit den Anforderungen von ITSEC/ITSEM und des entsprechenden nationalen Regelwerks durchgeführt werden.**

4.4.5 Eine Evaluation wird durchgeführt, indem alle in den ITSEC festgelegten Aufgaben ausgeführt werden. Zur Beschreibung der Struktur einer Evaluation und der Abhängigkeiten zwischen den Evaluatoraufgaben wird im vorliegenden Abschnitt der Begriff 'generischer Evaluationsarbeitsplan (EWP)' eingeführt.

4.4.6 Ein generischer EWP beschreibt, wie die für die Evaluation erforderlichen Arbeiten organisiert werden; er beschreibt also die mit der Evaluation zusammenhängenden Aktivitäten und die zwischen ihnen bestehenden Beziehungen.

4.4.7 Ein generischer EWP ist darauf ausgelegt, bei der Evaluation einer Vielzahl von Systemen und Produkten Verwendung zu finden. Außerdem soll er allgemein gesprochen für alle Evaluationsstufen anwendbar sein. Es sind viele allgemein verwendbare generische EWPs denkbar; einige von ihnen sind effizienter und flexibler als andere, jedoch kann möglicherweise jeder von ihnen gültige Auslegungen der ITSEC implementieren.

4.4.8 Der generische EWP drückt in einfacher Form aus, wie eine Evaluation in Übereinstimmung mit den Evaluationsgrundsätzen und den Grundprinzipien laut Teil 3 des ITSEM durchzuführen ist.

4.4.9 Die geforderten Evaluationsbeiträge sind in Teil 6, Anhang 6.A, aufgeführt. Der vorliegende Abschnitt befaßt sich mit der Evaluation dieser Evaluationsbeiträge. Die Evaluation anhand der ITSEC umfaßt folgende Tätigkeiten:

a) die Überprüfung der Übereinstimmung der Evaluationsbeiträge mit den ITSEC-Anforderungen;

b) die Überprüfung der ordnungsgemäßen Implementierung der Sicherheitsanforderungen, die in den Sicherheitsvorgaben spezifiziert sind;

c) die Überprüfung des betriebsbereiten EVG auf **ausnutzbare Schwachstellen**.

4.4.10 Das Obige kann wie folgt zusammengefaßt werden: "Es sind alle in den ITSEC festgelegten Aufgaben zur Bewertung der Korrektheit und der Wirksamkeit durchzuführen." Es ist jedoch unmöglich, jede einzelne Evaluatoraufgabe auf dieser generischen Ebene zu behandeln, da unter Umständen eine Vielzahl von EVG nach jeder der Evaluationsstufen evaluiert werden muß. Daher wird der Begriff 'Aktivität' eingeführt, wodurch sich die Möglichkeit ergibt, den Evaluationsprozeß generisch zu diskutieren.

4.4.11 Der Unterschied zwischen *Aufgaben* und *Aktivitäten* ist unbedingt zu beachten. Eine *Aufgabe* ist eine Evaluatoraufgabe laut den ITSEC. Eine *Aktivität* ist eine generische Gruppe von Aufgaben mit einem spezifischen Zweck wie etwa die Zuordnung einer Evaluatorentscheidung zu einer bestimmten **Darstellung**.

Generische Evaluationsaktivitäten

4.4.12 In der folgenden (ungeordneten) Liste sind die Bezeichnungen der während der Evaluationsphase durchgeführten generischen Evaluationsaktivitäten aufgeführt. Die Nummern der ITSEC-Absätze sind in geschweiften Klammern {} angegeben; *n* steht in der Liste für eine Zahl zwischen 1 und 6.

Analyse der Eignung überprüfen	{3.16}
Analyse des Zusammenwirkens überprüfen	{3.20}
Stärke der Mechanismen untersuchen	{3.24}
Konstruktionsschwachstellen untersuchen	{3.28}
Benutzerfreundlichkeit untersuchen	{3.33}
Operationelle Schwachstellen untersuchen	{3.37}
Die Anforderungen überprüfen	{En.4}
Den Architekturentwurf überprüfen	{En.7}
Den Feinentwurf überprüfen	{En.10}
Die Implementierung überprüfen	{En.13}
Die Entwicklungsumgebung überprüfen	{En.17, En.20, En.23}
Die Betriebsdokumentation überprüfen	{En.27, En.30}
Die Betriebsumgebung überprüfen	{En.34, En.37}
Penetrationstests durchführen	{3.24, 3.28, 3.33, 3.37}
Berichte erstellen	{5.11}

4.4.13 Mit Ausnahme von *Penetrationstest durchführen* entsprechen die technischen Evaluationsaktivitäten der Anwendung der Wirksamkeits- oder Korrektheitskriterien, wie sie in den ITSEC erscheinen.

4.4.14 Was die Bezeichnung der Aktivitäten angeht, besteht der einzige Unterschied zwischen *überprüfen* und *untersuchen* darin, daß *überprüfen* im wesentlichen die Analyse der Evaluationsbeiträge beinhaltet, während *untersuchen* auch eine Eingabe in Penetrationstests umfaßt. Die Durchführung von Penetrationstests ist zwar explizit mit diesen Aktivitäten verbunden, wurde jedoch aus zwei Gründen einer getrennten Aktivität zugeordnet:

a) um hervorzuheben, daß die vorhergehenden Analysen konsolidiert und die Tests während dieser Aktivität konzipiert werden;

b) um aufzuzeigen, daß eine große Zahl realer Tests normalerweise gemeinsam durchgeführt wird.

4.4.15 Die Aktivität *Analyse der Eignung überprüfen* erfordert die Überprüfung der vom Entwickler vorgenommenen Analyse der Eignung durch die Evaluatoren. Dabei können Schwachstellen aufgedeckt werden, die dadurch entstehen, daß eine sicherheitsspezifische Funktion ein Sicherheitsziel für eine in den Sicherheitsvorgaben aufgezeigte Bedrohung nicht zu erfüllen vermag.

4.4.16 Die Aktivität *Analyse des Zusammenwirkens überprüfen* erfordert die Prüfung der vom Entwickler durchgeführten Analyse des Zusammenwirkens durch die Evaluatoren sowie die Prüfung der Frage, ob die Gesamtmenge der sicherheitsspezifischen Funktionen die Gesamtheit der Sicherheitsziele angemessen berücksichtigt oder nicht.

4.4.17 Die Aktivität *Stärke der Mechanismen untersuchen* erfordert auf seiten der Evaluatoren die Identifizierung der Mechanismen, die nicht die von den Sicherheitsvorgaben geforderte Mindeststärke der Mechanismen erreichen. Die Stärke der Mechanismen wird in Teil 6, Anhang 6.C behandelt.

4.4.18 Das von den Evaluatoren bei der Bewertung der Korrektheit erarbeitete Wissen wird im Rahmen der Aktivität *Konstruktionsschwachstellen untersuchen* dazu verwendet, eventuelle Konstruktionsschwachstellen des EVG aufzuzeigen.

4.4.19 Im Rahmen der Korrektheitsevaluation ermittelte Fehler sind eine der möglichen Ursachen von Konstruktionsschwachstellen. Es ist jedoch durchaus möglich, daß eine Komponente als korrekt (im Sinne einer **korrekten Verfeinerung**) angesehen wird, aber dennoch Schwachstellen aufweist. Dies ist der Fall,

a) weil mit fortschreitender Verfeinerung eine neue Funktionalität hinzukommt;

b) weil mit den zur Verifizierung der Verfeinerung verwendeten Standardtechniken bestimmte Schwachstellen wie beispielsweise verdeckte Kanäle nicht ermittelt werden können.

4.4.20 Daher erfordert diese Aktivität auf seiten der Evaluatoren die Prüfung von Fehlern bei der Verfeinerung und der in den einzelnen Entwicklungsphasen zusätzlich eingeführten Funktionalität, um ausnutzbare Schwachstellen aufzudecken.

4.4.21 Die Aktivität *Benutzerfreundlichkeit untersuchen* erfordert die Prüfung der ungesicherten Betriebsarten des EVG durch die Evaluatoren. Folglich steht diese Bewertung in engem Zusammenhang mit den anderen betriebsbezogenen Bewertungen.

4.4.22 Die Aktivität *operationelle Schwachstellen untersuchen* erfordert die Prüfung des Betriebs des EVG durch die Evaluatoren. Die Evaluatoren versuchen, Schwachstellen in der gewählten Betriebsart des EVG aufzuzeigen.

4.4.23 Operationelle Schwachstellen betreffen den Grenzbereich zwischen IT- und Nicht-IT-**Gegenmaßnahmen** wie etwa die physische Sicherheit betreffende Betriebsprozeduren, nichtelektronische Formen der Schlüsselverwaltung und die Ausgabe von Sicherheitsausweisen. Nicht-IT-Gegenmaßnahmen sind für die Evaluatoren von Belang, wenn mindestens einer der folgenden Punkte zutrifft:

a) Sie sind Bestandteil der Betriebsdokumentation;

b) die Sicherheitsvorgaben werden auf der Basis einer System-Sicherheitspolitik formuliert (siehe ITSEC, Absätze 2.8-2.15);

c) sie sind Bestandteil der Produktbeschreibung.

4.4.24 Nicht-IT-Gegenmaßnahmen kommen im allgemeinen dann zum Tragen, wenn aufgrund von Konstruktionsschwachstellen solche Nicht-IT-Gegenmaßnahmen zur Gewährleistung der Sicherheit des EVG erforderlich werden. Daher sind die Evaluatoren bei der Evaluation operationeller Schwachstellen in erster Linie bemüht sicherzustellen, daß die Nicht-IT-Gegenmaßnahmen den erkannten Konstruktionsschwachstellen auch tatsächlich entgegenwirken.

4.4.25 Die Aktivität *Die Anforderungen überprüfen* setzt voraus, daß die Evaluatoren sicherstellen, daß die sicherheitsspezifischen Funktionen in den Sicherheitsvorgaben angemessen definiert und die Vorgaben in sich widerspruchsfrei sind. In den Sicherheitsvorgaben sollen die sicherheitsspezifischen Funktionen, die angestrebte Evaluationsstufe, die Bewertung der Stärke der Mechanismen und die bei der Evaluation zu berücksichtigenden externen Sicherheitsmaßnahmen eindeutig festgelegt werden.

4.4.26 Der erste Entwicklungsschritt von den Anforderungen zum Architekturentwurf ist von besonderer Bedeutung, da er für die Top-Level-Zuordnung abstrakter Funktionen zu logischen und physischen Komponenten sorgt. Eine wichtige Bewertungsaufgabe für die Evaluatoren, die im Rahmen der Aktivität *Den Architekturentwurf überprüfen* durchgeführt wird, ist die Entscheidung, ob die Trennung der sicherheitsspezifischen von den nicht sicherheitsspezifischen Funktionen 'klar und wirksam' ist, denn dies *ermöglicht die Konzentration der Evaluation auf begrenzte Bereiche des EVG, die zur Sicherheit beitragen, und erlaubt, der Erfüllung der Sicherheitsvorgaben in dem Maße leicht zu folgen, in welchem der Entwurf nach und nach verfeinert wird*. (Aus Absatz 4.20 der ITSEC)

4.4.27 Die Aktivität *Den Feinentwurf überprüfen* setzt voraus, daß die Evaluatoren sicherstellen, daß der Grundsatz der Trennung befolgt wird und daß die sicherheitsspezifischen Komponenten korrekt implementiert worden sind. Es können mehrere Feinentwurfsstufen vorliegen.

4.4.28 Die Ausführungen im vorstehenden Absatz gelten in sehr ähnlicher Weise für die Bewertung der Implementierung im Rahmen der Aktivität *Die Implementierung überprüfen*. Der Unterschied liegt allein im Detaillierungsgrad, insoweit als sich die Implementierung per Definition mit der Weiterentwicklung der Basiskomponenten und Funktionseinheiten befaßt, die durch die letzten Stufen des Feinentwurfs identifiziert werden (so daß funktionale Tests möglich werden).

4.4.29 Die Aktivität *Die Entwicklungsumgebung überprüfen* erfordert die Überprüfung der Entwicklungsstandards - insbesondere für die auf den verschiedenen Entwicklungsstufen zu verwendenden Sprachen - durch die Evaluatoren. Diese müssen das Vertrauen gewinnen, daß der evaluierte EVG dem entwickelten EVG entspricht und daß die bei der Implementierung verwendeten Notationen eindeutig sind. Diese Aktivität befaßt sich daher mit Fragen wie

a) der Konfigurationskontrolle;

b) Programmiersprachen und Compilern;

c) der Sicherheit beim Entwickler.

4.4.30 Die Aktivität *Die Betriebsdokumentation überprüfen* erfordert die Überprüfung der Frage durch die Evaluatoren, ob der EVG seinen Sicherheitszielen entsprechend verwaltet und eingesetzt werden kann.

4.4.31 Die Aktivität *Die Betriebsumgebung überprüfen* erfordert die Überprüfung der korrekten Auslieferung des EVG durch die Evaluatoren; des weiteren den Nachweis, daß der betriebsbereite EVG eine genaue Kopie des EVG in der Entwicklungsumgebung ist und nach Maßgabe seiner Sicherheitsziele generiert und betrieben werden kann.

4.4.32 Die Aktivität *Penetrationstest durchführen* erfordert von den Evaluatoren, daß sie die ITSEC-Tätigkeit 'Penetrationstests durchführen, anwenden und auswerten' (z.B. die im Rahmen der Aktivität *Konstruktionsschwachstellen untersuchen* durchgeführten Aufgaben), und dies immer mit Blick auf Aspekte der Wirksamkeitsbewertung und immer zu demselben Zweck: um zu ermitteln, ob potentielle Schwachstellen in der Praxis ausgenutzt werden können.

4.4.33 Die Ergebnisse der Evaluation müssen aufgezeichnet werden, weshalb die Aktivität *Berichte erstellen* eingeführt werden muß. Die Evaluatoren erstellen einen den Anforderungen von Kapitel 4.7 entsprechenden ETR.

4.4.34 In Abbildung 4.4.1 werden die ITSEC-Aufgaben in Verbindung mit den dazugehörigen Aktivitäten dargestellt. In der Abbildung schließt *überprüfen* * alle relevanten Überprüfungsaufgaben ein, die ein Evaluator laut den ITSEC durchführen muß. Die anderen Aufgaben werden in vollem Umfang dargelegt.

Abbildung 4.4.1 Aktivitäten und zugehörige Evaluatoraufgaben laut den ITSEC

Aktivität	Aufgabe
Analyse der Eignung überprüfen	Überprüfen *
Analyse des Zusammenwirkens überprüfen	Überprüfen *
Stärke der Mechanismen untersuchen	Überprüfen *
Konstruktionsschwachstellen untersuchen	Überprüfen *, unabhängige Schwachstellenanalyse durchführen, wobei sowohl die aufgeführten als auch alle anderen bekannten Konstruktionsschwachstellen zu berücksichtigen sind, die bei der Evaluation ermittelt werden.
Benutzerfreundlichkeit untersuchen	Überprüfen *, jede Konfigurations- und Installationsprozedur nachvollziehen, um zu überprüfen, ob der EVG sicher konfiguriert und eingesetzt werden kann, wobei allein die Benutzer- und Systemverwalterdokumentation als Orientierungshilfe zu verwenden ist.
Operationelle Schwachstellen untersuchen	Überprüfen *, unabhängige Schwachstellenanalyse durchführen, wobei sowohl die aufgeführten als auch alle anderen bekannten Konstruktionsschwachstellen zu berücksichtigen sind, die bei der Evaluation ermittelt werden.
Die Anforderungen überprüfen	Überprüfen *
Den Architekturentwurf überprüfen	Überprüfen *
Den Feinentwurf überprüfen	Überprüfen *
Die Implementierung überprüfen	Überprüfen * Die Bibliothek von Testprogrammen zur stichprobenw Überprüfung der Testergebnisse verwenden. Zusätzliche Tests zur Fehlersuche durchführen. Mutmaßliche Inkonsistenzen zwischen Quellcode und ausführbarem Code unter- suchen, die bei den Tests mit vom Antragsteller bereitgestellten Werkzeugen entdeckt wurden.
Die Entwicklungsumgebung überprüfen Konfigurationskontrolle Programmiersprachen und Compiler Sicherheit beim Entwickler	 Überprüfen *, die Entwicklerwerkzeuge zur Erstellung ausgewählter Teile des EVG verwenden und mit der vorgelegten Version des EVG vergleichen. Überprüfen * Überprüfen * Nach Fehlern in den Verfahren suchen.
Die Betriebsdokumentation überprüfen	Überprüfen *
Die Betriebsumgebung überprüfen Auslieferung und Konfiguration Anlauf und Betrieb	Überprüfen * Nach Fehlern in den Verfahren für die Systemgenerierung suchen. Überprüfen * Nach Fehlern in den Verfahren suchen.
Penetrationstests durchführen	(Stärke der Mechanismen) Erforderlichenfalls Penetrationstests durchführen, um die angestrebte Mindeststärke der Mechanismen zu bestätigen oder zu widerlegen. (Konstruktionsschwachstellen) Penetrationstest durchführen, um die tatsächliche praktische Ausnutzbarkeit der bekannten Schwachstellen zu bestätigen oder zu widerlegen. (Benutzerfreundlichkeit) Erforderlichenfalls weitere Tests durchführen, um die Analyse der Benutzerfreundlichkeit zu bestätigen oder zu widerlegen. (Operationelle Schwachstellen) Penetrationstest durchführen, um die tatsächliche praktische Ausnutzbarkeit der bekannten Schwachstellen zu bestätigen oder zu widerlegen.

Generischer Evaluationsarbeitsplan (EWP)

4.4.35 Die ITSEC führen eine implizite Ordnung der Aktivitäten ein, indem z.B. angegeben wird, daß Korrektheit und Wirksamkeit miteinander verknüpft sind. Daraus muß jedoch eine explizite Ordnung gemacht werden.

4.4.36 Es wird der Begriff 'Zwischenergebnis' eingeführt, um Informationen darzustellen, die von den Evaluatoren im Rahmen einer bestimmten Aktivität generiert und im Rahmen einer anderen verwendet werden. Sie können aus Evaluationsbeiträgen abgeleitet oder herauskopiert sein, werden aber einzig und allein von Evaluatoren zur Ausübung ihrer Funktionen verwendet. Diese Zwischenergebnisse sollen zur Unterstützung der **Wiederholbarkeit** und künftiger Reevaluationen aufgezeichnet werden. Zwischenergebnisse können zur Ableitung generischer Abhängigkeiten zwischen Evaluationsaktivitäten und somit auch eines Ablaufplans für die einschlägigen Aktivitäten herangezogen werden.

4.4.37 Einige Zwischenergebnisse werden direkt von Evaluationsbeiträgen abgeleitet. Zu diesen gehören

a) die in den Sicherheitsvorgaben aufgezeigten Bedrohungen;

b) die in den Sicherheitsvorgaben aufgezeigten externen Sicherheitsmaßnahmen;

c) die in den Sicherheitsvorgaben aufgezeigten sicherheitsspezifischen Funktionen;

d) die anhand der Anforderungen aufgezeigten sicherheitsrelevanten Ereignisse;

e) die Komponenten im Architekturentwurf (und deren Arten - sicherheitsspezifisch, sicherheitsrelevant oder andere);

f) die im Entwurf aufgezeigten sicherheitsrelevanten Funktionen;

g) die in den Evaluationsbeiträgen aufgezeigten Sicherheitsmechanismen;

h) die die Sicherheit betreffenden Systemverwaltungsfunktionen, die in der Betriebsdokumentation aufgezeigt werden;

i) die in der Analyse der Stärke der Mechanismen aufgezeigten kritischen Sicherheitsmechanismen.

4.4.38 Weitere Zwischenergebnisse ergeben sich aus den von den Evaluatoren durchgeführten Zusatzarbeiten, und zwar

a) die von den Evaluatoren aufgezeigten potentiellen Konstruktionsschwachstellen;

b) die von den Evaluatoren aufgezeigten potentiellen operationellen Schwachstellen;

c) die von den Evaluatoren aufgezeigten Fehler;

d) die von den Evaluatoren festgelegten Penetrationstests;

e) die von den Evaluatoren aufgezeigten ausnutzbaren Schwachstellen.

4.4.39 Der im Rahmen der Evaluation erstellte ETR stellt ein Ergebnis dar.

4.4.40 In Abbildung 4.4.2 sind die Evaluationsaktivitäten und die Evaluationsprodukte in tabellarischer Form dargestellt. Die Evaluationsprodukte sind entweder eine Ausgabe einer Aktivität (dargestellt durch 'O'=Output) oder eine Eingabe zu einer Aktivität (dargestellt durch 'I'=Input). Die Ausgabe einer Aktivität kann entweder ein komplettes Produkt oder ein Beitrag zu einem durch eine andere Aktivität erzeugten Evaluationsprodukt sein. So erbringen beispielsweise mehrere Wirksamkeitsaktivitäten einen Beitrag zu der von den Evaluatoren erstellten Liste der Konstruktionsschwachstellen, die anschließend als Eingabe in die Penetrationstests dient.

4.4.41 Die Evaluationsaktivitäten sind somit nicht nur auf die relevanten Entwickler-Evaluationsbeiträge ausgerichtet, sondern auch auf die Evaluationsprodukte. Beispielsweise setzt die Aktivität 'Konstruktionsschwachstellen überprüfen' voraus, daß die Evaluatoren die Ausgabe der Aktivität 'Stärke der Mechanismen untersuchen' sowie die entwicklereigene Liste der bekannten Konstruktionsschwachstellen überprüfen.

4.4.42 Abhängigkeiten in der Abfolge werden durch Anwendung der folgenden Regeln aufgezeigt:

a) Alle Aktivitäten, die ein Evaluationsprodukt erbringen oder zu ihm beitragen, müssen abgeschlossen sein, bevor eine Aktivität, die von diesem Evaluationsprodukt Gebrauch macht, ihrerseits abgeschlossen werden kann.

b) Damit eine Aktivität abgeschlossen werden kann, müssen alle dafür relevanten Evaluationsprodukte berücksichtigt worden sein (zu beachten ist, daß diese Regel nicht ausschließt, daß Aktivitäten nur teilweise durchgeführt und zu einem späteren Zeitpunkt abgeschlossen werden; beispielsweise kann eine Untermenge sicherheitsspezifischer Funktionen und Komponenten einem Penetrationstest unterzogen werden, bevor andere sicherheitsspezifische Funktionen bei der Implementierung überprüft worden sind).

4.4.43 Die Aktivität 'Penetrationstest durchführen' kann beispielsweise erst dann abgeschlossen werden, wenn die Aktivität 'Analyse der Eignung überprüfen' abgeschlossen worden ist (siehe Abbildung 4.4.3). Dies liegt daran, daß die Aktivität 'Analyse der Eignung überprüfen' Konstruktionsschwachstellen aufzeigen kann, die von den Evaluatoren im Rahmen der Aktivität 'Konstruktionsschwachstellen überprüfen' berücksichtigt werden müssen. Die von den Evaluatoren erstellte Liste der Konstruktionsschwachstellen wird anschließend dazu benutzt, die Penetrationstests festzulegen, die im Rahmen der Aktivität 'Penetrationstest durchführen' zur Klärung der Frage der Ausnutzbarkeit der Schwachstellen durchgeführt werden.

4.4.44 Anhand der in Abbildung 4.4.2 und in den obigen Regeln (a) und (b) aufgezeigten Abhängigkeiten kann ein Diagramm erstellt werden (siehe Abbildung 4.4.4), das die typische Abfolge des Abschlusses der Aktivitäten darstellt.

4.4.45 Abbildung 4.4.4 stellt somit einen 'generischen EWP' dar.

Abbildung 4.4.2 Abhängigkeit zwischen Aktivitäten

Aktivität / Zwischen ergebnis	Bedrohungen	Externe Sicherheitsmaßnahmen	SEF	Sicherheitsrelevante Ereignisse	Komponenten (einschl. Basiskomponenten)	Sicherheitsmechanismen	Systemverwalterfunktionen bzgl. Sicherheit	Kritische Sicherheitsmaßnahmen	Konstruktionsschwachstellen	SRF	Operationelle Schwachstellen	Fehler	Penetrationstests	Ausnutzbare Schwachstellen	ETR
Anforderungen	IO	IO	IO	IO		O					O	O			
Architektur		I	I	O	IO					O		O			
Entwurf			I	O	IO	O		O		O		O			
Implementierung			I	O	IO	I						O			
Entwicklungsumgebung	I*				I							O			
Betriebsdokumentation			I	I	I		IO					O			
Betriebsumgebung			I		I							O			
Eignung	I	I	I			I			O						
Zusammenwirken			I			I			O						
Stärke der Mechanismen						I		IO	O				O		
Konstruktionsschwachstellen	I	I	I			I		I	I	I			O		
Benutzerfreundlichkeit	I	I	I	I			I				O		O		
Operationelle Schwachstellen	I	I	I			I		I			I		O		
Penetrationstests													I	O	
ETR erstellen	I	I	I		I	I		I	I	I	I	I	I	I	O

Legende: * bedeutet, daß Bedrohungen der Entwicklungsumgebung in den Sicherheitsvorgaben dokumentiert sein können oder nicht
I bedeutet, daß eine Aktivität ein Zwischenergebnis als Eingabe benötigt
O bedeutet, daß eine Aktivität ein Zwischenergebnis als Ausgabe erzeugt

SEF: Sicherheitsspezifische Funktion
SRF: Sicherheitsrelevante Funktion

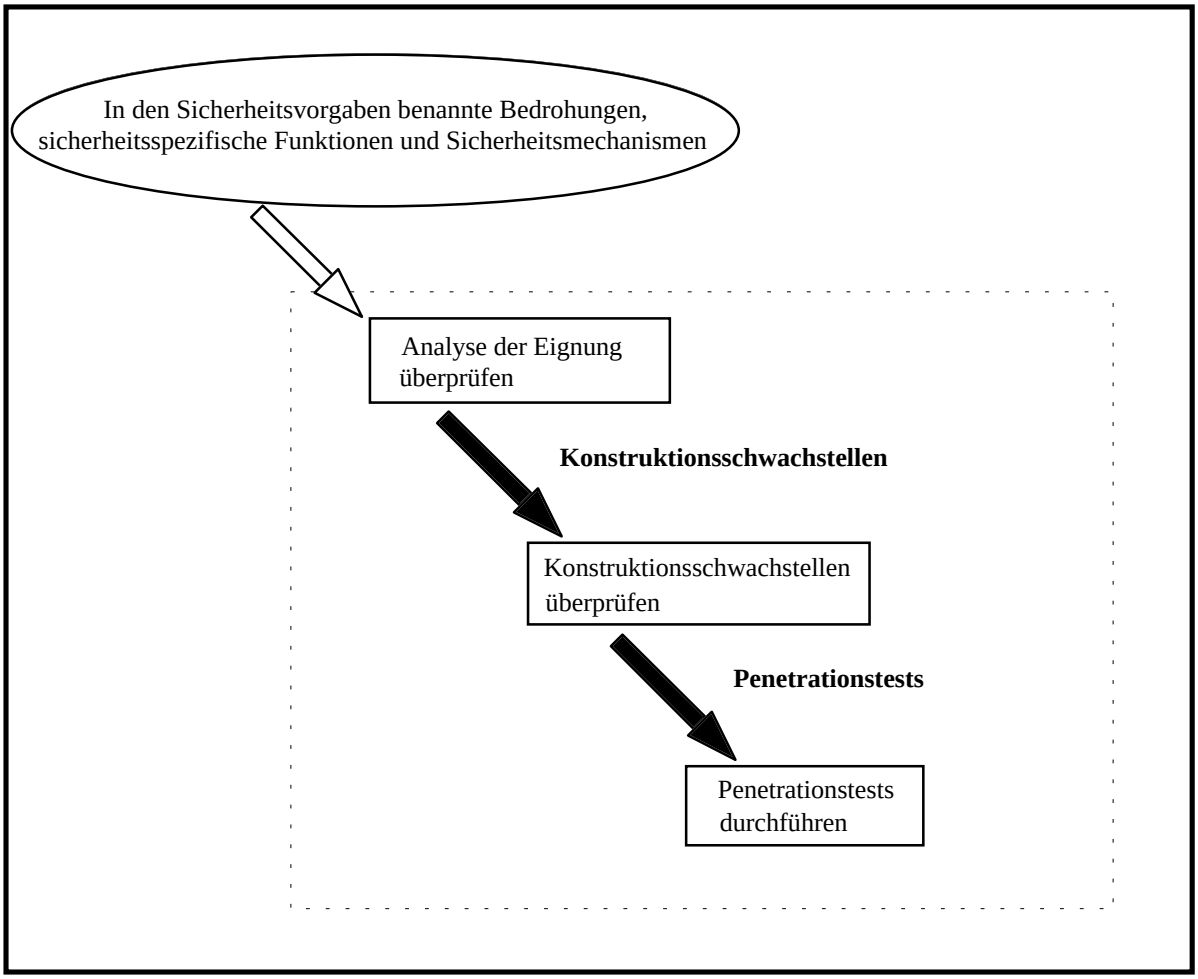


Abbildung 4.4.3 Beispiel für die Abhängigkeiten zwischen den Aktivitäten

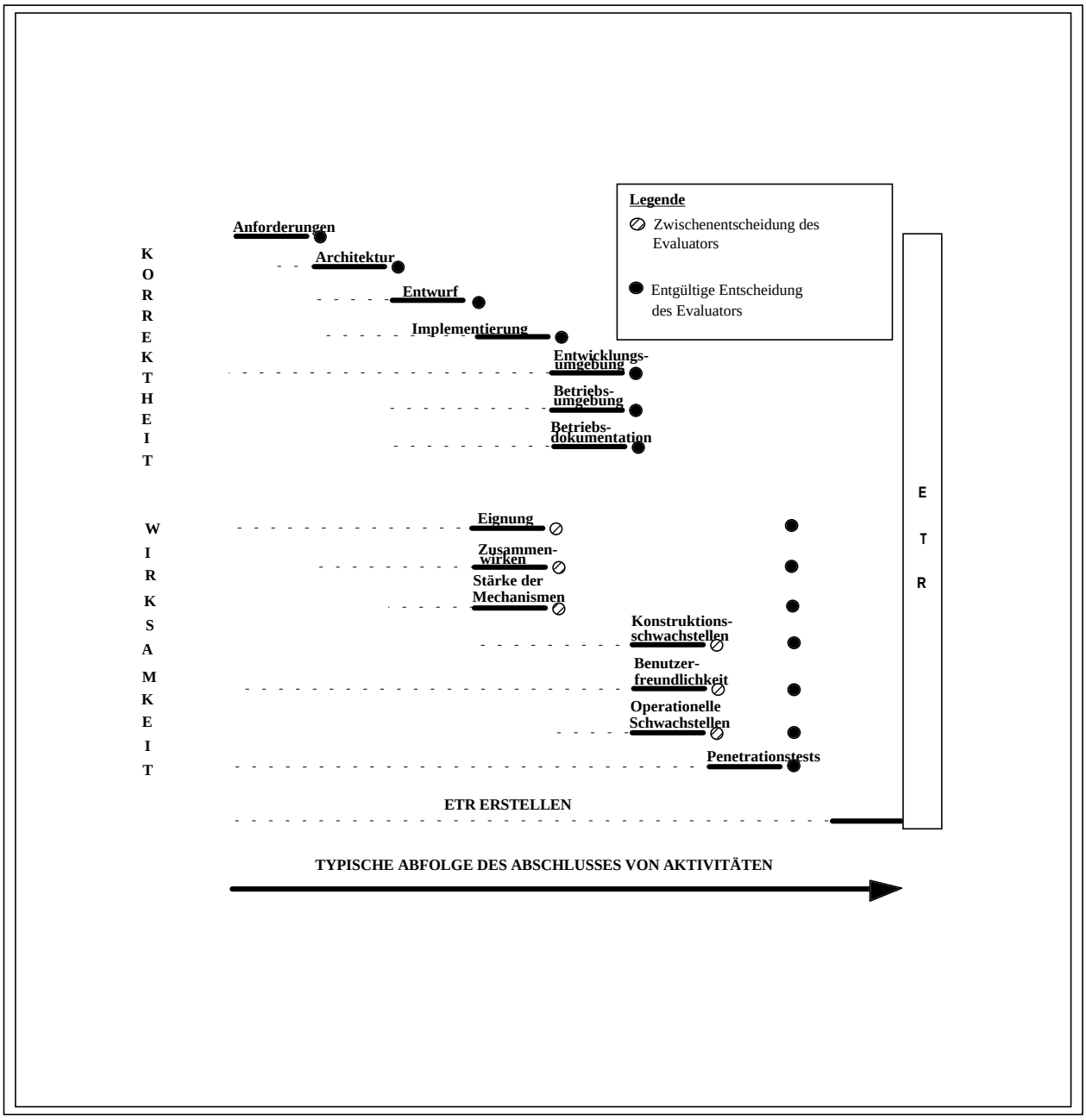


Abbildung 4.4.4 Generischer Evaluationsarbeitsplan (EWP)

Erstellung von Evaluationsarbeitsplänen (EWPs)

4.4.46 Bevor mit der Durchführung einer Evaluation begonnen wird, sollen sich die Evaluatoren Klarheit über die erforderlichen Arbeiten verschaffen. Daraus ergibt sich die Notwendigkeit einen Plan für die auszuführenden Arbeiten zu erstellen, d.h. eines EWP.

4.4.47 Um die Evaluationsarbeit in einer handhabbaren Art und Weise planen und darüber berichten zu können, ist das Konzept eines Arbeitspaketes erforderlich. Unter einem Arbeitspaket ist eine von den Evaluatoren bearbeitete Arbeitseinheit zu verstehen.

4.4.48 Eine Aktivität kann in mehrere Arbeitspakete unterteilt sein bzw. mehrere Aktivitäten können innerhalb eines Arbeitspakets ausgeführt werden.

4.4.49 Bei der Erstellung spezifischer EWPs anhand des vorstehend genannten generischen EWP müssen die spezifischen Merkmale einer Evaluation in den dazugehörigen Plan eingearbeitet werden. Dazu gehören

a) die angestrebte Evaluationsstufe und die Bewertung der Mindeststärke der Mechanismen;

b) spezifische Bezeichnungen von Evaluationsbeiträgen; z.B. Bezugnahme auf den entsprechenden Teil eines oder mehrerer Dokumente, die die Architektur enthalten (siehe Teil 6, Anhang 6.A);

c) eine spezifische Menge von Abstraktionsstufen für den Feinentwurf;

d) Angaben darüber, ob es sich um eine Reevaluation handelt und ob zertifizierte Komponenten des EVG vorhanden sind (dieser Punkt wird in Kapitel 4.6 behandelt);

e) Angaben darüber, ob es sich bei dem EVG um ein System oder um ein Produkt handelt;

f) die Anforderungen in bezug auf die Berichterstattung, z.B. externe Besprechungen;

g) eine Liste der Evaluationsbeiträge mit einem Zeitplan für die Verfügbarkeit der Evaluationsbeiträge durch den Antragsteller;

h) Angaben darüber, ob im ETR Reevaluationsinformationen erforderlich sind.

4.4.50 Die Wirkung der angestrebten Evaluationsstufe ist beträchtlich. Von der gewählten Evaluationsstufe hängt es ab, welche Evaluationsbeiträge von den Evaluatoren benötigt werden, welchen Inhalt die Evaluationsbeiträge haben müssen und was die Evaluatoren zu tun haben, um die Evaluationsbeiträge zu bewerten.

4.4.51 Laut den ITSEC wird beispielsweise keine Analyse des Quellcodes für E2 und darunter verlangt, weshalb der Antragsteller nicht verpflichtet ist, den Evaluatoren diesen Code zur Verfügung zu stellen (der Grund ist, daß manche korrektheitsbezogenen Aktivitäten auf den niedrigeren Evaluationsstufen nicht durchgeführt werden).

4.4.52 Bei einer Produktevaluation kleineren Umfangs nach einer niedrigen angestrebten Evaluationsstufe, in deren Fall der gesamte Evaluationsaufwand vielleicht weniger als ein halbes Personenjahr innerhalb eines Zeitraums von zwei Monaten beträgt, kann es durchaus angebracht sein, ein einziges Arbeitspaket mit der Bezeichnung *die Architektur auf Korrektheit untersuchen* zu bearbeiten oder sogar ein Arbeitspaket, das diese Aktivität mit der Aktivität *Analyse des Zusammenwirkens vornehmen* verbindet und sie zu einem einzigen Paket mit der Bezeichnung 'Architekturbewertung' zusammenfügt.

4.4.53 Im Gegensatz dazu wäre es bei der Evaluation eines umfangreichen, verteilten Systems nach E6, bei dem der gesamte Evaluationsaufwand unter Umständen mehrere Personenjahre beträgt, keineswegs unvernünftig, ein einziges Arbeitspaket für die eine Evaluatoraufgabe *Es ist zu überprüfen, ob die formalen Argumente wirksam sind* einzusetzen, da diese Aufgabe umfangreiche Überprüfungen der formalen Methodenarbeiten beinhalten kann.

4.4.54 Ein Beispiel für die Zerlegung einer Aktivität in Arbeitspakete wäre, wenn bei einer umfangreichen Systemevaluation die Aktivität *Penetrationstests durchführen* durch Arbeitspakete wie etwa 'Penetrationstests vorbereiten und spezifizieren' und 'Penetrationstests durchführen und weiterverfolgen' implementiert würde.

4.4.55 'Penetrationstest vorbereiten und spezifizieren' würde die administrativen Aspekte (wie Zugang zum Betriebsort und Verfügbarkeit von Büroräumen - siehe Teil 6, Anhang 6.A) sowie die technischen Aspekte der Dokumentierung eines Zeitplans für Penetrationstests und für den Anforderungen des nationalen Regelwerks entsprechende Tests umfassen.

4.4.56 Das Arbeitspaket 'Penetrationstest durchführen und weiterverfolgen' würde die konkrete Durchführung der dokumentierten Penetrationstests und die Protokollierung der Ergebnisse umfassen. Daneben kann es die Weiterverfolgung etwaiger Bereiche vermuteter Schwachstellen in Systemkomponenten beinhalten oder auch die Durchführung von Wiederholungstests mit Komponenten, die aufgrund der Aufdeckung von Schwachstellen bei früheren Penetrationstests festgelegt wurden.

4.4.57 Die Frage, ob der EVG ein System oder ein Produkt ist, hat technische Auswirkungen (z.B. erfordert die Überprüfung der Sicherheitsvorgaben etwas andere Arbeiten) wie auch planungsspezifische Auswirkungen (z.B. kann ein System über mehrere Betriebsorte verteilt sein, die alle aufgesucht werden müssen, und Penetrationstests können nur innerhalb eines vorab geplanten Zeitrahmens durchgeführt werden).

4.4.58 Ein Produkt kann der ITSEF als Evaluationsbeitrag zur Verfügung gestellt werden, so daß die Evaluatoren zur Durchführung von Penetrationstests ungehindert darauf zugreifen können; allerdings müßte die zu evaluierende Betriebsumgebung und Konfiguration von den Evaluatoren emuliert werden. Die Definition einer 'Evaluationskonfiguration' ist daher für die Produktevaluation besonders wichtig. Diese Definition soll zwischen Evaluatoren und Antragstellern abgesprochen werden. Sie muß im ETR dokumentiert werden (siehe Kapitel 4.7).

4.4.59 Die Ergebnisse der Penetrationstests werden im ETR - wie in Kapitel 4.7 beschrieben - festgehalten. Sie können auch in einer lokalen Evaluationsdatenbank gespeichert werden. Die Speicherung der Evaluationsergebnisse liegt im Ermessen des nationalen Regelwerks.

4.4.60 Wenn ein Antragsteller eine Modifikation eines EVG erwartet, das Zertifikat/den Zertifizierungsreport jedoch beibehalten möchte, kann er die Evaluatoren um Aufnahme von Informationen für eine **Auswirkungsanalyse** und die Reevaluation im optionalen Kapitel 7 des ETR ersuchen. Dies ist im EWP zu berücksichtigen.

Anwendung der ITSEC

Einleitung

4.4.61 Der Sinn einer Evaluation besteht darin, eine Evaluatorentscheidung über die Übereinstimmung eines EVG mit den Kriterien in den ITSEC herbeizuführen. Der Zertifizierungsprozeß erbringt ebenfalls eine Entscheidung, und zwar dahingehend, ob die Evaluation in Übereinstimmung mit ITSEC/ITSEM erfolgt ist und ob der EVG die angestrebte ITSEC-Evaluationsstufe erreicht hat.

4.4.62 Der vorliegende Abschnitt enthält Anleitungen für Evaluatoren, wie die ITSEC anzuwenden sind, um zu Evaluationsentscheidungen zu kommen.

Entscheidungen der Evaluatoren

4.4.63 Eine Entscheidung ergibt sich immer dann, wenn die Evaluatoren eine ITSEC-Evaluatoraufgabe abschließen. Die Entscheidung kann *akzeptierend, ablehnend* oder *nichtbeurteilend* sein. Beispielsweise kann die Aufgabe *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen* zu folgenden Entscheidungen führen:

a) *Akzeptierend*, wenn festgestellt wurde, daß die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

b) *Ablehnend*, wenn eine Nichterfüllung festgestellt wurde, derzufolge die zur Verfügung gestellten Informationen nicht alle Kriterien für Inhalt, Form und Nachweis erfüllten.

c) *Nichtbeurteilend*, wenn die Evaluatoren keine akzeptierende oder ablehnende Entscheidung treffen konnten. Diese Entscheidung weist darauf hin, daß die Evaluatoraufgabe nicht abgeschlossen ist, weil sie beispielsweise an einem Evaluationsbeitrag in Entwurfsform durchgeführt wurde oder der Evaluationsbeitrag für die Evaluatoren teilweise unverständlich war.

4.4.64 **Wenn eine ablehnende Entscheidung gefällt wird, müssen die Evaluatoren die betreffenden Beteiligte unter Zuhilfenahme des Mängelberichterstattungsverfahrens in Kenntnis setzen.** Es besteht die Möglichkeit, mit dem Antragsteller ein Verfahren zur Beseitigung des Mangels abzusprechen. Dies kann im Erfolgsfall eine Abänderung der Entscheidung bewirken.

4.4.65 **Alle auf 'nichtbeurteilend' lautenden Entscheidungen müssen letzten Endes in akzeptierende oder ablehnende Entscheidungen umgewandelt werden. Für den Fall, daß eine auf 'nichtbeurteilend' lautende Entscheidung gefällt wird, müssen die Evaluatoren mit dem Antragsteller ein Verfahren vereinbaren, das zu einer endgültigen Entscheidung führt.** Dieses könnte einschließen, daß man auf eine spätere Darstellung wartet, auf eine spätere Version derselben Darstellung wartet, oder daß man sich mit dem Entwickler trifft, um die anstehenden technischen Fragen zu besprechen. **Wird keine Lösung gefunden, muß eine ablehnende Entscheidung gefällt werden.**

4.4.66 **Für eine Entwicklungsdarstellung wie z.B. die Anforderungen oder den Architekturentwurf muß eine Entscheidung hinsichtlich ihrer Korrektheit ausgesprochen werden. Eine Darstellung bekommt eine akzeptierende Entscheidung zugesprochen, wenn alle an ihr durchgeführten Evaluatoraufgaben eine akzeptierende Entscheidung erbrachten. Eine Darstellung bekommt eine ablehnende Entscheidung zugesprochen, wenn eine der an ihr durchgeführten Evaluatoraufgaben eine ablehnende Entscheidung erbrachte. Eine Darstellung bekommt die Entscheidung 'nichtbeurteilend' zugesprochen, wenn die an ihr durchgeführten Evaluatoraufgaben zwar keine ablehnende Entscheidung, aber eine oder mehrere auf 'nichtbeurteilend' lautende Entscheidungen erbrachten.**

4.4.67 **Für jeden Wirksamkeitsaspekt (z.B. Benutzerfreundlichkeit oder Eignung) muß eine Entscheidung hinsichtlich der Wirksamkeit ausgesprochen werden. Eine Zwischenentscheidung wird aus den für den betreffenden Aspekt durchgeführten Evaluatoraufgaben in der gleichen Weise wie für die Korrektheit abgeleitet.**

4.4.68 Es ist zu bedenken, daß jeder Wirksamkeitsaspekt eine Evaluatoraufgabe *'Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in der Abbildung 4 für die angestrebte Evaluationsstufe angegeben sind'* beinhaltet. Abbildung 4 in den ITSEC zeigt, daß die Darstellung 'Betrieb' für alle Evaluationsstufen zu berücksichtigen ist. Desgleichen kann der Penetrationstest Schwachstellen im Hinblick auf eines der Wirksamkeitskriterien aufzeigen. **Daher kann eine endgültige Entscheidung über die Wirksamkeit erst nach Abschluß der Penetrationstests gefällt werden.**

4.4.69 Die Bewertungen der Konstruktionsschwachstellen und der operationellen Schwachstellen setzt voraus, daß die Evaluatoren unabhängige Analysen unter Berücksichtigung der im Verlauf der Evaluation entdeckten Schwachstellen durchführen. **Dies bedeutet, daß diese Bewertungen erst nach der Evaluation auf Korrektheit abgeschlossen werden können.**

4.4.70 Die wechselseitige Abhängigkeit der Evaluatoraufgaben wird im obigen Abschnitt *Generischer Evaluationsarbeitsplan* (*EWP*) ausführlicher behandelt.

4.4.71 Sobald eine Evaluation endgültig abgeschlossen ist, steht das Ergebnis für den EVG als Ganzes fest. Um dies zu erreichen, sind alle auf 'nichtbeurteilend' lautenden Entscheidungen endgültig zu klären (und durch eine akzeptierende oder ablehnende Entscheidung zu ersetzen).

4.4.72 Es kann sein, daß ein EVG die Korrektheitskriterien nicht erfüllt, aber dennoch für eine niedrigere Evaluationsstufe geeignet ist, sofern diese Stufe nicht die Kriterien beinhaltet, die der EVG nicht erfüllt hat. In diesem Fall kann die Zuweisung einer niedrigeren Evaluationsstufe empfohlen werden. Wenn ein EVG die angestrebte Stärke der Mechanismen nicht erfüllt, kann unter Umständen eine geringere Stärke der Mechanismen zugestanden werden. **Wenn der EVG einen anderen Wirksamkeitsaspekt nicht erfüllt, müssen die Evaluatoren eine ablehnende Entscheidung treffen.**

4.4.73 Der Entwickler kann sich bereit erklären, einen abgelehnten EVG oder abgelehnte Evaluationsbeiträge, einschließlich der Sicherheitsvorgaben, zu ändern. Wenn die Änderungen ausreichend sind, kann die ablehnende Entscheidung aufgehoben werden.

Kapitel 4.5 Evaluationstechniken und Evaluationswerkzeuge

Zielsetzung dieses Abschnitts

4.5.1 Die technische Gleichwertigkeit von Evaluationsergebnissen wird durch Verwendung von Standardverfahren, einschließlich einer geeigneten Evaluationstechnik, unterstützt. Dies setzt voraus, daß geeignete Techniken und Werkzeuge eingesetzt werden.

4.5.2 Während des Evaluationsprozesses können die Evaluatoren Evaluationstechniken und Evaluationswerkzeuge verwenden, um den EWP mit einem optimalen Kosten/Leistungs-Verhältnis und in der kürzestmöglichen Zeit zu realisieren. Die Verwendung solcher Techniken und Werkzeuge trägt zur **Objektivität**, Wiederholbarkeit und **Reproduzierbarkeit** bei. Teil 6, Anhang 6.E enthält allgemeine Hinweise für Ersteller von Evaluationswerkzeugen.

4.5.3 Zweck dieses Abschnitts ist es, sowohl grundlegende Techniken wie etwa die Überprüfung von Dokumenten und ihre Umsetzung als auch die Techniken und Werkzeuge zu beschreiben, die zu ihrer Unterstützung eingesetzt werden können.

4.5.4 Zu den Zielsetzungen dieses Abschnitts gehören folgende:

a) auf die grundlegenden Evaluationstechniken einzugehen;

b) Fragen bezüglich Auswahl und Einsatz von Werkzeugen für die Evaluation zu diskutieren;

c) unterschiedliche Kategorien von Techniken und Werkzeugen aufzuzeigen und zu beschreiben und etwas zu der möglichen Relevanz dieser Kategorien für die Evaluationsaktivitäten zu sagen.

4.5.5 Es gehört nicht zu den Aufgaben des ITSEM, bestimmte Techniken und Werkzeuge zu empfehlen; für diese kommen unter Umständen nationale Normen zur Anwendung, und das Angebot an geeigneten Techniken und Werkzeugen nimmt ständig weiter zu. Dennoch wurde dieser Abschnitt als Beitrag zur Verwirklichung des angestrebten Ziels der technischen Gleichwertigkeit der Evaluationsergebnisse aufgenommen.

4.5.6 Es werden keine spezifischen Beispiele für Techniken und Werkzeuge vorgeschrieben, da unter allen Umständen der Eindruck vermieden werden soll, es würden bestimmte Produkte empfohlen.

Grundlegende Evaluationstechniken

Allgemeines

4.5.7 Dieser Abschnitt befaßt sich mit den für Evaluationen verwendeten grundlegenden Techniken. Diese eignen sich für eine Vielzahl von Evaluationsstufen und EVG.

Informelle Prüfung

4.5.8 Die grundlegendste Evaluationstechnik ist die informelle Prüfung von Dokumenten.

4.5.9 Diese Technik kann für alle ITSEC-Evaluatoraufgaben *überprüfen* und *suchen* verwendet werden. Bei informellen oder nicht maschinenlesbaren Darstellungen gibt es kaum Alternativen für diese Methode. Sie weist gewisse Risiken auf, denen durch Befolgung der nachfolgenden empfohlenen Leitlinien begegnet werden kann:

a) Informelle Prüfungen eignen sich nicht für eine einzige Person, die über längere Zeit allein arbeitet, da die Qualität der Ergebnisse abnimmt. Soweit möglich, sollen zwei Evaluatoren die Arbeit gemeinsam durchführen.

b) **Evaluatoren, die informelle Prüfungen durchführen, müssen ausreichende dokumentarische Nachweise (z.B. Zwischenergebnisse) erbringen, damit eine Bewertung ihrer Arbeit möglich ist.**

Rückführbarkeitsanalyse

4.5.10 Eine etwas formellere Technik ist die Rückführbarkeitsanalyse. Sie wird verwendet, um zwei Darstellungen auf ihre Konsistenz zu überprüfen. Sie umfaßt folgende Schritte:

a) Für jede Komponente der höheren Darstellung ist zu überprüfen (wenn möglich mit Hilfe des Abbildbarkeitsnachweises des Entwicklers), ob sie in der niedrigeren Darstellung korrekt implementiert ist.

b) Für jede Komponente in der niedrigeren Darstellung ist zu überprüfen, ob ihr Vorhandensein durch die höhere Darstellung gerechtfertigt wird.

4.5.11 Auch hier werden die Arbeiten weitgehend manuell durchgeführt, wobei die oben angeführten Leitlinien zur Anwendung kommen. In einigen Fällen kann eine Datenbank oder ein Hypertextsystem zur Verfolgung der Übereinstimmung zwischen den Darstellungen von Nutzen sein.

4.5.12 **Die Evaluatoren müssen in der Lage sein nachzuweisen, daß sie alle relevanten Teile des EVG bei ihrer Analyse berücksichtigt haben.**

Abbildbarkeitsanalyse

4.5.13 Die Abbildbarkeitsanalyse ist eines der grundlegenden Prinzipien der Evaluation. Sie wird zur Beschreibung des Begriffs der korrekten Verfeinerung der sicherheitsspezifischen Funktionen innerhalb der Darstellungen des EVG bis zu seiner endgültigen Ausgestaltung in Form eines ausführbaren Codes und elektronischer Schaltungen verwendet.

4.5.14 Das Vertrauen in den EVG wird von den Evaluatoren dadurch aufgebaut, daß sie überprüfen, ob die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben im Architekturentwurf, im Feinentwurf, bei der Implementierung und beim Betrieb des EVG durchgängig korrekt verfeinert sind. Das Vertrauen nimmt daher in dem Maße zu, wie weitere Darstellungen eines EVG auf ihre Abbildbarkeit hin überprüft werden (daher nimmt die Anzahl der Darstellungen und ihr Detaillierungsgrad mit der Höhe der Evaluationsstufe zu).

4.5.15 Daher besteht eine grundlegende Evaluationstechnik darin, jede einzelne sicherheitsspezifische Funktion durch die verschiedenen Darstellungen des EVG bis zum Betrieb des EVG zu verfolgen.

4.5.16 Dies wurde im Abschnitt *Generischer Evaluationsarbeitsplan* (*EWP*) weiter oben durch die vielen Zwischenergebnisse angedeutet, die sich auf die Abbildbarkeit beziehen.

Der Reviewprozeß

4.5.17 Der Evaluationsprozeß erfordert einen erheblichen Aufwand an informeller Analysearbeit. Wichtig ist, daß nachgewiesen werden kann, daß solche Analysen objektiv durchgeführt worden sind. Eine Möglichkeit, dies zu tun, besteht darin, die Arbeit jedes einzelnen Evaluators durch andere überprüfen zu lassen. Dadurch wird das subjektive Element in den Ergebnissen so gering wie möglich gehalten. Der im folgenden beschriebene *Reviewprozeß* ist eine mögliche Vorgehensweise für diese Überprüfung, auch wenn unter Umständen eine formelle Besprechung nicht erforderlich ist.

4.5.18 **Alle Evaluationsergebnisse (siehe Kapitel 4.7) müssen einem Review unterzogen werden.**

4.5.19 Am Reviewprozeß sollen zumindest die Personen beteiligt sein, die folgende Rollen übernommen haben:

a) der Projektleiter, der für die technische Durchführung der Evaluation verantwortlich ist;

b) der Autor, der/die Evaluator(en), der/die die Analyse durchgeführt haben;

c) der Moderator, der als unabhängiger Dritter dafür zu sorgen hat, daß der Review ordnungsgemäß durchgeführt wird.

4.5.20 Weitere Personen können ebenfalls herangezogen werden, z.B. technische Spezialisten, Vertreter der Zertifizierungsstelle, weitere Evaluatoren (insbesondere wenn Autor und Projektleiter ein und dieselbe Person sind).

4.5.21 Der Reviewprozeß durchläuft eine Reihe von Phasen:

a) Wenn ein Evaluationsergebnis fertiggestellt ist, wird vom Projektleiter für einen allen Beteiligten zusagenden Termin eine Reviewsitzung anberaumt. Der Termin für die Sitzung soll so gewählt werden, daß alle Teilnehmer Zeit für eine sorgfältige Prüfung des Evaluationsergebnisses haben.

b) Vor der Sitzung begutachten die Teilnehmer das Ergebnis und überprüfen es auf Fehler.

c) Während der Sitzung diskutieren die Teilnehmer über das Ergebnis und eventuell festgestellte Fehler. Sie prüfen, ob Änderungen erforderlich sind. Im allgemeinen sollen die Sitzungsteilnehmer in erster Linie entscheiden, ob Änderungen erforderlich sind, und nicht, wie diese Änderungen aussehen sollen.

d) Am Ende der Sitzung entscheiden die Teilnehmer, ob das Ergebnis in der vorgelegten Form annehmbar ist, ob nur geringfügige Änderungen erforderlich sind oder ob umfangreichere Änderungen erforderlich sind, die in einer weiteren Reviewsitzung geprüft werden müssen.

e) Die Entscheidung wird protokolliert. Wird unter den Teilnehmern keine Einstimmigkeit erzielt, gilt die Entscheidung des Projektleiters. Abweichende Meinungen sind jedoch zu Protokoll zu nehmen.

Umsetzung

4.5.22 Unter Umsetzung oder Modellierung ist die Übertragung einer Darstellung in eine andere Notation zu verstehen. Beispielsweise kann ein Z-Schema in Prolog umgesetzt werden, damit für die Evaluatoren sämtliche Feinheiten der ursprünglichen Darstellung verständlich werden. In vielen Fällen ist der eigentliche Umsetzvorgang für die Evaluatoren vom Verständnis her genau so nützlich wie das Endprodukt.

Versagensanalyse

4.5.23 Ein EVG, dessen Sicherheitsvorgaben Verfügbarkeitsanforderungen enthalten, ist einer Reihe von Bedrohungen ausgesetzt, die sich auf Fehler des EVG beziehen. Bei diesen Bedrohungen kann es sich entweder um böswillige, auf die Verringerung der Verfügbarkeit ausgerichtete Versuche von außen handeln oder aber um unbeabsichtigte Bedrohungen von innen, die aus Fehlern des EVG selbst resultieren.

4.5.24 Externe Bedrohungen der Verfügbarkeit können bei der Wirksamkeitsbewertung in der gleichen Weise berücksichtigt werden wie externe Bedrohungen der Vertraulichkeit oder Integrität. Diese Analysen beschäftigen sich mit der Sicherheitsfunktionalität, die zur Abwehr eines außerhalb des EVG gestarteten Angriffs bereitgestellt wird.

4.5.25 Interne Ursachen von Verfügbarkeitsverlusten müssen mittels einer Technik bewertet werden, die die Fehlerarten des EVG analysiert. Eine solche Technik ist die Failure Mode and Effects Analysis (FMEA), die bei Zuverlässigkeitsprüfungen zur Ermittlung der Zuverlässigkeit von Geräten und Systemen verwendet wird. Die FMEA-Technik wird in einer US-Militärnorm [MS1629A] eingehend beschrieben.

4.5.26 Die FMEA-Technik stellt eine standardisierte Technik zur Betrachtung aller Fehlerarten des EVG und deren Auswirkung auf die Verfügbarkeit des EVG dar, wobei im EVG getroffene Kompensationsmaßnahmen, die den Fehlerauswirkungen entgegenwirken sollen, berücksichtigt werden.

4.5.27 Die Analyse zeigt für jede betrachtete Komponente folgendes auf:

a) Funktion;

b) Fehlerarten und -ursachen;

c) Fehlerauswirkungen für jede Darstellung;

d) Fehlererkennungsmethode;

e) Kompensationsmaßnahmen;

f) resultierender Schweregrad.

4.5.28 Diese Technik kann von Evaluatoren zur Bewertung der Frage herangezogen werden, ob im EVG angemessene Vorkehrungen getroffen worden sind, um den durch eigene Fehler verursachten Bedrohungen der Verfügbarkeit begegnen zu können.

Durchführung der Evaluatoraktivitäten

Allgemeines

4.5.29 In Abbildung 4.4.1 sind alle Aktivitäten aufgeführt, die von den Evaluatoren durchzuführen sind. Im folgenden werden diese Aktivitäten beschrieben und geeignete Techniken vorgeschlagen. Es werden jedoch nicht alle Evaluatoraufgaben im Detail abgedeckt.

Analyse der Eignung überprüfen

4.5.30 Die für diese Aktivität hauptsächlich verwendete Technik ist die informelle Prüfung.

Analyse des Zusammenwirkens überprüfen

4.5.31 Die für diese Aktivität hauptsächlich verwendete Technik ist die informelle Prüfung.

4.5.32 Es kann sich die Notwendigkeit ergeben, nach verdeckten Kanälen im EVG zu suchen, auch wenn diese in den Sicherheitsvorgaben nicht erwähnt sind. Die meisten Techniken für die Analyse verdeckter Kanäle basieren auf der Shared Resource Matrix Method [SRMM]. Eventuell erweisen sich Quellcode-Analysewerkzeuge und Matrixmanipulationswerkzeuge für die Evaluatoren bei Anwendung dieser Methode auf einen EVG als nützlich.

Konstruktionsschwachstellen untersuchen

4.5.33 Die zur Überprüfung der Analyse des Entwicklers hauptsächlich verwendete Technik ist die informelle Prüfung.

4.5.34 **Von den Evaluatoren wird auch die Durchführung einer eigenen Analyse ausgehend von den bei der Evaluation erkannten Schwachstellen verlangt. Dies bedeutet, daß die Evaluatoren ein Verzeichnis der bei der Evaluation festgestellten Mängel führen müssen. Dazu gehören zwingend Mängelberichte sowie weniger formale Berichte über kleinere Korrektheitsfehler.**

4.5.35 Bei der von den Evaluatoren durchgeführten Analyse sollen folgende generische Methoden berücksichtigt werden, die zur Ausnutzung einer Schwachstelle herangezogen werden könnten:

a) Ändern der vordefinierten Abfolge des Aufrufens von Komponenten;

b) Ausführen einer zusätzlichen Komponente;

c) Verwenden von Interrupts oder Steuerungsfunktionen zur Unterbrechung der Abfolge;

d) Direktes oder indirektes Lesen, Schreiben oder Modifizieren interner Daten;

e) Ausführen von Daten, deren Ausführung nicht vorgesehen ist, oder Ausführbarmachen dieser Daten;

f) Verwenden einer Komponente in einem unerwarteten Kontext oder für einen unerwarteten Zweck;

g) Erzeugen einer unerwarteten Eingabe für eine Komponente;

h) Aktivieren der Fehlerüberbrückung;

i) Verwenden von in feinere Darstellungen eingebrachten Implementierungsdetails;

j) Aufbrechen von Überlagerungen;

k) Verwenden von Interferenzen zwischen Komponenten, die auf einer höheren Abstraktionsstufe nicht sichtbar sind;

l) Ungültigmachen von Annahmen und Eigenschaften, auf denen Komponenten einer niedrigeren Stufe beruhen;

m) Nutzen der Verzögerung zwischen dem Zeitpunkt der Überprüfung und dem Zeitpunkt der Verwendung.

4.5.36 Die auf die Korrektheit des *Betriebs* bezogenen Evaluatoraufgaben können sowohl Konstruktionsschwachstellen als auch operationelle Schwachstellen aufzeigen. Beispielsweise kann die Betrachtung der in der Benutzerdokumentation beschriebenen Anwenderbefehle ergeben, daß das Ziel der Gegenmaßnahme nicht erreicht wird, wenn die Befehle in einer unerwarteten Reihenfolge erteilt werden. Bei der Schwachstelle handelt es sich um eine Konstruktionsschwachstelle und nicht um eine operationelle Schwachstelle, da sie von Eigenschaften des EVG Gebrauch macht, die während dessen Konstruktion eingeführt wurden.

Stärke der Mechanismen untersuchen

4.5.37 Diese Aktivität wird hauptsächlich in Form einer informellen Prüfung durchgeführt.

4.5.38 Kryptographische Mechanismen werden von den ITSEFs nicht bewertet (siehe ITSEC, Absatz 3.23).

4.5.39 Teil 6, Anhang 6.C befaßt sich mit der Stärke der Mechanismen.

Benutzerfreundlichkeit untersuchen

4.5.40 Diese Aktivität wird hauptsächlich in Form einer informellen Prüfung durchgeführt.

4.5.41 Die Evaluatoren müssen *jede Konfigurationsprozedur nachvollziehen, um zu überprüfen, ob der EVG sicher konfiguriert und benutzt werden kann, wobei nur die Dokumentation für den Anwender und den Systemverwalter als Grundlage zu benutzen ist.* Dies setzt voraus, daß sie Zugang zu dem EVG haben.

4.5.42 Bei einem Produkt dürfte dies wohl kaum ein Problem sein. Bei der Evaluation eines Systems kann dies schwierig sein, da der EVG möglicherweise bereits konfiguriert und installiert ist und die Evaluatoren eventuell keine Möglichkeit haben, den Prozeß nachzuvollziehen. In diesem Fall muß unterschieden werden zwischen

a) den Teilschritten der Installation und Konfiguration, die nur einmal vorgenommen werden. Bei diesen sollte eine Überprüfung der Frage, ob Konfiguration und Installation des EVG korrekt vorgenommen wurden, eigentlich ausreichen. **Wenn solche Teile eines EVG neu installiert oder neu konfiguriert werden, muß eine Reevaluation des EVG erfolgen.**

b) den Teilschritten der Installation und Konfiguration, die später geändert werden können. **Bei diesen müssen die Evaluatoren die Installations- und Konfigurationsprozeduren nachvollziehen.** Diese Teile brauchen jedoch nicht einer Reevaluation unterzogen werden, wenn sie neu installiert oder neu konfiguriert werden.

4.5.43 Die Evaluatoren müssen, *wo erforderlich, zusätzliche Tests durchführen, um die Analyse der Benutzerfreundlichkeit zu bestätigen oder zu widerlegen.* Diese können im Rahmen der Penetrationstestaktivität durchgeführt werden.

Operationelle Schwachstellen untersuchen

4.5.44 Diese Aktivität wird unter Verwendung ähnlicher Techniken durchgeführt wie bei der Aktivität *Konstruktionsschwachstellen überprüfen.*

Die Anforderungen überprüfen

4.5.45 Diese Aktivität wird hauptsächlich in Form einer informellen Prüfung der Sicherheitsvorgaben durchgeführt.

4.5.46 Auf höheren Evaluationsstufen können die Evaluatoren zur Prüfung komplexer Teile der Sicherheitsvorgaben Umsetzungswerkzeuge (Animation Tools) verwenden.

4.5.47 Bei der Bewertung der Angemessenheit formaler Beschreibungen ab Stufe E4 sollen die Evaluatoren folgende Fragen betrachten:

a) Erfolgt die formale Beschreibung auf einem akzeptierbaren Abstraktionsniveau, d.h., ist es z.B. akzeptierbar, ein Hardware-Gatter mit den Mitteln klassischer Logik (bei der die Ausgabe des Gatters entweder 0 oder 1 sein kann) zu beschreiben anstatt mit ternärer Logik (bei der die Ausgabe des Gatters entweder 0, 1 oder unbestimmt sein kann)?

b) Ist die formale Beschreibung in einer geeigneten Notation ausgedrückt, d.h., ist es z.B. akzeptierbar, zur Beschreibung eines EVG, der aus einer Reihe simultaner, wechselwirkender Prozesse besteht, etwa Z statt CSP zu verwenden?

c) Ist die Auslassung von Teilen der Sicherheitsvorgaben in der formalen Beschreibung gerechtfertigt, z.B. aufgrund der Tatsache, daß diese mit dem aktuellen Stand der Technik für formale Methoden nicht bearbeitet werden können?

4.5.48 Die Sicherheitsvorgaben werden in Teil 6, Anhang 6.B behandelt.

4.5.49 **Wenn der Antragsteller Informationen zur Reevaluation in Kapitel 7 des ETR verlangt, müssen die Evaluatoren die notwendigen Informationen während dieser Aktivität sammeln.**

Den Architekturentwurf überprüfen

4.5.50 Die für diese Aktivität hauptsächlich verwendeten Techniken sind die informelle Prüfung oder die informelle Rückführbarkeitsanalyse. Auf höheren Evaluationsstufen (d.h. ab E4) bietet sich eventuell die Modellierung an.

4.5.51 Auf der Evaluationsstufe E6 wird vom Entwickler der Nachweis der Konsistenz zwischen dem formalen Architekturentwurf und dem formalen Modell der Sicherheitspolitik verlangt. Dies kann durch eine informelle Prüfung evaluiert werden, oder es können automatisierte Proof-Checking-Tools verwendet werden.

4.5.52 **Wenn der Antragsteller Informationen zur Reevaluation in Kapitel 7 des ETR verlangt, müssen die Evaluatoren die notwendigen Informationen während dieser Aktivität sammeln.**

4.5.53 **Wenn nach den Kriterien Beschreibungen in semiformaler oder formaler Notation verlangt werden, müssen die Evaluatoren überprüfen, ob die verwendeten Notationen und die Art ihrer Verwendung angemessen sind. Dazu müssen sie die Notation mit den Anforderungen in den ITSEC-Absätzen 2.65 bis 2.80 (Spezifikationsformen) vergleichen.**

4.5.54 Beispielsweise können die Evaluatoren bei der Überprüfung der Frage, ob die Notation als formale Notation akzeptiert werden kann, folgendes berücksichtigen:

a) Entspricht die Notation einer anerkannten Norm oder ist sie anderweitig wissenschaftlich anerkannt (z.B. Z, CSP, VDM und HOL)?

b) Ist die Notation ansonsten für die Zertifizierungsstelle akzeptierbar?

c) Kann der Antragsteller nachweisen, daß die Notation über eine klar definierte Syntax und Semantik verfügt?

4.5.55 **Die Evaluatoren müssen nachprüfen, ob die zum Darstellen des Architekturentwurfs verwendete Sprache die Möglichkeit bietet, sicherheitsrelevante Merkmale auszudrücken.**

4.5.56 Beispielsweise sind sowohl Datenmodelle als auch Datenflußdiagramme als semiformale Notationen geeignet. Eine einzelne Notation wie etwa ein Datenmodell oder Datenflußdiagramm ist jedoch unter Umständen nicht in der Lage, alle Facetten der Architektur des EVG auszudrücken. In einem solchen Fall könnte der Antragsteller mehrere Notationen verwenden, die zusammengenommen ein vollständiges Bild der Architektur vermitteln.

Den Feinentwurf überprüfen

4.5.57 Die für diese Aktivität hauptsächlich verwendeten Techniken sind die informelle Prüfung und die informelle Rückführbarkeitsanalyse.

4.5.58 **Wenn den Evaluatoren eine semiformale Beschreibung des Entwurfs geliefert wird, müssen sie überprüfen, ob die Beschreibung dem von den ITSEC geforderten Formalisierungsgrad entspricht.** Zu den akzeptierbaren semiformalen Darstellungsformen gehören graphische Darstellungen (z.B. Datenflußdiagramme, Prozeßstrukturdiagramme) oder eine klar definierte, begrenzte Verwendung der Umgangssprache (siehe ITSEC, Absätze 2.72 bis 2.75).

4.5.59 Wird den Evaluatoren beispielsweise eine Program Description Language (PDL) vorgelegt, dann könnten sie gewährleisten, daß der Entwickler über eine definierte Menge von PDL-Normen verfügt, die die Syntax und Semantik der PDL-Konstrukte klar definieren.

4.5.60 Wenn ein Entwickler Computer Aided Software Engineering (CASE)-Werkzeuge verwendet, sollen die Evaluatoren bestätigen, daß die zugrundeliegende Methode, die von dem Werkzeug eingebracht wird, akzeptierbar ist und den Qualitätsstandards des Entwicklers entspricht.

4.5.61 Für die Evaluationsstufen ab E5 verlangen die ITSEC, daß *[der EVG] ... weitgehend die Konzepte der hierarchischen Dekomposition, der Abstraktion und der Datenabschottung anwenden muß*. Diese Techniken sind im sicherheitskritischen Bereich [ISO65A] wohlbekannt und sollen zur Verständlichkeit und Pflege des Entwurfs beitragen. Man beachte, daß aufgrund der Tatsache, daß diese Techniken zwar weitgehend, aber nicht allumfassend anzuwenden sind, ihre Nichtanwendung im Einzelfall nicht zwangsläufig zu einer ablehnenden Entscheidung der Evaluatoren führen muß. **Vielmehr müssen die Evaluatoren prüfen, ob der EVG-Entwurf nach ihrer Ansicht verständlich ist.** Wenn nicht, sind die Konzepte der hierarchischen Dekomposition, Abstraktion und Datenabschottung wahrscheinlich nicht sachgerecht angewendet worden.

4.5.62 **Schnittstellenspezifikationen müssen durch Überkreuzprüfung mit den übrigen Spezifikationen sicherheitsspezifischer und sicherheitsrelevanter Funktionalität auf Vollständigkeit und Wirk-samkeit überprüft werden.**

4.5.63 **Globale Variablen, die auf Stufe E5 und E6 identifiziert werden, müssen als eine Art Schnittstelle betrachtet werden. Die Evaluatoren müssen sicherstellen, daß diese nur einmal definiert werden, und daß die Verwendung jeder globalen Variablen durch eine Funktionseinheit gerechtfertigt und mit der Definition der globalen Variable vereinbar ist.** Es muß eine Checkliste erstellt werden, wobei die im Feinentwurf identifizierten globalen Variablen auf die Benutzung durch Funktionseinheiten abgebildet werden.

4.5.64 **Wenn der Antragsteller Informationen zur Reevaluation in Kapitel 7 des ETR verlangt, müssen die Evaluatoren die notwendigen Informationen während dieser Aktivität sammeln.**

Die Implementierung überprüfen

4.5.65 Obwohl bei dieser Aktivität die Wahrscheinlichkeit, daß sie vom Einsatz automatisierter Werkzeuge profitiert, größer sein dürfte als bei jeder anderen, können die informelle Prüfung und die Rückführbarkeitsanalyse weiterhin verwendet werden.

4.5.66 Wenn die Implementierung einen Quellcode einschließt, können Werkzeuge zur statischen Quellcodeanalyse verwendet werden, um die Codequalität zu bewerten und nach bestimmten Arten von Schwachstellen zu suchen. Wenn die Implementierung Hardware-Konstruktionszeichnungen umfaßt, können die CAD-Werkzeuge des Entwicklers bei der Analyse von Nutzen sein.

4.5.67 Die Evaluatoren müssen *die Bibliothek der Testprogramme für eine stichprobenweise Überprüfung der Testergebnisse heranziehen.* Dies ist eine von zwei Evaluatoraufgaben, bei denen Stichproben zugelassen sind. **Die folgenden Grundregeln sind bei der Auswahl einer Stichprobe zu befolgen:**

a) **Die Stichprobe muß eine Auswahl von Tests enthalten, die eine Vielzahl von Komponenten, sicherheitsspezifischen und sicherheitsrelevanten Funktionen, Entwicklungs-orten (falls mehr als einer vorhanden ist) und Hardware-Plattformtypen (falls mehr als einer vorhanden ist) abdecken**.

b) **Antragsteller und Entwickler dürfen nicht im voraus über die Stichprobe informiert werden**.

c) **Die Größe der Stichprobe muß für die Zertifizierungsstelle akzeptierbar sein**. Damit die Evaluationskosten vorausberechenbar sind, kann vor Beginn der Evaluation eine Stichprobengröße vereinbart werden.

4.5.68 **Wenn Stichprobenprüfungen durchgeführt werden, muß eine Begründung gegeben und die verwendete Stichprobe aufgezeichnet werden.**

4.5.69 Diese Aufgabe kann den Einsatz der Entwicklungssysteme erfordern. Dies soll beim Abschluß des Vertrags mit dem Antragsteller berücksichtigt werden.

4.5.70 Die Evaluatoren müssen (ab E2) *überprüfen, ob die Tests alle sicherheitsspezifischen Funktionen, die in den Sicherheitsvorgaben angegeben sind, umfassen*. **Als Mindestanforderung müssen die Evaluatoren überprüfen, ob für jede prüfbare Aussage in den Sicherheitsvorgaben mindestens ein Test zum Nachweis der Aussage definiert worden ist.** Die Begründung des Entwicklers (ab Evaluationsstufe E4 gefordert), *warum die gewählte Testabdeckung ausreicht*, kann nützliche Informationen darüber liefern.

4.5.71 Die Evaluatoren müssen (ab E3) *überprüfen, ob die Tests alle im Feinentwurf identifizierten sicherheitsspezifischen und sicherheitsrelevanten Funktionen sowie alle im Quellcode bzw. in den Hardware-Konstruktionszeichnungen identifizierten Sicherheitsmechanismen umfassen.* **Beim Feinentwurf müssen die Evaluatoren überprüfen, ob alle Schnittstellen zu allen sicherheitsspezifischen oder sicherheitsrelevanten Basiskomponenten in einem Test verwendet wurden.** Die Evaluatoren können dies anhand der vom Entwickler erklärten *Übereinstimmung zwischen den Tests und den sicherheitsspezifischen und sicherheitsrelevanten Funktionen, die im Feinentwurf definiert sind*, überprüfen.

4.5.72 Eine angemessene Abdeckung des Quellcodes ist erreicht, wenn der Antragsteller folgendes nachweisen kann:

a) bei E3: alle Anweisungen des sicherheitsspezifischen Quellcodes wurden getestet;

b) ab E4: alle Anweisungen und Verzweigungen des gesamten Quellcodes, der zu einer sicherheitsspezifischen oder sicherheitsrelevanten Basiskomponente gehört, sind getestet worden.

4.5.73 *Quellcodeabdeckung:* In diesem Kasten wird das Testen von Anweisungen und Verzweigungen erläutert. Um jede Quellcodeanweisung eines sequentiellen Programms testen zu können, muß der Entwickler jede Quellcodeanweisung im Programm mindestens einmal ausführen. Um jede Anweisung und Verzweigung testen zu können, muß der Entwickler jede Quellcodeanweisung im Programm mindestens einmal ausführen und jedes Flußkontrollkonstrukt auf alle möglichen Arten ausführen.

4.5.74 Die Bedeutung dieser Anforderungen wird am besten anhand eines Beispiels erläutert. Nehmen wir das folgende Programmsegment:

```
if a
then B;
else C:
endif;

if d
then E;
endif;
```

4.5.75 Um jede Anweisung dieses Programms zu testen, muß der Entwickler die Anweisungen *B, C* und *E* ausführen, etwa durch Ausführen des Programms mit den wahren Bedingungen *a* und *d* (führt B und E aus) und anschließend mit der falschen Bedingung *a* und der wahren Bedingung *d* (führt C und E aus).

4.5.76 Um alle Anweisungen und Verzweigungen dieses Programms zu testen, muß der Entwickler die Anweisungen *B, C* und *E* wie zuvor ausführen, er muß aber auch den Fall abdecken, bei dem *E* ausgelassen wird. Dies könnte durch Ausführung des Programms mit den wahren Bedingungen *a* und *d* (führt B und E aus) und anschließend mit den falschen Bedingungen *a* und *d* (führt nur C aus) erreicht werden.

4.5.77 Die Testabdeckung der Hardware-Konstruktionszeichnungen ist ein Sonderfall, der unter das nationale Regelwerk fällt.

4.5.78 Die Evaluatoren können die *Übereinstimmung zwischen den Tests und den sicherheitsspezifischen und sicherheitsrelevanten Funktionen im Feinentwurf* und die *Übereinstimmung zwischen den Tests und den Sicherheitsmechanismen, wie sie im Quellcode bzw. in den Hardware-Konstruktionszeichnungen dargestellt sind*, als Hilfsmittel zur Überprüfung der Vollständigkeit verwenden.

4.5.79 Bestimmte Compiler bieten Möglichkeiten für die Überwachung von Quellcodezeilen bei der Ausführung von Tests. Diese Möglichkeiten können von Entwicklern zur Feststellung von Übereinstimmungen der Tests verwendet werden. Die Evaluatoren können sie zur Überprüfung der Testabdeckung verwenden, sofern sie Vertrauen in die Unverfälschtheit dieser Möglichkeiten haben.

4.5.80 Die Evaluatoren müssen *alle erneut durchgeführten Tests nach der Korrektur von Fehlern überprüfen*. Es sind also Regressionstests angesprochen, d.h. erneute Tests nach der Korrektur von Fehlern, die von Evaluatoren oder Entwicklern festgestellt worden sind.

4.5.81 In diesem Fall wird von dem Grundsatz ausgegangen, daß die vorgenommenen Korrekturen mit dem Feinentwurf vereinbar sein sollen. Wird der EVG nach Entdeckung eines Fehlers verändert, sollen die geänderten Komponenten erneut getestet werden. Darüber hinaus soll als Beweis dafür, daß keine Folgefehler eingebracht worden sind, ein gewisser Teil der Systemtests wiederholt werden.

4.5.82 **Die Evaluatoren müssen die Aussagen des Entwicklers in bezug auf Regressionstests im Testplan überprüfen, um sicherzustellen, daß angemessene Wiederholungstests durchgeführt werden. Die Evaluatoren müssen sicherstellen, daß die Regressionstestpolitik befolgt wird.**

4.5.83 Die Evaluatoren müssen *zusätzliche Tests durchführen, um Fehler zu suchen.* **Die Evaluatoren müssen daher für jede sicherheitsspezifische Funktion mindestens einen zusätzlichen Test durchführen; der Test muß sich von dem vom Antragsteller durchgeführten Test unterscheiden. Wo dies nicht durchführbar ist, muß eine Begründung für jede Einschränkung der Tests gegeben werden.** Auf Stufe E1 und E2 erfolgen die Tests auf der Ebene der Sicherheitsvorgaben.

4.5.84 **Zusätzlich muß auf Stufe E3 bis E6 ein zusätzlicher Test für jede sicherheitsspezifische und sicherheitsrelevante Funktion durchgeführt werden; der Test muß sich von dem vom Antragsteller durchgeführten Test unterscheiden. Wo dies nicht durchführbar ist, muß eine Begründung für jede Einschränkung der Tests gegeben werden.** Die Tests werden auf der Ebene des Feinentwurfs und des Quellcodes durchgeführt.

4.5.85 Die Evaluatoren können bei der Durchführung solcher zusätzlichen Tests diese skizzieren und dann die Unterstützung des Antragstellers bei der Testdurchführung in Anspruch nehmen. **In diesem Fall müssen die Evaluatoren bei der Durchführung der Tests zugegen sein.** Wahlweise können die Evaluatoren beschließen, diese Funktionstests im Rahmen der Penetrationstests durchzuführen (siehe unten).

4.5.86 **Die Evaluatoren müssen auch nachprüfen, daß die tatsächlich erzielten Testergebnisse den erwarteten Ergebnissen entsprechen.**

4.5.87 **Wenn der Antragsteller Informationen zur Reevaluation in Kapitel 7 des ETR verlangt, müssen die Evaluatoren die notwendigen Informationen während dieser Aktivität sammeln.**

Die Entwicklungsumgebung überprüfen

4.5.88 Die Evaluatoren sollen die Dokumentation der Entwicklungsumgebung informell untersuchen.

4.5.89 Ab E2 müssen die Evaluatoren *überprüfen, ob die dokumentierten Verfahren angewendet werden*. Dazu wird empfohlen, dem Entwicklungsstandort einen oder mehrere Besuche abzustatten. Zweck dieser Besuche ist,

a) sich einen besseren Einblick in den Entwicklungsprozeß durch Begutachtung im praktischen Einsatz zu verschaffen;

b) nachzuprüfen, daß die dokumentierten Vorgehensweisen in der Praxis angewendet werden.

4.5.90 Der Besuch ist mit dem Entwickler abzustimmen. Vor dem Besuch sollen die Evaluatoren eine Checkliste der Themen vorbereiten, die sie besprechen möchten. Diese kann dem Entwickler ausgehändigt werden, damit er sich auf den Besuch entsprechend vorbereiten kann.

4.5.91 Während des Besuchs sollen die Evaluatoren das Entwicklungspersonal befragen und die Vorgehensweise bei der Konfigurationskontrolle und die Sicherheitspraktiken protokollieren.

4.5.92 Die Evaluatoren müssen (ab E4) *ausgewählte Teile des EVG unter Verwendung der Werkzeuge des Entwicklers neu erstellen und die Ergebnisse mit dem vorliegenden EVG vergleichen.* Dies ist eine von zwei Evaluatoraufgaben, bei denen Stichprobenuntersuchungen zugelassen sind.

4.5.93 **Die Evaluatoren müssen jeden Erstellungsprozeß verwenden.** Wenn der Erstellungsprozeß einheitlich ist (alle Komponenten werden auf die gleiche Weise erstellt), braucht nur eine Komponente neu erstellt zu werden. **Wenn alle Komponenten unterschiedlich erstellt werden, müssen die Evaluatoren jede Komponente neu erstellen.** Es ist nicht anzunehmen, daß die Evaluatoren in der Lage sein werden, Hardware-Komponenten zu erstellen. **Im Falle von Hardware-Komponenten müssen die Evaluatoren bei der Herstellung solcher Komponenten am Entwicklungsort zugegen sein.**

4.5.94 Unter Umständen müssen die Evaluatoren das Entwicklungssystem verwenden, um diese ITSEC-Aufgabe durchzuführen. Dies soll im Vertrag mit dem Antragsteller berücksichtigt werden.

4.5.95 Werkzeuge zum Dateivergleich können zur Gegenüberstellung der neu erstellten Komponente und des Originals verwendet werden. Es ist zu beachten, daß wenn beim Erstellungsprozeß die Komponente mit einem Zeitstempel versehen wird, dieser nicht mit dem Original übereinstimmt.

4.5.96 **Wenn Informationen zur Reevaluation im ETR verlangt werden, müssen die Evaluatoren diejenigen Entwicklungswerkzeuge aufzeigen, die sicherheitsrelevant sind.**

Die Betriebsdokumentation überprüfen

4.5.97 Dies geschieht durch informelle Prüfung und Reviews. Die Evaluatoren machen sich mit der Betriebsdokumentation vertraut und vergewissern sich, daß genaue Informationen vorliegen, die für eine sichere Verwendung und Konfiguration des EVG ausreichen.

Die Betriebsumgebung überprüfen

4.5.98 Dies geschieht durch informelle Prüfung. Die Evaluatoren machen sich mit der Auslieferung, der Konfiguration, dem Systemstart und der Betriebsdokumentation vertraut und vergewissern sich, daß genaue Informationen vorliegen, die für eine sichere Pflege und einen sicheren Betrieb des EVG ausreichen. Ab E2 müssen die Evaluatoren Informationen von der Zertifizierungsstelle über das geforderte *Verfahren..., mit dem die Authentizität des EVG garantiert wird,* einholen.

Penetrationstest durchführen

4.5.99 Zur Auswahl von Penetrationstests kann das folgende Verfahren nach [LINDE] angewendet werden:

a) Die Evaluatoren listen alle bei der Evaluation entdeckten Fehler, Inkonsistenzen und Schwachstellen auf;

b) die Evaluatoren weisen in der Liste diejenigen Punkte aus, die zu einer Sicherheitslücke führen könnten und wahrscheinlich durch Penetrationstests praktisch nachweisbar sind;

c) die Evaluatoren legen für die ausgewählten Punkte Prioritäten fest, so daß diejenigen, bei denen die Wahrscheinlichkeit der Testbarkeit am größten ist, zuerst an die Reihe kommen, während diejenigen, bei denen die Wahrscheinlichkeit der Testbarkeit am geringsten ist, zuletzt getestet werden.

4.5.100 **Damit die Tests nachvollziehbar sind, müssen die Evaluatoren einen Testbericht erstellen, der das Verfahren zur Durchführung jedes einzelnen Penetrationstests und die zu erwartenden Testergebnisse beschreibt.** Im nationalen Regelwerk können eigene Anforderungen für die Durchführung von Tests vorgesehen sein, die außerhalb der ITSEF (z.B. am Entwicklungsort) durchgeführt werden.

4.5.101 Die Evaluatoren sollen den Antragsteller über ihre Anforderungen in bezug auf Penetrationstests informieren. Dazu können folgende gehören:

a) ein angemessener Zugang zum EVG;

b) technische Unterstützung durch den Entwickler;

c) entsprechende Räumlichkeiten, wozu bei Bedarf auch sichere Aufbewahrungsmöglich-keiten gehören können;

d) die Verwendung von Magnetdatenträgern.

4.5.102 Penetrationstests können den EVG beeinträchtigen oder ihm Schaden zufügen. Damit solche Schäden auf ein Mindestmaß reduziert werden, sollen die Evaluatoren mit den Antragstellern Maßnahmen wie etwa die Erstellung von Sicherungskopien besprechen.

4.5.103 Zwar sollen die meisten Penetrationstests anhand definierter Berichte durchgeführt werden, jedoch sind auch Ad-hoc-Tests (d.h. Tests ohne vorbereiteten Testbericht) gestattet. **Solche Tests müssen jedoch begründet werden und so detailliert aufgezeichnet werden, daß sie nachvollziehbar sind.**

4.5.104 Penetrationstests können durch Verwendung von Sicherheitskonfigurations- und Protokollierungswerkzeuge unterstützt werden. Diese Werkzeuge untersuchen eine Systemkonfiguration und suchen nach gemeinsamen Schwachstellen wie etwa allgemeinlesbaren Dateien und fehlenden Paßwörtern.

Auswahl und Verwendung von Evaluationswerkzeugen

Einleitung

4.5.105 **Wird bei der Herbeiführung einer Evaluationsentscheidung ein automatisiertes Werkzeug verwendet, muß der ETR ausreichende Informationen über dieses Werkzeug und die Art seines Einsatzes enthalten, damit die Entscheidung nachvollzogen werden kann.**

4.5.106 **Jede Verwendung von Werkzeugen in dieser Form muß für die Zertifizierungsstelle akzeptierbar sein.** Zur Vermeidung unnötiger Arbeit wird den ITSEFs geraten, vor Verwendung der Werk-zeuge die Zustimmung der Zertifizierungsstelle einzuholen.

4.5.107 Zertifizierungsstellen können - sofern sie dies wollen - eine Liste der automatisierten Werkzeuge führen, die zur Durchführung bestimmter ITSEC-Evaluatoraufgaben herangezogen werden können.

Evaluationswerkzeuge

4.5.108 Dieser Unterabschnitt enthält Kurzbeschreibungen der verschiedenen Arten von Werkzeugen, die für die Evaluatoren unter Umständen von Nutzen sein können.

4.5.109 *Animation Tools:* Diese Werkzeuge werden im Frühstadium einer Entwicklung benutzt, um Darstellungen auf höherer Stufe wie etwa die Sicherheitsvorgaben zu überprüfen. Solche Werkzeuge können wie folgt genutzt werden:

a) Konvertierung der Darstellung zur Umsetzung in eine ausführbare formale Spezifikation;

b) Ausführung der formalen Spezifikation, um die Eigenschaften der Darstellung zu testen.

4.5.110 Praktische Erfahrungen zeigen, daß die Erstellung der formalen Spezifikation mindestens so wertvoll ist wie ihre Ausführung.

4.5.111 *CASE-Tools:* Ist zur Erstellung eines Feinentwurfs ein CASE-Tool verwendet worden, können die Evaluatoren versuchen, das Werkzeug zur Durchführung einer unabhängigen Validierung des Entwurfs unter Verwendung der von dem Werkzeug bereitgestellten Validierungsfunktionen einzusetzen. Dies kann durch Einsatz des Werkzeuge zur Überprüfung des Entwurfs und durch Verwendung seiner Berichtsfunktionen zur Identifizierung von Fehlern und Auslassungen wie etwa den folgenden geschehen:

a) Datenflüsse, die zwischen Diagrammen auf unterschiedlichen Ebenen der Entwurfshierarchie nicht konsistent sind;

b) Datenspeicher, bei denen Datenflüsse hinein-, aber nicht herausführen (d.h., die Daten werden generiert, aber nicht von einem Prozeß verwendet);

c) Objekte (z.B. Datenelemente, Datenflüsse oder Datenspeicher), die zwar definiert sind, die aber nicht durch einen Prozeß benutzt werden;

d) Benutzung von nicht definierten Objekten.

4.5.112 *Detailed Design Checking Tools* können unterteilt werden in

a) *Rule Conformance Tools:* Diese Werkzeuge verifizieren syntaktisch und semantisch, ob der Quellcode seiner Spezifikation entspricht. Bei diesen Werkzeugen handelt es sich häufig um Erweiterungen der Werkzeuge zur Quellcodeüberprüfung.

b) *Proof Tools:* Diese Werkzeuge sind in der Lage, eine symbolische Prüfung auf partielle oder vollständige Korrektheit durchzuführen, und zwar

auf syntaktischer Ebene: Vollständigkeit, Kohärenz, Konformität;

auf semantischer Ebene: partielle oder vollständige Gültigkeit.

c) *Tracking Tools:* Diese Werkzeuge sind in der Lage, die Pfade in einem Anwendungsprogramm zu analysieren und in Text- und graphischer Form Bericht zu erstatten, einen Prozeduraufrufbaum zu generieren und Querverweisinformationen bereitzustellen. Diese Kategorie umfaßt Syntaxanalysatoren, Semantikprüfprogramme, statische Analysatoren usw.

d) *Reverse Engineering Tools:* Diese Werkzeuge sind in der Lage, Verbindungen zwischen Funktionen und Spezifikationen neu zu schaffen und herzustellen.

e) *Covert Channel Analysis Tools:* Das Vorhandensein verdeckter Kanäle kann durch Anwendung der Informationsflußanalyse überprüft werden. Diese Überprüfung würde zeigen, daß ein Informationsfluß zwischen Prozessen in einer nicht spezifizierten Weise unmöglich ist.

4.5.113 *Source Code Analysis Tools* können unterteilt werden in

a) *Data Use Analysers:* Diese Werkzeuge überprüfen ein Quellcodeprogramm auf unkorrekte Datenverwendung, z.B. daß Datenelemente vor dem Beschreiben gelesen werden;

b) *Control Flow Analysers:* Diese Werkzeuge suchen nach Kontrollflußfehlern wie etwa Schleifen ohne Ausgang oder einem nicht erreichbaren Code;

c) *Information Flow Analysers:* Diese Werkzeuge untersuchen Abhängigkeiten zwischen Datenelementen, um nach unerwünschten Abhängigkeiten zu suchen;

d) *Compliance Analysers:* Diese Werkzeuge vergleichen die Funktionalität des Quellcodes mit einer formalen Spezifikation und versuchen, die Rückführbarkeit zu belegen.

4.5.114 *Object Code Analysis Tools:* Bei E6 wird vom Antragsteller verlangt, daß er den Evaluatoren Werkzeuge zum Auffinden von Inkonsistenzen zwischen Quellcode und Objektcode zur Verfügung stellt. Mit diesen Werkzeuge können vermutete Inkonsistenzen untersucht werden.

4.5.115 *Build Tools:* Ab E3 sind klar definierte Programmiersprachen vorgeschrieben. Das Beispiel 1(b) in Teil 5 des ITSEM ist ein Beispiel dafür, wie die relevanten Evaluatoraufgaben durchzuführen sind. Ab E5 muß der Quellcode etwaiger Laufzeitbibliotheken zur Verfügung gestellt werden. Daher sind Compilerwerkzeuge im Umgang mit diesen Informationen durchaus von Nutzen.

4.5.116 Ab E4 verwenden die Evaluatoren die entwicklereigenen Werkzeuge, um ausgewählte Teile des EVG neu zu erstellen, und vergleichen das Ergebnis mit der vorgelegten Version des EVG. In dieser Hinsicht können Compiler und andere Build-Werkzeuge für die Evaluation von Nutzen sein. Insofern ist es notwendig, daß die Evaluatoren mit dem Gebrauch (und möglichen Mißbrauch) solcher Werkzeuge vertraut sind.

4.5.117 Falls ein Compiler zu einem vertrauenswürdigen Bestandteil des Systems wird (wenn beispielsweise böswillige Softwareentwickler in den Sicherheitsvorgaben als Bedrohung erwähnt werden), ist er in der üblichen Weise einer Evaluation zu unterziehen. Dies betrifft insbesondere das Problem der transitiven Trojanischen Pferde.

4.5.118 *Test Werkzeuge:* Es gibt Werkzeuge für bestimmte Compiler, mit denen die in einer Testreihe ausgeführten Quellcodezeilen aufgezeichnet werden können. Dies kann bei der Erbringung eines Nachweises der Testabdeckung genutzt werden.

4.5.119 Die Evaluatoren müssen unter Umständen Software entwickeln, um Penetrationstests durchzuführen. Außerdem kann es für die Evaluatoren wünschenswert sein, Zugang zu den entwicklereigenen Testwerkzeuge (wie etwa Testumgebung und Überwachungswerkzeuge) gewährt zu bekommen.

4.5.120 **Jede Verwendung von Testwerkzeugen muß im ETR dokumentiert werden. Von den Evaluatoren verwendete Testsoftware muß archiviert werden.**

4.5.121 *Hardware Analysis Tools:* Die Evaluation von Hardware erfordert eine gewisse Tool-Unterstützung, die für die Evaluation von Software nicht geeignet ist. Die Unterschiede betreffen in erster Linie die Verwendung von CAD-Werkzeuge und die Nichtanwendbarkeit der Codeanalyse. Die CAD-Werkzeuge können als Werkzeuge zur Entwurfsunterstützung angesehen werden (ganz wie CASE-Werkzeuge), und alles, was vorstehend zu den Design-Werkzeuge gesagt wurde, gilt auch für CAD-Werkzeuge. Man beachte, daß es aller Wahrscheinlichkeit nach unmöglich ist, ohne den Einsatz von CAD-Werkzeuge während der Entwicklung einen ausreichenden Nachweis der korrekten Implemen-tierung zu erbringen, außer bei sehr einfachen Geräten. CAD-Werkzeuge können folgende Möglich-keiten bieten:

a) Gerätebibliotheken;

b) schematische Erfassung (Zeichenpaket);

c) Erzeugung von Netzlisten;

d) Simulation;

e) Entwurf von Platinen (PCB);

f) Tests.

4.5.122 *Configuration and Audit Tools:* Für eine Reihe weitverbreiteter Betriebssysteme gibt es Sicherheitskonfigurations- und Protokollierungswerkzeuge. Diese Werkzeuge sind wahrscheinlich bei Penetrationstests von Nutzen.

4.5.123 Ein Werkzeug für die Sicherheitskonfiguration untersucht, wie ein Betriebssystem konfiguriert worden ist; dabei sucht es nach bekannten generischen Schwachstellen wie etwa allgemein lesbaren Dateien und erratbaren Paßwörtern.

4.5.124 Ein Werkzeug für die Sicherheitsprotokollierung untersucht ein **Protokoll** und sucht nach Anzeichen für Sicherheitslücken.

Zusammenfassung: Empfohlene Techniken und Werkzeuge

4.5.125 Abbildung 4.5.1 enthält eine Analyse nützlicher Techniken für Evaluatoren. Die Tabelle wurde auf der Grundlage der einzelnen Evaluatoraktivitäten erstellt.

4.5.126 Als Pendant dazu enthält Abbildung 4.5.2 eine Analyse nützlicher Werkzeuge für Evaluatoren. Zusätzliche Werkzeuge können verwendet werden, wenn dies zur Erhöhung der Zuverlässigkeit oder zur Senkung der Evaluationskosten beiträgt.

Abbildung 4.5.1 Evaluationstechniken

ITSEC Evaluations-stufe	Evaluatoraktivitäten (nur zusätzliche Aktivitäten sind aufgeführt)	TECHNIKEN (nur zusätzliche Techniken sind aufgeführt)
E1	Architekturentwurf überprüfen Implementierung überprüfen	informelle Prüfung oder Rückführbarkeitsanalyse Funktionstests Penetrationstests
E2	Feinentwurf überprüfen Implementierung überprüfen	informelle Prüfung oder Rückführbarkeitsanalyse Analyse der Testabdeckung Penetrationstests
E3	Implementierung überprüfen	Analyse der Quellcode-Testabdeckung Penetrationstests
E4	Anforderungen überprüfen Architekturentwurf überprüfen Feinentwurf überprüfen	semiformale Prüfung oder Rückführbarkeitsanalyse formales Modell der Sicherheitspolitik untersuchen semiformale Prüfung oder Rückführbarkeitsanalyse semiformale Prüfung oder Rückführbarkeitsanalyse
E5	Feinentwurf überprüfen	semiformale Prüfung oder Rückführbarkeitsanalyse Schichtenabfolge des Feinentwurfs, Abstraktion und Datenabschottung untersuchen
E6	Architekturentwurf überprüfen	formale Prüfung oder Rückführbarkeitsanalyse
Alle	Entwicklungsumgebung überprüfen	informelle Prüfung Besichtigung der Entwicklungsumgebung
Alle	Betriebsdokumentation überprüfen	informelle Prüfung
Alle	Betriebsumgebung überprüfen	informelle Prüfung
Alle	Analyse der Eignung überprüfen	Prüfung
Alle	Analyse des Zusammenwirkens überprüfen	Prüfung, einschließlich Suche nach verdeckten Kanälen (wo angebracht)
Alle	Stärke der Mechanismen untersuchen	Prüfung
Alle	Schwachstellen in der Konstruktion untersuchen	Prüfung Schwachstellenanalyse FMEA (wo angebracht)
Alle	Benutzerfreundlichkeit untersuchen	Prüfung
Alle	Operationelle Schwachstellen untersuchen	Prüfung Schwachstellenanalyse

Abbildung 4.5.2 Evaluationswerkzeuge		
ITSEC-Evaluations-stufe	Evaluatoraktivitäten	WERKZEUGE (TOOLS) (nur zusätzliche Werkzeuge sind aufgeführt)
E1	Implementierung überprüfen	Testprogramme und Testwerkzeuge (optional)
E2		
E3	Implementierung überprüfen	Testabdeckungswerkzeuge (optional)
E4	Anforderungen überprüfen Architektur überprüfen Feinentwurf überprüfen Entwicklungsumgebung überprüfen	Animation Tools (optional) CASE-Tools des Entwicklers (optional) CASE-Tools des Entwicklers (optional) Build Tools des Entwicklers
E5	Implementierung überprüfen	Source Code Analysis Tools (optional)
E6	Architektur überprüfen Implementierung überprüfen	Proof Checking Tools (optional) Werkzeuge zur Auffindung von Inkonsistenzen zwischen Quellcode und ausführbarem Code (z.B. Disassembler und/oder Debugger)
E3-E6	Analyse des Zusammenwirkens überprüfen	Source Code Analysis Tools und Matrixmanipulationswerkzeuge (optional)

Kapitel 4.6 Wiederverwendung von Evaluationsergebnissen

Einleitung

4.6.1 Eine Evaluation ist ein komplexer, aufwendiger und zeitintensiver Prozeß. Arbeits- und Kostenaufwand können je nach angestrebter Evaluationsstufe und Komplexität des EVG erheblich sein. Zur Reduzierung des erforderlichen Arbeitsumfangs können die Ergebnisse früherer Evaluationen herangezogen werden, und zwar

a) für die Evaluation eines EVG, der einen oder mehrere früher evaluierte EVG enthält;

b) für die Reevaluation eines zertifizierten EVG nach Modifikation des EVG, seiner Sicherheitsvorgaben oder seiner Evaluationsbeiträge.

4.6.2 Das vorliegende Kapitel enthält Ratschläge für Evaluatoren zur Wiederverwendung von Evaluationsergebnissen.

4.6.3 Kapitel 4.3 befaßt sich mit der Frage der Reevaluation und der Wiederverwendung von Evaluationsbeiträgen.

4.6.4 Teil 6, Kapitel 6.3 und Anhang 6.D enthalten Anleitungen für den Antragsteller/Entwickler zur Durchführung von Auswirkungsanalysen nach Modifikation eines zertifizierten EVG.

Überblick

4.6.5 Einschlägige Beispiele für die Wiederverwendung von Evaluationsergebnissen sind

a) Produkte oder Systeme, die aus mehr als einem Produkt bestehen, wobei mindestens eine Komponente schon einmal als Produkt evaluiert worden ist;

b) Produkte oder Systeme, die schon einmal evaluiert worden sind und an denen Änderungen vorgenommen worden sind, die eine Reevaluation erforderlich machen (z.B. im Fall eines neuen Produktrelease);

c) Zusammenfügungen von bereits früher auf unterschiedlichen Evaluationsstufen evaluierten Produkten (Vertrauenswürdigkeitsprofile);

d) Installation eines Systems, das aus einem bereits früher evaluierten Produkt besteht;

e) Erhöhung der Evaluationsstufe eines bereits früher evaluierten Produkts;

f) Modifikation eines EVG, seiner Sicherheitsvorgaben oder eines seiner Evaluationsbeiträge (z.B. neues Release eines Produkts).

4.6.6 Im allgemeinen hängt der Umfang, in dem eine Wiederverwendung von Evaluationsergebnissen erforderlich und sinnvoll ist, von folgendem ab:

a) der Verwendung des evaluierten EVG;

b) der Funktionalität des evaluierten EVG;

c) der erreichten Evaluationsstufe;

d) den Sicherheitsvorgaben des neuen EVG, in den der evaluierte EVG eingebettet wird.

4.6.7 Im Mittelpunkt der in diesem Kapitel enthaltenen generischen Hinweise für Evaluatoren stehen Produkte oder Systeme, die aus mehr als einem Produkt bestehen, von denen zumindest ein Teil bereits früher als Produkt evaluiert worden ist.

4.6.8 Die Frage der Wiederverwendung von bereits früher evaluierten EVG in einem anderen als dem in den Sicherheitsvorgaben der ursprünglichen Evaluation spezifizierten Kontext ist noch Gegenstand der Forschung. Der hier behandelte Sachverhalt steht in einem engen Zusammenhang mit Problemen im Bereich der Systemakkreditierung.

Generische Hinweise für den Evaluator

4.6.9 Immer wenn Zweifel hinsichtlich der Anwendung der Kriterien in den ITSEC bestehen und das ITSEM keine Hinweise dazu enthält, ist Rat bei der Zertifizierungsstelle einzuholen. Dies wäre beispielsweise der Fall, wenn ein EVG aus Komponenten besteht, die nach unterschiedlichen Evaluationsstufen evaluiert wurden.

4.6.10 Im allgemeinen besteht keine Möglichkeit, die Evaluationsstufe einer Zusammenfügung ausgehend von den Evaluationsstufen ihrer Komponenten vorab zu bestimmen. Die Zusammenfügung könnte in Anbetracht der geforderten Evaluationsbeiträge eine niedrigere Evaluationsstufe als die kleinste Evaluationsstufe der Komponenten oder gar eine höhere Evaluationsstufe als die höchste Stufe der Komponenten erreichen. Dies ist durch die in Absatz 4.6.6 beschriebenen Abhängigkeiten begründet. Die Stärke einer Zusammenfügung könnte auch von der gewählten Art der Sicherheitsziele wie etwa der Vertraulichkeit, der Integrität und der Verfügbarkeit abhängen.

4.6.11 Erst nach der Evaluation, insbesondere nach einer sowohl vom Antragsteller/Entwickler als auch vom Evaluator vorgenommenen Analyse der Wirksamkeit, kann Vertrauen in die Zusammenfügung gewonnen werden.

4.6.12 Für dieses Problem sind unterschiedliche Lösungsansätze entwickelt worden. Ein Vorschlag lautet, eine *funktionale Aufteilung* zu verwenden [TNI]. Ein anderer Ansatz ist durch die *partielle Ordnung von TCB-Untermengen* gegeben [TDI]. Das in Systemen mit virtuellen Maschinen verwendete Prinzip sieht die strikte Trennung durch einen Message-Passing-Kernel vor. Das in Teil 6, Anhang 6.F vorgestellte Zusammenfügungsmodell kann den Evaluatoren ebenfalls als Hinweis bei der Durchführung der Reevaluationsarbeit dienen.

4.6.13 In den folgenden Absätzen werden Grundregeln für EVG vorgestellt, die aus mindestens zwei Komponenten bestehen, von denen mindestens eine bereits nach derselben Evaluationsstufe evaluiert worden ist wie der zusammengefügte EVG. Wenn mehr als eine Komponente bereits früher evaluiert worden ist, wird davon ausgegangen, daß alle Komponenten nach derselben Evaluationsstufe evaluiert worden sind.

4.6.14 Wie für jeden anderen EVG müssen auch für die Zusammenfügung Sicherheitsvorgaben vorhanden sein. Es muß die Möglichkeit einer Abbildung der Sicherheitsvorgaben der Komponenten auf die Sicherheitsvorgaben der Zusammenfügung vorhanden sein. Dies muß im Rahmen der Analyse der Eignung überprüft werden.

4.6.15 Die Evaluation des zusammengefügten EVG hinsichtlich der Wirksamkeitskriterien muß unter allen Umständen stattfinden.

4.6.16 Die Analyse der Eignung muß zeigen, ob die Sicherheitseigenschaften der Einzelkomponenten zusammengenommen die angegebenen Sicherheitseigenschaften des zusammengefügten EVG bilden.

4.6.17 Die Analyse des Zusammenwirkens bei einem zusammengefügten EVG muß in derselben Weise erfolgen wie die Analyse des Zusammenwirkens bei der Evaluation eines nicht zusammengefügten EVG.

4.6.18 Die Evaluatoren müssen überprüfen, ob die in einer Komponente vorhandene Schnittstelle in der Zusammenfügung nur in der Weise verwendet wird und verwendet werden kann, daß die Sicherheitseigenschaften des zusammengefügten EVG nicht beeinträchtigt werden.

4.6.19 Die Analyse der Konstruktionsschwachstellen ist auf der Basis der Zusammenarbeit der Einzelkomponenten vorzunehmen. Die internen Details der Zielkomponente dürfen keine Annahmen verletzen, die für die Ausgangskomponente getroffen wurden. Es muß bewertet werden, ob eine potentielle Schwachstelle einer Komponente im Kontext der Zusammenfügung ausnutzbar ist. Die Liste der bei der Evaluation einer Einzelkomponente erkannten Schwachstellen könnte Schwachstellen enthalten, die nicht relevant sind, wenn die Komponente in einer Zusammenfügung verwendet wird.

4.6.20 Die Analyse der Benutzerfreundlichkeit für den zusammengefügten EVG muß in derselben Weise wie die Analyse der Benutzerfreundlichkeit bei der Evaluation eines nicht zusammengefügten EVG erfolgen.

4.6.21 Bei einer bereits evaluierten und in einer Zusammenfügung verwendeten Komponente brauchen die Korrektheitskriterien für den Entwicklungsprozeß nicht erneut evaluiert zu werden. Die Evaluatoren können davon ausgehen, daß die Entscheidung hinsichtlich der Korrektheit weiterhin Gültigkeit hat. Dies gilt nicht für Tests, welche die Wirksamkeit im neuen Kontext betreffen.

4.6.22 Die Evaluation der Korrektheit des zusammengefügten EVG als Ganzes ist auch dann erforderlich, wenn der EVG vollständig aus bereits evaluierten Komponenten besteht. Daher sollen Sicherheitsvorgaben, Architektur, Entwicklungsumgebung und Tests für den EVG als Ganzes evaluiert werden. Eine komplette Bewertung der Korrektheit gemäß den ITSEC und des ITSEM ist für diejenigen Komponenten des EVG erforderlich, die nicht bereits früher evaluiert worden sind.

4.6.23 Falls die Zusammenfügung die Benutzer- und Systemverwalter-Dokumentation betrifft, sind die Kriterien in den ITSEC für die Betriebsdokumentation anzuwenden.

4.6.24 Die Kriterien in den ITSEC für die Entwicklungsumgebung, Aspekt 1, Konfigurationskontrolle, sowie für die Betriebsumgebung sind wie bei der Evaluation eines nicht zusammengefügten EVG anzuwenden. Was diese Aspekte betrifft, braucht bei den bereits evaluierten Komponenten nichts veranlaßt zu werden.

Kapitel 4.7 Ergebnisse der Evaluation

Einleitung

Zielsetzungen

4.7.1 Das vorliegende Kapitel enthält eine detaillierte Beschreibung des geforderten Ergebnisses einer Evaluation, d.h. des ETR und der Mängelberichte.

Anwendungsbereich

4.7.2 In Kapitel 4.4 wurde die Erstellung von Evaluationsberichten im Rahmen des Evaluationsprozesses beschrieben. Es befaßt sich in erster Linie mit dem ETR, der von den Evaluatoren für den Antragsteller der Evaluation und für die Zertifizierungsstelle erstellt wird.

4.7.3 In den nationalen Regelwerken werden zusätzliche Evaluationsberichte wie etwa Berichte über Evaluationsmethoden, Mängelberichte oder Berichte über einzelne Arbeitseinheiten verlangt. Diese unterliegen den Bestimmungen des jeweiligen nationalen Regelwerks und werden in diesem Kapitel nur dann angesprochen, wenn sie den Inhalt des ETR betreffen.

Zusammenfassung

4.7.4 In diesem Kapitel wurde durchgängig von der Annahme ausgegangen, daß der ETR ein Einzeldokument ist, das aus der in Kapitel 4.4 beschriebenen Aktivität *Berichte erstellen* resultiert. Die nationalen Regelwerke können diese Annahme ignorieren und abweichende Regelungen treffen.

4.7.5 Weiter unten in diesem Kapitel wird beispielsweise gesagt, daß in einem Teil des ETR die Sicherheitsvorgaben für den EVG beschrieben werden. Ein nationales Regelwerk kann Regelungen treffen, daß die Sicherheitsvorgaben in den ETR einbezogen werden oder daß darin auf die Sicherheitsvorgaben verwiesen wird (d.h., daß der ETR zusammen mit den Sicherheitsvorgaben veröffentlicht wird).

4.7.6 Ein weiteres Beispiel wäre die Einbeziehung eines EWP anstelle des Kapitels, in dem die Evaluationsarbeiten beschrieben werden. Der EWP soll in diesem Fall zumindest die nachstehend zusammenfassend aufgeführten Punkte enthalten.

4.7.7 Für einen ETR gilt folgende Zielsetzung:

a) er soll die während der Evaluation tatsächlich durchgeführten Arbeiten beschreiben;

b) er soll die erzielten Ergebnisse und die aus den Arbeiten gezogenen Schlußfolgerungen darstellen.

4.7.8 Zur Zielgruppe eines ETR gehören:

a) die Zertifizierungsstelle;

b) der Antragsteller der Evaluation;

c) Evaluatoren, die eine Reevaluation durchführen.

4.7.9 Für den Fall, daß Antragsteller und Entwickler nicht identisch sind, sollen die nationalen Regelwerke auch Regelungen für die Weitergabe der Gesamtheit oder eines Teils des ETR an Entwickler vorsehen, die eine Wiederverwendung eines EVG als Teil eines anderen EVG in Betracht ziehen. Es sind Regelungen für die Weitergabe eines ETR an einen anderen Staat zu treffen. Wie dies geregelt wird, bleibt den nationalen Regelwerken überlassen.

4.7.10 Die Zertifizierungsstelle ist für die Abnahme eines ETR zuständig.

4.7.11 In diesem Kapitel werden die Mindestanforderungen an *Inhalt und Struktur des ETR* (anhand von Kapitel- und Abschnittsüberschriften) aufgezeigt und der Inhalt jedes einzelnen Kapitels und Abschnitts der Reihe nach behandelt.

Inhalt und Struktur des technischen Evaluationsberichts (ETR)

Ausgangsmaterial

4.7.12 Das nationale Regelwerk schreibt die Regeln für die Kennzeichnung und Handhabung von ETR vor und beschreibt die Form des Ausgangsmaterials in einem ETR. Zum Beispiel kann der EVG bei im Behördenbereich eingesetzten Systemen der Geheimhaltung unterliegen, während bei kommerziellen Systemen und Produkten eventuell Auflagen hinsichtlich der Firmenvertraulichkeit und des Datenschutzes gemacht werden.

4.7.13 Beispiele für das Ausgangsmaterial sind

a) Haftungseinschränkungen;

b) vorgeschriebene Logos;

c) Urheberrechtsklauseln.

Hauptdokument

4.7.14 In Abbildung 4.7.1 wird eine Struktur für einen ETR vorgeschlagen. Es ist davon auszugehen, daß diese Struktur mit zunehmender Evaluationserfahrung verfeinert wird.

4.7.15 Nachfolgend wird der Inhalt jedes aufgeführten Kapitels/Abschnitts beschrieben. Die nationalen Regelwerke können nach Wahl andere Strukturen für ETR vorsehen. Im konkreten Fall muß der technische Inhalt jedoch das unten aufgeführte Material umfassen.

4.7.16 **Es ist zu beachten, daß ein ETR Begründungen für alle von den Evaluatoren getroffenen Entscheidungen geben muß. Verweise auf nicht zugängliches Material sind nicht zulässig.**

ETR Kapitel 1 - Einleitung

Hintergrund

4.7.17 **Dieser Abschnitt enthält eine Einführung in den Hintergrund der Evaluation. Er muß folgendes enthalten:**

a) den von der Zertifizierungsstelle vergebenen Identifikator für die Evaluation;

b) den Namen und die Version des evaluierten EVG;

c) die Identität des Entwicklers (ggf. einschließlich Unterauftragnehmern);

d) die Identität des Antragstellers;

e) den gesamten Zeitrahmen der Evaluation;

f) die Identität der ITSEF.

Zielsetzungen

4.7.18 **In diesem Abschnitt muß die Zielsetzung des ETR (wie oben erläutert) angegeben werden.**

4.7.19 Ausführlicher dargestellt lautet die Zielsetzung wie folgt:

a) Vorlegen der Nachweise zur Begründung der Evaluationsentscheidungen und der Evaluationsschlußfolgerungen;

b) Unterstützung der Reevaluation des EVG, falls dies vom Antragsteller verlangt wird.

4.7.20 Der obige Punkt b) ist besonders wichtig, wenn Evaluationen effizient sein sollen. Dazu sind mehr Informationen in den ETR aufzunehmen als bei einer isolierten Betrachtung von Punkt a). Die Evaluatoren sollen diese Tatsache während der gesamten Evaluation im Auge behalten, insbesondere jedoch bei der Erstellung des ETR.

Anwendungsbereich

4.7.21 **In diesem Abschnitt muß angegeben werden, daß der ETR die gesamte Evaluation abdeckt. Wenn dies nicht der Fall ist, muß eine Begründung gegeben werden.**

Struktur

4.7.22 **In diesem Abschnitt muß die Struktur des ETR eingeführt werden.** Abweichungen von der in diesem Kapitel vorgeschlagenen Struktur des ETR werden von den nationalen Regelwerken geregelt.

ETR Kapitel 2 - Publizierbare Zusammenfassung

4.7.23 Dieses Kapitel dient als Grundlage für alle die Ergebnisse der Evaluation betreffenden Informationen, die von der Zertifizierungsstelle freigegeben werden.

4.7.24 In den Fällen, in denen von nationalen Regelwerken Listen zertifizierter EVG erstellt werden, bildet dieses Kapitel die Grundlage für die in diese Listen aufgenommenen Informationen.

4.7.25 **Die Zusammenfassung darf daher keine Informationen enthalten, die in irgendeiner Weise kommerziell vertraulich sind oder der nationalen Geheimhaltung unterliegen (Antragsteller und Zertifizierungsstelle bestätigen dies bei Abnahme des ETR).**

4.7.26 **Dieses Kapitel muß folgendes enthalten:**

a) die Identität der ITSEF;

b) die tatsächlich erreichte Evaluationsstufe;

c) die Kennung des EVG zusammen mit der Versions-/Releasenummer;

d) eine Zusammenfassung der wichtigsten Schlußfolgerungen der Evaluation;

e) die Identität des Antragstellers;

f) eine Kurzbeschreibung des EVG;

g) eine Kurzbeschreibung der Sicherheitseigenschaften des EVG.

ETR Kapitel 3 - Beschreibung des EVG

Funktionalität des EVG

4.7.27 **Dieser Abschnitt muß eine Zusammenfassung der operationellen Aspekte des EVG sowie der Funktionen enthalten, für deren Durchführung er ausgelegt ist, einschließlich**

a) des zu verarbeitenden Datentyps (erforderlichenfalls mit Vertraulichkeitsstufen);

b) der verschiedenen Arten von Anwendern (mit obigem verknüpft).

Entwicklungsprotokoll

4.7.28 **Dieser Abschnitt muß (bei begleitenden und, soweit möglich, auch bei nachfolgenden Evaluationen) in groben Zügen die Entwicklungsstufen bei der Erstellung des EVG darlegen.**

4.7.29 **Sämtliche Entwicklungsmethodiken, Techniken, Werkzeuge und Normen, die für die Erstellung des EVG relevant und nicht durch das Kapitel über die Ergebnisse abgedeckt sind, müssen kurz dargelegt werden.**

4.7.30 **Die Evaluationsbeiträge des EVG müssen besonders hervorgehoben werden (wobei Einzelangaben wie Ausgabestatus, Daten, Referenznummern und Autoren als Anhang A des ETR nach-geordnet werden).**

EVG-Architektur

4.7.31 **In diesem Abschnitt muß der Top-Level-Entwurf des EVG zusammengefaßt dargelegt werden. In ihm muß der Grad der Trennung zwischen sicherheitsspezifischen und anderen Komponenten belegt werden. Die Verteilung der sicherheitsspezifischen Funktionen des EVG auf Hardware, Firmware und Software (sowie möglicherweise auch die nichttechnischen Verfahren) innerhalb der Architektur des EVG muß in groben Zügen dargelegt werden.**

4.7.32 Die Versionsnummern aller Komponenten werden in Anhang C des ETR aufgeführt.

Beschreibung der Hardware

4.7.33 **Die Beschreibung der Hardware muß ausreichende Detailangaben über alle Komponenten auf der Architekturebene enthalten, die für die Evaluation relevant sind.**

Beschreibung der Firmware

4.7.34 **Die Beschreibung der Firmware muß ausreichende Detailangaben über alle Komponenten auf der Architekturebene enthalten, die für die Evaluation relevant sind.**

Beschreibung der Software

4.7.35 **Die Beschreibung der Software muß ausreichende Detailangaben über alle Teile der EVG-Software enthalten, die für die Evaluation relevant sind. In der Beschreibung muß die Software mit den Hardware- und Firmware-Komponenten verknüpft werden.**

ETR Kapitel 4 - Sicherheitseigenschaften des EVG

4.7.36 Es wird betont, daß das Verstehen des Inhalts der Sicherheitsvorgaben eine wesentliche Voraussetzung für das Verstehen des ETR ist. Ebenso ist der gleichzeitige Zugang zu den Sicherheitsvorgaben und dem ETR für eine effiziente Reevaluation unabdingbar. **In diesem Kapitel muß entweder auf die Sicherheitsvorgaben verwiesen werden, oder die Sicherheitsvorgaben müssen nochmals vollständig wiedergegeben werden.**

4.7.37 Der Inhalt dieses Kapitels wird im folgenden zusammengefaßt. Weitere Informationen sind in den ITSEC (Kapitel 2 und Anhang A) zu finden.

a) System-Sicherheitspolitik/Produktbeschreibung;

b) Spezifikation der sicherheitsspezifischen Funktionen;

c) Spezifikation der Sicherheitsmechanismen;

d) postulierte Mindeststärke der Mechanismen;

e) angestrebte Evaluationsstufe.

ETR Kapitel 5 - Evaluation

4.7.38 Kapitel 4.4 befaßt sich mit dem Prozeß der Evaluation und der Erstellung des eigentlichen EWP. Kapitel 5 des ETR enthält Detailangaben zu den durchgeführten Evaluationsarbeiten, wobei insbesondere aufgetretene Probleme (im technischen oder im administrativen Bereich) angesprochen werden. Das Kapitel soll den Analyseprozeß in den Zertifizierungsstellen dahingehend unterstützen, daß der gesamte Evaluationsprozeß sowohl aus technischer als auch aus administrativer Sicht verfeinert (und damit effizienter und kostengünstiger gestaltet) werden kann.

Evaluationsprotokoll

4.7.39 Dieser Abschnitt gleicht vom Aufbau her dem oben erwähnten Abschnitt über das Entwicklungsprotokoll in Kapitel 3. **Er muß einen Überblick über den verwendeten Evaluationsprozeß und die wichtigen Meilensteine geben, die**

a) zu Beginn der Evaluation des EVG zugewiesen wurden (z.B. für die Erstellung des EWP, des ETR usw.);

b) tatsächlich im Verlauf der Evaluation erreicht wurden.

4.7.40 Zu den wichtigen Meilensteinen können folgende gehören:

a) alle Besprechungen in der Startphase der Evaluation;

b) die Vorlage der Sicherheitsvorgaben;

c) der Zeitpunkt der Durchführung von Penetrationstests;

d) Besuche des bzw. der Entwicklungs- oder Betriebsorte des EVG;

e) der Abschluß der technischen Arbeiten.

4.7.41 **Alle verwendeten Evaluationsmethoden, Techniken, Werkzeuge und Normen müssen in groben Zügen dargelegt werden.**

Evaluationsprozeß

4.7.42 **In diesem Abschnitt muß eine Zusammenfassung des EWP gegeben werden. Die Zusammenfassung muß folgendes enthalten:**

a) die vom Arbeitsplan abgedeckten *Evaluatoraufgaben,* die unter Bezugnahme auf die ITSEC zu begründen sind;

b) die bearbeiteten *Arbeitspakete* (unter Verweis auf ITSEM-Kapitel 4.5 zum Nachweis der Verwendung akzeptierbarer Verfahren und auf ETR Anhang D für weitere Einzelheiten) - dabei müssen alle Unterschiede zwischen den im EWP vorgeschlagenen und den in der Praxis durchgeführten Arbeiten - zusammen mit einer Begründung für das Vorhandensein dieser Diskrepanzen - besonders hervorgehoben werden;

c) eine Kurzbeschreibung der Abbildung der Evaluationsbeiträge (die in Anhang A des ETR aufgeführt sind) auf die ITSEC-*Konstruktionsphasen* - darin müssen alle Unterschiede zwischen den ursprünglich angenommenen und den tatsächlich ausgelieferten oder verwendeten Konstruktionsphasen enthalten sein.

Zielsetzung der Evaluation

4.7.43 **In diesem Abschnitt müssen die evaluierten Komponenten des EVG und getroffene Annahmen über nicht untersuchte Komponenten ausgewiesen werden.**

Beschränkungen und Annahmen

4.7.44 **In diesem Abschnitt müssen alle Beschränkungen der Evaluation und alle während der Evaluation getroffenen Annahmen herausgestellt werden.**

ETR Kapitel 6 - Zusammenfassung der Evaluationsergebnisse

4.7.45 **In diesem Kapitel müssen die Evaluationsergebnisse unter Bezugnahme auf die in den ITSEC ausgewiesenen Evaluatoraufgaben zusammengefaßt werden.** Daher lehnt sich das Kapitel in seinem Aufbau im wesentlichen an die mit der Wirksamkeit und der Korrektheit befaßten Kapitel der ITSEC an.

4.7.46 **Für Unterabschnitte müssen Bezeichnungen verwenden werden, die der einzelnen Evaluatoraufgabe für die jeweilige Phase oder den jeweiligen Aspekt entsprechen.**

4.7.47 **Alle Unterabschnitte müssen auf die relevanten Arbeitspaketberichte verweisen, die in Anhang D des ETR enthalten sind.**

4.7.48 Die ersten sechs Abschnitte werden nachstehend lediglich aufgelistet. Die abschließenden vier Abschnitte (Penetrationstests, entdeckte ausnutzbare Schwachstellen, Beobachtungen zu nicht ausnutzbaren Schwachstellen und entdeckte Fehler) werden in den danach folgenden Absätzen kurz erläutert.

a) Wirksamkeit - Konstruktion

- Aspekt 1 - Eignung der Funktionalität
- Aspekt 2 - Zusammenwirken der Funktionalität
- Aspekt 3 - Stärke der Mechanismen
- Aspekt 4 - Bewertung der Konstruktionsschwachstellen

b) Wirksamkeit - Betrieb

- Aspekt 1 - Benutzerfreundlichkeit
- Aspekt 2 - Bewertung der operationellen Schwachstellen

c) Konstruktion - Der Entwicklungsprozeß

- Phase 1 - Anforderungen
- Phase 2 - Architekturentwurf
- Phase 3 - Feinentwurf
- Phase 4 - Implementierung

d) Konstruktion - Die Entwicklungsumgebung

- Aspekt 1 - Konfigurationskontrolle
- Aspekt 2 - Programmiersprachen und Compiler
- Aspekt 3 - Sicherheit beim Entwickler

e) Betrieb - Die Betriebsdokumentation

- Aspekt 1 - Benutzerdokumentation
- Aspekt 2 - Systemverwalter-Dokumentation

f) Betrieb - Die Betriebsumgebung

- Aspekt 1 - Auslieferung und Konfiguration
- Aspekt 2 - Anlauf und Betrieb

Penetrationstests

4.7.49 Wie in Kapitel 4.5 sind die Penetrationstestergebnisse gesondert behandelt worden, da die Penetrationstests in der Regel am einfachsten als Teil eines Arbeitspakets durchgeführt werden.

4.7.50 **Alle während der Penetrationstests verwendeten Konfigurationsoptionen müssen aufgezeichnet werden.**

4.7.51 **In den Ergebnissen der Penetrationstests muß auf folgendes verwiesen werden:**

a) auf das ursprüngliche Arbeitspaket, in dem sie formuliert wurden;

b) auf die durch die ITSEC vorgeschriebene Evaluatoraufgabe.

Entdeckte ausnutzbare Schwachstellen

4.7.52 **In diesem Abschnitt müssen die bei der Evaluation entdeckten ausnutzbaren Schwachstellen beschrieben und folgende Angaben gemacht werden:**

a) die sicherheitsspezifische Funktion, in der die Schwachstelle entdeckt wurde;

b) eine Beschreibung der Schwachstelle;

c) die bei Entdeckung der Schwachstelle ausgeführte Evaluatoraufgabe;

d) das bei Entdeckung der Schwachstelle ausgeführte Arbeitspaket;

e) den Entdecker der Schwachstelle (Entwickler oder Evaluator);

f) das Datum der Entdeckung der Schwachstelle;

g) ob die Schwachstelle behoben wurde (mit Datum) oder nicht;

h) die Quelle der Schwachstelle (falls möglich).

Beobachtungen zu nicht ausnutzbaren Schwachstellen

4.7.53 **In diesem Abschnitt müssen Angaben zu den nicht ausnutzbaren Schwachstellen gemacht werden, die bei der Evaluation entdeckt wurden (die im betriebsbereiten EVG verbleibenden Schwachstellen sind hervorzuheben).**

Entdeckte Fehler

4.7.54 **In diesem Abschnitt müssen die Auswirkungen von im Laufe der Entwicklung entdeckten Fehlern aus der Sicht der Evaluatoren zusammengefaßt werden. Alle auf den entdeckten Fehlern basierenden konkreten Ergebnisse oder Schlußfolgerungen hinsichtlich der Fähigkeit des EVG, die angestrebte Evaluationsstufe zu erfüllen, müssen vollständig begründet werden.**

ETR Kapitel 7 - Hinweise zur Reevaluation und Auswirkungsanalyse

4.7.55 Dieses Kapitel ist optional. Es kann ausgelassen werden, wenn der Antragsteller erklärt hat, daß er keine Informationen zur Reevaluation oder Auswirkungsanalyse benötigt.

4.7.56 **Falls vorhanden, muß in diesem Kapitel des ETR folgendes aufgezeichnet werden (durch Ausweisung der Konstruktionsphase, des Konstruktionsaspekts oder des Betriebsaspekts in Verbindung mit einem Verweis auf die Evaluationsbeiträge):**

a) die Einstufung aller Teile des EVG in jeder untersuchten Konstruktionsphase in sicherheitsspezifisch, sicherheitsrelevant oder nicht sicherheitsrelevant (laut Definition in Teil 3 des ITSEM);

b) die Identifizierung derjenigen Entwicklungswerkzeuge des EVG, die sicherheitsrelevant sind (laut Definition in Teil 3 des ITSEM);

c) in welcher Art und Weise sich die Beschränkungen oder Annahmen der Evaluation auf die Reevaluation oder Wiederverwendung auswirken könnten;

d) aus den Evaluationstechniken oder -werkzeuge gezogene Lehren, die für eine Reevaluation von Nutzen wären (es kann sein, daß in den nationalen Regelwerken die Erstellung eines gesonderten Dokuments für ihre Aufzeichnung beschlossen wird);

e) alle notwendigen Archivierungsdetails zum erneuten Starten der Evaluation (es kann sein, daß in den nationalen Regelwerken die Erstellung eines gesonderten Dokuments für ihre Aufzeichnung beschlossen wird);

f) etwaige spezifische Fachkenntnisse, die für die 'Reevaluatoren' vor Beginn der Reevaluation empfehlenswert sind (es kann sein, daß in den nationalen Regelwerken die Erstellung eines gesonderten Dokuments für ihre Aufzeichnung beschlossen wird);

g) den Evaluatoren bekannte Möglichkeiten, den EVG so zu konfigurieren, daß er unsicher wird.

ETR Kapitel 8 - Schlußfolgerungen und Empfehlungen

4.7.57 **Die Schlußfolgerungen und Empfehlungen der Evaluation müssen in diesem Kapitel beschrieben werden. Die wichtigste Schlußfolgerung bezieht sich darauf, ob der EVG die Sicherheitsvorgaben erfüllt hat und keine ausnutzbaren Schwachstellen aufweist.**

4.7.58 Empfehlungen werden normalerweise der Zertifizierungsstelle gegenüber ausgesprochen. Es ist zu beachten, daß diese Empfehlungen die in den Anwendungsbereich der Evaluation fallenden Teile des EVG betreffen, und daß es andere, den Evaluatoren nicht bekannte Faktoren geben kann, die den Inhalt des Zertifikats/Zertifizierungsreports des EVG ebenfalls beeinflussen können.

4.7.59 Die Empfehlungen können auch Anregungen für andere Beteiligte wie etwa den Antragsteller oder Entwickler enthalten, die an die Zertifizierungsstelle weiterzuleiten sind. Diese Empfehlungen können auch eine entsprechende Anmerkung enthalten, daß die Ergebnisse der Evaluation nur für eine bestimmte Version des EVG mit einer spezifischen Konfiguration gültig sind und daß die Zertifizierungsstelle, wie in Teil 6, Anhang 6.D beschrieben, über alle Änderungen des EVG zu informieren ist.

ETR Anhang A - Liste der Evaluationsbeiträge

4.7.60 **In diesem Anhang müssen alle Evaluationsbeiträge mit Versionsnummer und Empfangsdatum angegeben werden (im allgemeinen genügt die Angabe der neuesten Version eines Evaluations-beitrags, sofern keine Ergebnisse aus früheren Versionen vorliegen), oder es muß ein Verweis auf die Liste der Evaluationsbeiträge erfolgen.**

4.7.61 **Abweichungen von den in Teil 6, Anhang 6.A angegebenen Evaluationsbeiträgen müssen besonders hervorgehoben und begründet werden.**

ETR Anhang B - Liste der Abkürzungen/Glossar

4.7.62 **In diesem Anhang müssen alle im Rahmen des ETR verwendeten Akronyme oder Abkürzungen erläutert werden. Außerdem müssen alle Begriffe definiert werden, die nicht im ITSEC- oder ITSEM-Glossar erscheinen.**

ETR Anhang C - Evaluierte Konfiguration

4.7.63 **Die Konfigurationen des bei der Evaluation untersuchten EVG (insbesondere die im Rahmen der Penetrationstests, der Bewertung der Benutzerfreundlichkeit und der Arbeiten an dem betriebsbereiten EVG verwendeten Konfigurationen) müssen übersichtlich angegeben werden.**

4.7.64 **Alle getroffenen Annahmen oder nicht berücksichtigten Konfigurationen müssen hervorgehoben werden.**

Beschreibung der Hardware

4.7.65 **Die Hardware-Beschreibung muß Konfigurationsinformationen zu allen Komponenten auf der Architekturebene enthalten, die für die Evaluation (und somit für die sicherheitsspezifischen Funktionen) relevant sind.**

Beschreibung der Firmware

4.7.66 **Die Firmware-Beschreibung muß Konfigurationsinformationen zu allen Komponenten (wie oben beschrieben) enthalten, die für die Evaluation (und somit für die sicherheitsspezifischen und möglicherweise sicherheitsrelevanten Funktionen) relevant sind.**

Beschreibung der Software

4.7.67 **Die Software-Beschreibung muß Konfigurationsinformationen für Teile der EVG-Software enthalten, die für die Evaluation (und somit für die sicherheitsspezifischen und sicherheitsrelevanten Funktionen) relevant sind.**

ETR Anhang D - Arbeitspaketberichte

4.7.68 Dieser Anhang braucht nicht erstellt zu werden, wenn alle Arbeitspaketberichte in Kapitel 6 des ETR enthalten sind.

4.7.69 **Sofern vorhanden, muß dieser Anhang Aufzeichnungen aller durchgeführten Arbeiten enthalten (einschließlich der Stichprobenprüfung der Ergebnisse durchgeführter Tests sowie verwendeter Techniken und Werkzeuge), die zur Begründung der getroffenen Entscheidungen bei der Durchführung der Evaluatoraufgaben erforderlich sind.**

ETR Anhang E - Mängelberichte

4.7.70 Die Vorschriften für die Erstellung von Mängelberichten werden im Rahmen der nationalen Regelwerke erlassen. **Alle ausgegebenen Mängelberichte müssen in diesen Anhang aufgenommen werden.** Sie können vor Beendigung der Evaluation freigegeben werden. **Mängelberichte müssen mindestens folgende Punkte umfassen:**

a) die von der Zertifizierungsstelle zugewiesene Kennung der Evaluation;

b) Name und Version des evaluierten EVG;

c) die Aktivität, in deren Verlauf der Mangel entdeckt wurde;

d) Beschreibung des Mangels.

Abbildung 4.7.1 Struktur des ETR (1 von 2)

ETR Kapitel 1 - Einleitung

- Hintergrund
- Zielsetzung
- Anwendungsbereich
- Struktur

ETR Kapitel 2 - Publizierbare Zusammenfassung

ETR Kapitel 3 - Beschreibung des EVG

- Funktionalität des EVG
- Entwicklungsprotokoll
- EVG-Architektur
  - Beschreibung der Hardware
  - Beschreibung der Firmware
  - Beschreibung der Software

ETR Kapitel 4 - Sicherheitseigenschaften des EVG

- System-Sicherheitspolitik/Produktbeschreibung
- Spezifikation der sicherheitsspezifischen Funktionen
- Spezifikation der Sicherheitsmechanismen
- Postulierte Mindeststärke der Mechanismen
- Angestrebte Evaluationsstufe

ETR Kapitel 5 - Evaluation

- Evaluationsprotokoll
- Evaluationsprozeß
- Umfang der Evaluation
- Beschränkungen und Annahmen

Abbildung 4.7.1 Struktur des ETR (2 von 2)

ETR Kapitel 6 - Zusammenfassung der Evaluationsergebnisse

- Wirksamkeit - Konstruktion
  - Aspekt 1 - Eignung der Funktionalität
  - Aspekt 2 - Zusammenwirken der Funktionalität
  - Aspekt 3 - Stärke der Mechanismen
  - Aspekt 4 - Bewertung der Konstruktionsschwachstellen
- Wirksamkeit - Betrieb
  - Aspekt 1 - Benutzerfreundlichkeit
  - Aspekt 2 - Bewertung der operationellen Schwachstellen
- Konstruktion - Der Entwicklungsprozeß
  - Phase 1 - Anforderungen
  - Phase 2 - Architekturentwurf
  - Phase 3 - Feinentwurf
  - Phase 4 - Implementierung
- Konstruktion - Die Entwicklungsumgebung
  - Aspekt 1 - Konfigurationskontrolle
  - Aspekt 2 - Programmiersprachen und Compiler
  - Aspekt 3 - Sicherheit beim Entwickler
- Betrieb - Die Betriebsdokumentation
  - Aspekt 1 - Benutzerdokumentation
  - Aspekt 2 - Systemverwalter-Dokumentation
- Betrieb - Die Betriebsumgebung
  - Aspekt 1 - Auslieferung und Konfiguration
  - Aspekt 2 - Anlauf und Betrieb
- Penetrationstests
- Entdeckte ausnutzbare Schwachstellen
- Beobachtungen zu nicht ausnutzbaren Schwachstellen
- Entdeckte Fehler

ETR Kapitel 7 - Hinweise zur Reevaluation und Auswirkungsanalyse

ETR Kapitel 8 - Schlußfolgerungen und Empfehlungen

ETR Anhang A - Liste der Evaluationsbeiträge

ETR Anhang B - Liste der Abkürzungen/Glossar

ETR Anhang C - Evaluierte Konfiguration

ETR Anhang D - Arbeitspaketberichte

ETR Anhang E - Mängelberichte

Teil 5 Anwendungsbeispiele für die ITSEC

Inhalt

Abbildungen

Kapitel 5.1 Einleitung

Zielsetzung dieses Teils

5.1.1 Im vorliegenden Teil soll an Beispielen gezeigt werden, wie der im ITSEM beschriebene Ansatz gemeinsam mit den Kriterien in den ITSEC auf die Evaluation von Systemen und Produkten angewandt werden kann.

5.1.2 Dieser Teil ist nicht verbindlich. Er soll die ITSEC und das ITSEM nicht ausführlich beschreiben, sondern nur ihre Anwendung veranschaulichen.

5.1.3 Dieser Teil soll in der Hauptsache vollständige Beispiele liefern für

a) begleitende Evaluationen;

b) nachfolgende Evaluationen;

c) Software;

d) Hardware;

e) Produkte;

f) Systeme;

g) **die Reevaluation**;

h) **die Wiederverwendung** von Evaluationsergebnissen.

5.1.4 Die obigen Punkte (d), (g) und (h) werden in der vorliegenden Version des ITSEM nicht behandelt, sind jedoch für zukünftige Versionen vorgesehen.

5.1.5 Die Beispiele 1 bis 6 basieren auf Evaluationserfahrungen, die in Europa vor Veröffentlichung der ITSEC gemacht wurden. Als Quellen dienen reale Evaluationen, die jedoch bereinigt und an die ITSEC angepaßt wurden.

5.1.6 Beispiel 7 ist theoretischer, spekulativer Natur.

5.1.7 Beispiel 8 befaßt sich mit der Sicherheit beim Entwickler.

Zusammenhang zwischen diesem Teil und den ITSEC

5.1.8 Die Beispiele behandeln folgende Themen:

a) Prüfung der Entwicklungsumgebung (auf E2 und E4);

b) Prüfung der Anforderungen auf Korrektheit (auf E4);

c) Prüfung der Architektur auf Korrektheit (auf E4);

d) Prüfung des Entwurfs auf Korrektheit (auf E2);

e) Prüfung der Implementierung auf Korrektheit (auf E2);

f) Prüfung des Betriebs auf Korrektheit (primär auf E2, aber mit Beispielen auf allen Stufen, die die Begriffe *darlegen/angeben*, *beschreiben* und *erklären* im Kontext eines Benutzerhandbuchs abdecken);

g) Bewertung der Wirksamkeit (E3);

h) *Prüfung der Sicherheit beim Entwickler* (auf E2 und E4).

5.1.9 In den Abbildungen 5.1.1, 5.1.2 und 5.1.3 sind die Aufgaben des Evaluators in Tabellenform zusammengefaßt. Die Kriterien sind unterteilt in Aufgaben zur Bewertung der Korrektheit (Abbildungen 5.1.1 und 5.1.2) und Aufgaben zur Bewertung der Wirksamkeit (Abbildung 5.1.3).

5.1.10 Die Einträge in den Tabellenfeldern verweisen auf die Absatznummern in [ITSEC].

5.1.11 In den Tabellenreihen gelten folgende Konventionen. Ein Pluszeichen ('+') gibt an, daß zusätzliche Aufgaben des Evaluators durchzuführen sind bzw. daß zusätzliche **Evaluationsbeiträge** zu erbringen sind, die über die für die vorausgegangene Evaluationsstufe genannten hinausgehen. Anders ausgedrückt: Wenn ein Feld kein Pluszeichen enthält, wird auf den gleichen Absatz verwiesen wie in dem Eintrag links von diesem Feld.

5.1.12 Die Kriterien für die Wirksamkeit sind nicht für jede Evaluationsstufe in den ITSEC gesondert angegeben. Die Bewertung der Wirksamkeit erfolgt jedoch auf den höheren Evaluationsstufen mit zunehmender Strenge, hauptsächlich aufgrund der Tatsache, daß das von den Evaluatoren gewonnene Verständnis mit der Höhe der Evaluationsstufen zunimmt.

5.1.13 Der Hauptkorpus dieses Teils umfaßt acht Beispiele. Die durch Beispiele abgedeckten Aufgaben sind in den Abbildungen 5.1.1, 5.1.2 und 5.1.3 jeweils durch Schattierung hervorgehoben.

5.1.14 In den Überschriften der Beispiele wird die Evaluationsaktivität sowie die angestrebte Evaluationsstufe angegeben.

5.1.15 In diesem Teil bezieht sich der Begriff ***Mängelbericht*** auf die formale Aufzeichnung eines **Fehlers** durch die Evaluatoren.

	E1	E2	E3	E4	E5	E6
Aufgaben zu den Anforderungen	E1.4	E2.4	E3.4	2 E4.4+	E5.4	E6.4
Aufgaben zum Architekturentwurf	E1.7	E2.7+	E3.7	3 E4.7	E5.7+	E6.7+
Aufgaben zum Feinentwurf		4 E2.10+	E3.10	E4.10	E5.10	E6.10
Aufgaben zur Implementierung	E1.13	5 E2.13+	E3.13+	E4.13	E5.13	E6.13+

+ zeigt größere Strenge der Aufgabe an

n zeigt die durch Beispiele abgedeckten Aufgaben an

n: in Beispiel n behandelt

Abbildung 5.1.1 ITSEC-Evaluatoraufgaben zur Korrektheit (i)

	E1	E2	E3	E4	E5	E6
Aufgaben zur Konfigurationskontrolle	**E1.17**	**1a E2.17+**	**E3.17**	**E4.17+**	**E5.17+**	**E6.17**
Aufgaben zu Programmiersprachen und Compilern			**E3.20+**	**1b E4.20**	**E5.20**	**E6.20**
Aufgaben zur Sicherheit beim Entwickler		**8a E2.23+**	**E3.23**	**8b E4.23**	**E5.23**	**E6.23**
Aufgaben zur Benutzerdokumentation	**E1.27**	**6a E2.27**	**E3.27**	**E4.27**	**E5.27**	**E6.27**
Aufgaben zur Systemverwalter-dokumentation	**E1.30**	**6b E2.30**	**E3.30**	**E4.30**	**E5.30**	**E6.30**
Aufgaben zu Auslieferung und Konfiguration	**E1.34**	**6c E2.34+**	**E3.34**	**E4.34**	**E5.34**	**E6.34**
Aufgaben zu Anlauf und Betrieb	**E1.37**	**6d E2.37**	**E3.37**	**E4.37**	**E5.37**	**E6.37**

+ zeigt größere Strenge der Aufgabe an

n zeigt die durch Beispiele abgedeckten Aufgaben an

n: in Beispiel n behandelt

Abbildung 5.1.2 ITSEC-Evaluatoraufgaben zur Korrektheit (ii)

	E1	E2	E3	E4	E5	E6
Aufgaben zur Eignung der Funktionalität	**3.16**	**3.16+**	**7 E3.16+**	**3.16+**	**3.16+**	**3.16+**
Aufgaben zum Zusammen-wirken der Funktionalität	**3.20**	**3.20+**	**7 E3.20+**	**3.20+**	**3.20+**	**3.20+**
Aufgaben zur Stärke der Mechanismen	**3.24**	**3.24+**	**7 E3.24+**	**3.24+**	**3.24+**	**3.24+**
Aufgaben zur Bewertung von Konstrukt.-Schwachstellen	**3.28**	**3.28+**	**7 E3.28+**	**3.28+**	**3.28+**	**3.28+**
Aufgaben zur Benutzerfreundlichkeit	**3.33**	**3.33+**	**7 E3.33+**	**3.33+**	**3.33+**	**3.33+**
Aufgaben zur Bewertung operation. Schwachstellen	**3.37**	**3.37+**	**7 E3.37+**	**3.37+**	**3.37+**	**3.37+**

+ zeigt größere Strenge der Aufgabe an

n zeigt die durch Beispiele abgedeckten Aufgaben an

n: in Beispiel n behandelt

Abbildung 5.1.3 ITSEC-Evaluatoraufgaben zur Wirksamkeit

Kapitel 5.2 Beispiel 1, Prüfung der Entwicklungsumgebung (E2 und E4)

Einleitung

5.2.1 In diesem Beispiel werden zwei Unterbeispiele (1(a) und 1(b)) vorgestellt, die jeweils einen Aspekt der Entwicklungsumgebung auf verschiedenen Evaluationsstufen behandeln.

Beispiel 1(a) – Prüfung der Unteraktivität Konfigurationskontrolle (E2.17)

Einleitung

5.2.2 Dieses Unterbeispiel behandelt die Aufgaben zu Aspekt 1 der Entwicklungsumgebung - Konfigurationskontrolle. Die Evaluation wies folgende Merkmale auf:

a) Der EVG war ein Echtzeitsystem;

b) die angestrebte Evaluationsstufe war E2;

c) die Evaluation wurde parallel zur Systementwicklung durchgeführt.

Relevante Evaluationsbeiträge

5.2.3 Als Evaluationsbeiträge standen für diese Arbeit zur Verfügung:

a) Konfigurationsliste mit Angabe der Version des zu evaluierenden EVG;

b) Informationen zum Konfigurationskontrollsystem.

Durchgeführte Arbeiten

5.2.4 Die Informationen zum Konfigurationskontrollsystem waren in den vom Entwickler mitgelieferten Verfahrensvorschriften für das Projektkonfigurationsmanagement enthalten. Diese wurden von den Evaluatoren geprüft (indem sie sie lasen und verstanden). Insbesondere überprüften die Evaluatoren,

a) ob in der Konfigurationsliste alle Basiskomponenten aufgeführt waren, aus denen der EVG aufgebaut war;

b) ob in den Verfahrensvorschriften vorgeschrieben war, daß alle Basiskomponenten und die gesamte relevante Dokumentation mit einer eindeutigen Kennung versehen sein mußten und daß die Angabe dieser Kennung in Verweisen Pflicht war;

c) ob in den Verfahrensvorschriften vorgeschrieben war, daß der in Evaluation befindliche EVG mit der einzubringenden Dokumentation des Evaluationsbeitrags übereinstimmte, und ob nur genehmigte Änderungen möglich waren.

5.2.5 Die Evaluatoren hatten anschließend Gelegenheit, den Entwicklungsort zu besichtigen und die Anwendung der Konfigurationskontrollverfahren zu bestätigen, und zwar

a) durch Bewertung sonstiger vorgelegter Dokumente im Hinblick auf die Einhaltung der vorgeschriebenen Vorgehensweisen;

b) durch Befragung von Mitarbeitern, um herauszufinden, ob sie mit den Vorgehensweisen vertraut sind und ob diese ihrer Meinung nach eingehalten wurden.

5.2.6 Um sicherzustellen, daß die Verfahren konsequent angewandt wurden, führten die Evaluatoren folgendes durch:

a) Einzelbefragungen mehrerer Mitarbeiter des Entwicklungsteams, wobei in jedem Gespräch die gleichen Fragen gestellt wurden;

b) Befragungen von Mitarbeitern in höherer und niedrigerer Stellung: ranghöhere Mitarbeiter wissen eventuell besser Bescheid, welche Verfahren anzuwenden sind, rangniedrigere Mitarbeiter dagegen haben vielleicht einen realistischeren Einblick in die tatsächliche Praxis.

5.2.7 Um des weiteren zu überprüfen, ob die dokumentierten Verfahren beachtet wurden, führten die Evaluatoren anschließend folgendes durch:

a) Auswahl mehrerer Objekte;

b) Verfolgung ihres Änderungsprotokolls durch das Konfigurationskontrollsystem (Überprüfen von Bereichen wie die ordnungsgemäße Genehmigung von Änderungen, die ordnungsgemäße Verwendung von Formularen für Änderungsanforderungen usw.).

5.2.8 Da die ITSEC-Korrektheitskriterien für die Konfigurationskontrolle erfüllt wurden, konnte eine *akzeptierende* Entscheidung gefällt werden.

Beispiel 1(b) – Prüfung der Unteraktivität Programmiersprachen und Compiler (E4.20)

Einleitung

5.2.9 Dieses Unterbeispiel behandelt die Aufgaben des Evaluators zu Aspekt 2 der Entwicklungsumgebung – Programmiersprachen und Compiler.

5.2.10 Der EVG wurde mit einer strukturierten Programmiersprache und mit einem im Handel erhältlichen Compiler implementiert, der über Erweiterungen zum ISO-Standard für diese Sprache verfügte. Die angestrebte Evaluationsstufe war E4.

Relevante Evaluationsbeiträge

5.2.11 Der Beitrag zu dieser Aufgabe umfaßte

a) das Referenzhandbuch zum Compiler;

b) die vom Entwicklungsteam einzuhaltenden Programmierstandards, einschließlich einer Definition der zu verwendenden Compiler-Optionen.

Durchgeführte Arbeiten

5.2.12 Die Evaluationsbeiträge für die bei der Entwicklung des EVG verwendete Implementierungssprache und die Compiler wurden dahingehend untersucht, ob der Entwickler eine klar definierte Programmiersprache verwendete. Die Evaluatoren stellten fest, daß das Referenzhandbuch des Compilers keinen Anspruch auf Einhaltung eines anerkannten Standards für die Sprache erhob (z. B. ANSI- oder ISO-Normen).

5.2.13 Die entwicklereigenen Programmierstandards legten eine Teilmenge von Anweisungen der Programmiersprache fest, die aus dem ISO-Standard für diese Sprache abgeleitet wurde. Da der Compiler nicht anhand eines anerkannten Standards validiert worden war, hielten die Evaluatoren es für notwendig, das Referenzhandbuch des Compilers dahingehend zu überprüfen, ob die Bedeutung aller in den Standards des Entwicklers bezeichneten Anweisungen eindeutig festgelegt war.

5.2.14 Die Compiler-Dokumentation wurde ebenfalls untersucht, um die Auswirkungen der in den Standards des Entwicklers bezeichneten Compiler-Optionen zu überprüfen. Beispielsweise erzeugen bestimmte Sprachcompiler unerwartete Effekte (wie etwa die Optimierung von Quellcode-Anweisungen aus Schleifen heraus), wenn die Option OPTIMISATION gewählt wird.

5.2.15 Die Evaluatoren stellten fest, daß es sich bei dem betreffenden Compiler um ein gängiges kommerzielles Produkt handelte, das als solches gründlich getestet war. Bekannte Compiler-Probleme waren in den Release-Anmerkungen zum Compiler genau dokumentiert, und es stellte sich heraus, daß sie keine Auswirkungen auf die Entwicklung des EVG zeigten.

5.2.16 Neben der Definition einer Teilmenge der Sprachanweisungen schlossen die Programmierstandards des Entwicklers die Verwendung von Strukturen und Techniken aus, die die Entwickler für "unsicher" erachteten. Dazu gehörten

a) berechnete *GOTOs*;

b) Aliasnamen (z. B. *EQUIVALENCE* in Fortran).

5.2.17 Die Evaluatoren stellten weiterhin fest, daß die Standards des Entwicklers zwangsläufig auch zu defensiven Programmierpraktiken führten, darunter

a) die Verwendung von Datentypen (Aufzählungstypen, Unterbereiche usw.);

b) die gemeinsame Definition von Typen und Variablen, die von mehr als einer Komponente verwendet wurden (z. B. durch Verwendung von *INCLUDE*-Anweisungen);

c) die Behandlung von Ausnahmebedingungen: Bereichsprüfung und Überprüfung der Feldgrenzen von Gruppenfeldern, Maßnahmen bei Division durch Null und Zahlenbereichsüberlauf;

d) eine Typprüfung zwischen getrennten Kompilierungseinheiten.

5.2.18 Die Evaluatoren konnten bestätigen, daß die Programmierstandards des Entwicklers eingehalten wurden. Die Überprüfung auf Einhaltung der Standards des Entwicklers erfolgte parallel zur Prüfung des Quellcodes im Rahmen der Prüfung der Implementierung auf Korrektheit.

5.2.19 Abschließend untersuchten die Evaluatoren die "Generierungsdateien" und ihre Verwendung um sicherzustellen, daß die von den Programmierstandards geforderten Compiler-Optionen im gesamten Entwicklungsprojekt durchgängig angewandt wurden.

5.2.20 Abschließend konnten die Evaluatoren diesem Aspekt der Entwicklungsumgebung eine *akzeptierende* Entscheidung zusprechen.

Kapitel 5.3 Beispiel 2, Prüfung der Anforderungen auf Korrektheit (E4)

Einleitung

5.3.1 Dieses Beispiel behandelt die Aufgaben des Evaluators in der Konstruktionsphase 1 des Entwicklungsprozesses – Anforderungen. Der EVG war ein kundenspezifisches System. In den Sicherheitsvorgaben für den EVG war die Funktionalitätsklasse F-B1 festgelegt.

Relevante Evaluationsbeiträge

5.3.2 Die Sicherheitsvorgaben umfaßten

a) die System-Sicherheitspolitik (System Security Policy, SSP);

b) die IT-Sicherheitspolitik (System Electronic Information Security Policy, SEISP);

c) das Sicherheitsmodell (Security Policy Model, SPM);

d) die angestrebte Evaluationsstufe E4;

e) die Bewertung der Mindeststärke der Mechanismen als mittel;

f) die vorgeschriebenen kryptographischen Mechanismen.

5.3.3 Die Beziehungen zwischen den obigen Bestandteilen der Sicherheitsvorgaben sind in Abbildung 5.3.1 dargestellt.

5.3.4 SSP, SEISP und SPM entsprachen ITSEC Version 1.2, Absätze 2.27 bis 2.29.

5.3.5 Das SPM lieferte ein formales Modell der Anforderungen für das System hinsichtlich Identifikation, **Authentisierung** und Zugriffskontrolle in der Z-Notation. Das SPM beinhaltete Vorbedingungs-prüfungen, um zu zeigen, daß Statusübergänge sicher erfolgten. Das SPM lieferte außerdem eine informelle Interpretation der formal definierten Anforderungen an Identifikation, Authentisierung und Zugriffskontrolle. Das SPM verwies auf das Bell-La Padula-Modell der zugrundeliegenden Sicher-heitspolitik.

5.3.6 Die sicherheitsspezifischen Funktionen der SEISP wurden als informelle Interpretation des Sicherheitsmodells in bezug auf die Sicherheitsvorgaben bewertet.

Durchgeführte Arbeiten

5.3.7 Die Evaluationsbeiträge zu den Anforderungen wurden auf Inhalt, Form und Nachweis überprüft. Die Evaluatoren stellten fest, daß die Anforderungen an die Identifikation, Authentisierung und Zugriffskontrolle korrekt in einer semiformalen Form spezifiziert worden waren, während die Anforderungen an die Beweissicherung, Protokollauswertung und Wiederaufbereitung nur informell spezifiziert worden waren.

5.3.8 Die Evaluatoren verfaßten einen Mängelbericht mit der Empfehlung, diejenigen Anforderungen, die nicht in semiformaler Form dargestellt waren, mit Hilfe von Datenflußdiagrammen, einer logischen Datenstruktur und Entity-Life-Protokollen entsprechend der Darstellungsform zu beschreiben, die für die korrekt in semiformaler Form spezifizierten Sicherheitsanforderungen verwendet wurde (für das Projekt war eine strukturierte Systemanalyse- und Entwurfsmethodik (Structured Systems Analysis And Design Methodology, SSADM) verwendet worden).

5.3.9 Die Überprüfung durch die Evaluatoren umfaßte

a) die Zuordnung der sicherheitsspezifischen Funktionen in der SEISP zu den in der SSP aufgeführten Sicherheitszielen und Sicherheitsbedrohungen;

b) die manuelle Verifizierung der SEISP anhand der SSP, um die Konsistenz innerhalb der Dokumentation zu gewährleisten;

c) die Validierung der sicherheitsspezifischen Funktionen der SEISP anhand des formalen SPM und des darin enthaltenen Textes;

d) die Überprüfung, ob das SPM der Intention des Bell-La Padula-Modells entsprach.

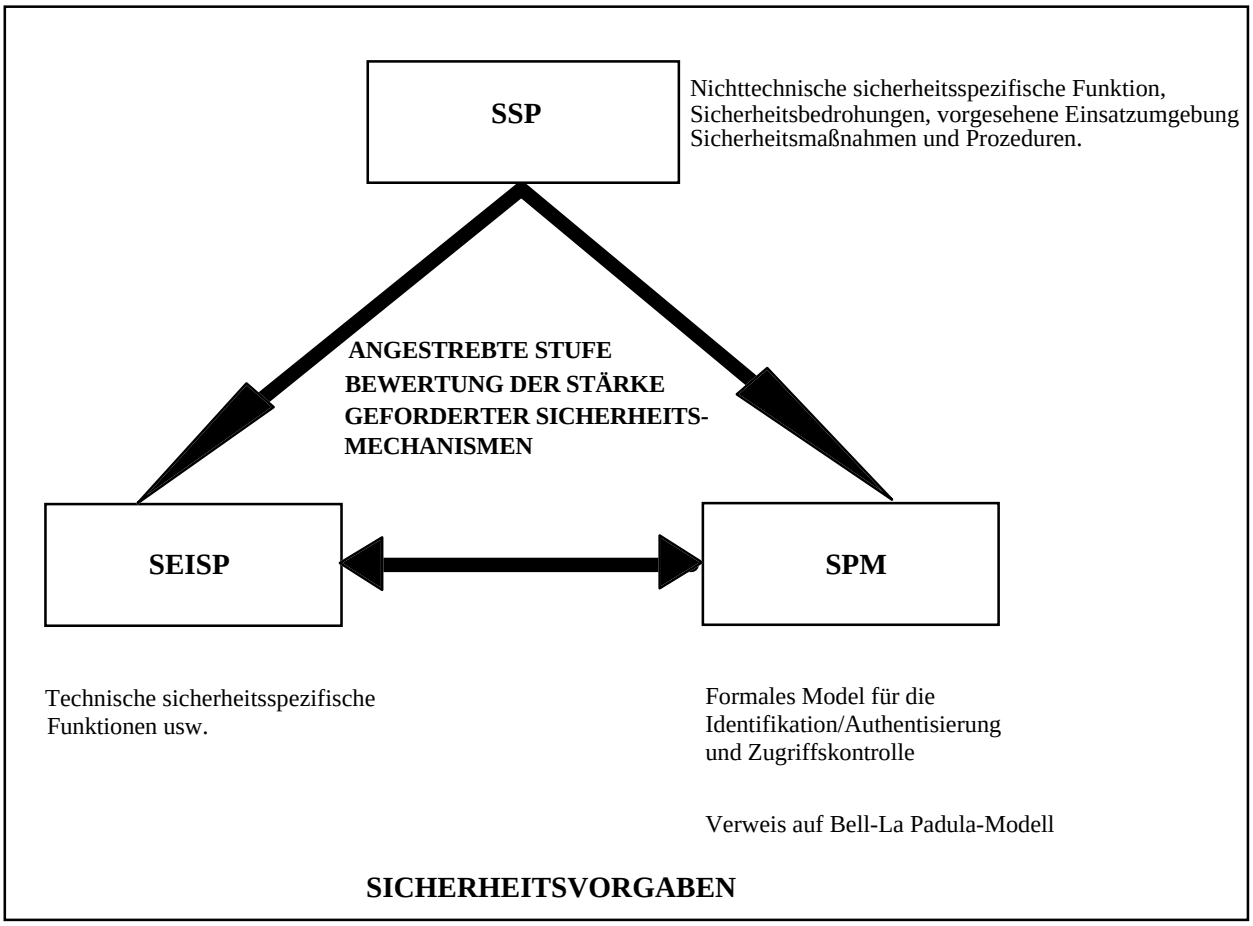
5.3.10 Das SPM wurde validiert durch

a) Lesen und umfassendes Verstehen des Dokuments;

b) Verstehen und unabhängiges Prüfen der Nachweise für Prädikatenvorbedingungen (um sicherzustellen, daß Zustandsübergänge wirklich sicher erfolgten);

c) Validieren, daß der Anfangszustand sicher war.

5.3.11 Da die ITSEC-Korrektheitskriterien für Anforderungen nicht eindeutig erfüllt wurden, konnte eine "nichtbeurteilende" Entscheidung ausgesprochen werden. Diese nichtbeurteilende Entscheidung wurde später in eine *akzeptierende* Entscheidung umgewandelt, nachdem die Evaluatoren die semiformale Spezifikation für die vom Antragsteller in einer späteren Phase der Evaluation zur Verfügung gestellten Anforderungen an Beweissicherung, Protokollauswertung und Wiederaufbereitung überprüfen konnten.



Legende:
SSP – System Security Policy = System-Sicherheitspolitik
SEISP – System Electronic Information Security Policy = IT-Sicherheitspolitik
SPM – Formal Security Policy Model = Formales Sicherheitsmodell

Abbildung 5.3.1 Schematischer Aufbau der Dokumentation

Kapitel 5.4 Beispiel 3, Prüfung der Architektur auf Korrektheit (E4)

Einleitung

5.4.1 Dieses Beispiel behandelt die Aufgaben des Evaluators in der Konstruktionsphase 2 des Entwicklungsprozesses – Architekturentwurf. Der EVG war ein verteiltes System, das zahlreiche Komponenten umfaßte und unmittelbar vor Veröffentlichung der ITSEC entwickelt worden war. Es zeigte sich, daß die gelieferte Gesamtdokumentation die Anforderungen von E4 voll und ganz erfüllte, wobei einige Dokumente den Anforderungen höherer Stufen entsprachen. In den Sicherheitsvorgaben für den EVG war die Funktionalitätsklasse F-B3 mit geringen Zusatzfunktionen festgelegt.

Relevante Evaluationsbeiträge

5.4.2 Als Beiträge zu dieser Arbeit standen die Sicherheitsvorgaben und der Architekturentwurf für den EVG zur Verfügung.

5.4.3 In Abbildung 5.4.1 ist der Aufbau der den Evaluatoren von den Entwicklern zur Verfügung gestellten Dokumentation schematisch dargestellt. Die Evaluatoren ermittelten, welche Teile der Gesamt-dokumentation den Architekturentwurf enthielten. Der Architekturentwurf ist in Abbildung 5.4.1 dargestellt.

5.4.4 Die Architektur umfaßte folgendes:

a) Funktionale Systemspezifikation (System Functional Specification, SFS);

b) Formale Sicherheitsspezifikation (Formal Security Specification, FSS);

c) Sicherheitsarchitekturdokument (Security Architecture Document, SAD).

5.4.5 Der EVG wurde unter Verwendung der SSADM entwickelt. Die SFS bestand aus den Ergebnissen der SSADM-Stufen 1 bis 3. Die SSADM-Ergebnisse umfaßten folgendes:

a) Datenflußdiagramme (DFDs);

b) DFD-Prozeßbeschreibungen;

c) Beschreibungen externer Einheiten (in den DFDs);

d) einen E/A-Katalog;

e) Logische Datenstruktur (LDS);

f) Einheitenbeschreibungen;

g) ein Datenverzeichnis;

h) eine Querverweisliste Einheiten/Datenspeicher;

i) einen Ereigniskatalog;

j) eine Ereignis-Einheit-Matrix;

k) Diagramme von Entity-Life-Protokollen (Entity Life History, ELH).

5.4.6 Die SFS bildete den logischen Entwurf, durch den die funktionalen Anforderungen aus der Systeman-forderungsspezifikation (System Requirements Specification, SRS) mit der IT-Sicherheitspolitik (System Electronic Information Security Policy, SEISP) verbunden wurden. Ein Teil der SFS, die logische Mensch-Maschine-Schnittstelle (Logical Man-Machine Interface, MMI(L)), stellte die Anwendersicht des Systems (durch Zustandsübergangsdiagramme) für alle Anwendertypen dar. Die SFS ließ die materiellen Aspekte der MMI wie etwa den Bildschirmaufbau unberücksichtigt.

5.4.7 Ein Teil der SFS, die externen Schnittstellenspezifikationen (External Interface Specifications, EIS), definierte die externen Schnittstellen (zu externen Systemen und vorhandenen eingebetteten Systemen). Die EIS skizzierten die mit dem Systemnetz zu verbindenden externen und eingebetteten Systeme und enthielten Detailangaben zu den Übertragungsschnittstellen. Die für die Übertragungs-schnittstellen relevanten sicherheitsspezifischen Funktionen wurden explizit angegeben.

5.4.8 Es ist zu beachten, daß MMI(L) und EIS als getrennte Dokumente erstellt wurden. Für die Beange der Evaluation wurden sie jedoch als Bestandteil der Funktionsspezifikation des Systems betrachtet.

5.4.9 Die FSS umfaßte eine in 'Z' geschriebene formale Spezifikation, die Einzelheiten über eine Teilmenge der sicherheitsspezifischen Funktionen enthielt, und zwar die obligatorische Zugriffs-kontrolle, die Beweissicherung und die Protokollauswertung. Die Spezifikation enthielt eine textliche Erweiterung dieser Teilmenge. Zwischen SFS und FSS gab es eine Übereinstimmung. Obwohl dies auf E4 nicht gefordert war, diente die FSS zur Erläuterung, welche in der SFS spezifizierten Ereignisse sicherheitsrelevant waren.

5.4.10 Das SAD bot einen Überblick über die vorgesehene EVG-Konfiguration und beschrieb auf hohem Abstraktionsniveau, wie die Sicherheitspolitik im Rahmen dieser Konfiguration implementiert werden soll. Es lieferte eine Beschreibung, wie die sicherheitsspezifischen Funktionen erfüllt würden. Es beschrieb ebenfalls, wie die Anforderungen an die Trennung erfüllt würden.

5.4.11 Das SAD präzisierte die Vorgehensweisen und Verfahren, die auf den Lebenszyklus von Entwurf und Entwicklung hinsichtlich sicherheitsspezifischer, sicherheitsrelevanter und nicht sicherheitsrelevanter Teile des EVG anzuwenden sind, wie etwa

a) Qualitätssicherungsmaßnahmen;

b) Methoden für den Feinentwurf;

c) Vorschriften für die Abbildbarkeitsdokumentation;

d) funktionale Tests;

e) Konfigurationsmanagement;

f) Änderungskontrolle.

5.4.12 Diese Punkte wurden extrahiert und als Beitrag für andere Evaluationstätigkeiten verwendet (die nicht Bestandteil dieses Beispiels sind):

a) Feinentwurf (Punkt (b), als Hintergrundinformation);

b) Implementierung (Punkt (d), da hier die anzuwendende Teststrategie beschrieben wurde und insbesondere dargelegt wurde, welche Testmaßnahmen welchen Teil abdecken würden und wieso die Abdeckung ausreichen würde);

c) Konfigurationskontrolle (Punkte (a), (b) und (f), die das Konfigurationsmanagementsystem im Gesamtzusammenhang der Qualitätssicherungsmaßnahmen erläuterten, Werkzeuge für das Konfigurationsmanagement nannten und ihre Verwendung erläuterten und das Abnahmeverfahren und die für die Durchführung von Änderungen erforderliche Autorisierung erklärten).

5.4.13 Eine der Systemkomponenten war eine sicherheitsspezifische und sicherheitsrelevante Workstation. Das SAD

a) lieferte einen Überblick über die Architektur der Workstation;

b) nannte die sicherheitsspezifischen Komponenten (wie etwa die Schnittstelle zum Netz) und die sicherheitsrelevanten Komponenten.

5.4.14 Auf sicherheitsspezifische Funktionen wurde in der SEISP, der SFS (Prozeßbeschreibungen) und der FSS (Texterweiterung) Bezug genommen. Die Verweise wurden in getrennten Abbildbarkeitsdoku-menten verknüpft, die folgende Möglichkeiten boten:

a) Vorwärtsabbildbarkeit von den sicherheitsspezifischen Funktionen der SEISP bis zu den SFS- und FSS-Funktionen;

b) Rückwärtsabbildbarkeit von der SFS- und FSS-Funktionalität bis zu den sicherheitsspezifischen Funktionen der SEISP.

5.4.15 Die Abbildbarkeitsdokumente lieferten Begründungen für nicht nachvollziehbare Aussagen in SFS und FSS.

Durchgeführte Arbeiten

5.4.16 Alle Evaluationsbeiträge auf Architekturentwurfsebene wurden dahingehend untersucht, ob die ITSEC-Anforderungen an Inhalt, Form und Nachweis erfüllt worden waren. Insbesondere wurde überprüft,

a) ob alle vorgesehenen externen Schnittstellen ausgewiesen und entsprechende kryptographische Mechanismen und Mechanismen der zeitlichen Trennung in Betracht gezogen worden waren (in EIS und SAD);

b) ob alle Hardware- und Firmware-Komponenten ausgewiesen waren und ob die Funktionalität der unterstützenden Schutzmechanismen angemessen war, beispielsweise ob in der Work-station hinreichende Wiederaufbereitungsmöglichkeiten für den gesamten Speicher vorhanden waren (im SAD);

c) ob die Trennung von sicherheitsspezifischen, sicherheitsrelevanten und anderen Komponenten durchführbar und sinnvoll war (in SAD und SFS).

5.4.17 Die projektspezifischen Vorgehensweisen der SSADM-Dokumentation wurden übernommen. Sie wurden dahingehend untersucht, ob die Evaluatoren eine genaue Kenntnis von Syntax und Semantik der semiformalen Notation besaßen. Um sicherzustellen, daß die Vorgehensweisen für das Projekt korrekt implementiert waren, wurde die SFS mit den Dokumentationsstandards verglichen.

5.4.18 Die Überprüfung des Abbildbarkeitsnachweises beinhaltete eine manuelle Verifizierung der SFS und der FSS anhand der SEISP. Bei der Verifizierung wurde die Einbringung nicht nachvollziehbarer Funktionalität berücksichtigt, wodurch gewährleistet wurde, daß diese Funktionalität hinreichend begründet war.

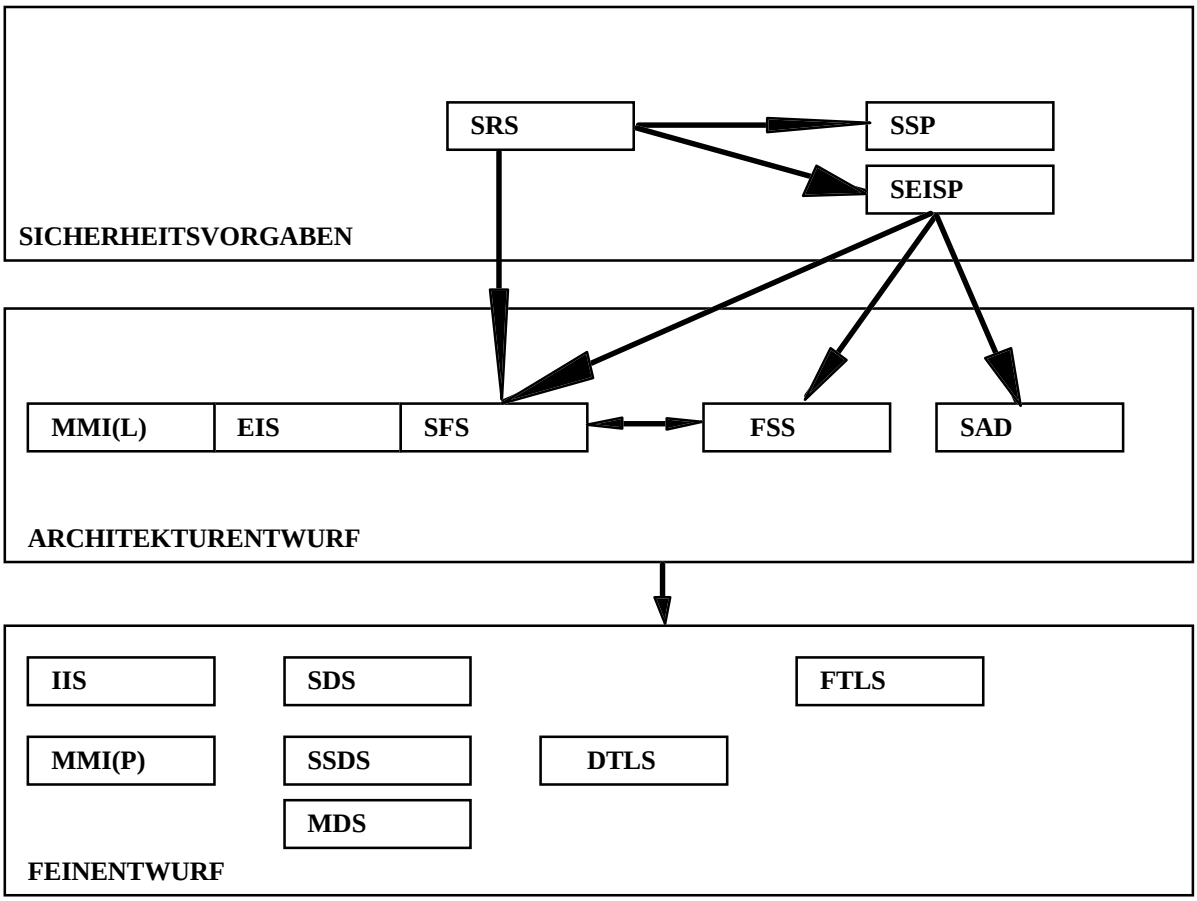
5.4.19 Die Evaluatoren stellten fest, daß die SSADM-Dokumentation in der SFS die sicherheitsspezifische, sicherheitsrelevante und sonstige Funktionalität nicht logisch trennte, und verfaßten einen Mängel-bericht. Der Antragsteller prüfte diesen Aspekt und zog einen an der eigentlichen Evaluation nicht beteiligten Berater hinzu, der einen praktischen Ansatz zur Lösung des Problems empfehlen sollte.

5.4.20 Die Sicherheitsberater stellten fest, daß die im Ereigniskatalog beschriebenen Ereignisse nicht als sicherheitsrelevant oder nichtsicherheitsrelevant eingestuft worden waren. Durch eingehende Befassung sowohl mit der FSS als auch mit den Ereignisursachen konnte der Berater entscheiden, welche Ereignisse sicherheitsrelevant waren.

5.4.21 Laut Empfehlung des Beraters hätte sich für den Entwickler als geeigneterer Lösungsansatz die Ausweisung der Sicherheitsfunktionalität als Prozeß innerhalb der Top-Level-DFD angeboten. Diese hätte dann in die sicherheitsspezifischen Funktionen (wie etwa Zugriffskontrolle, Beweissicherung usw.) verfeinert werden können und hätte so eine deutliche logische Trennung der Funkionalität bewirkt und die Unabhängigkeit der sicherheitsspezifischen Komponenten klar zum Ausdruck gebracht. Der Berater machte jedoch geltend, auf Stufe E4 sei die Anwendung der SSADM innerhalb der SFS völlig korrekt, und wenn alle DFD-Prozesse auf niedrigerer Stufe entweder als sicherheitsspezifisch oder als nichtsicherheitsspezifisch eingestuft seien, sei die Beschreibung der materiellen Trennung im SAD hinreichend, um die Erfüllung der Evaluationskriterien durch den Architekturentwurf zu gewährleisten.

5.4.22 Die Evaluatoren schlossen sich dieser Argumentation an. Die Prozeßkategorisierung wurde anschließend der ITSEF zur Verfügung gestellt, woraufhin die Evaluation fortgesetzt werden konnte.

5.4.23 Da die ITSEC-Korrektheitskriterien für die Architektur erfüllt wurden, konnte eine *akzeptierende* Entscheidung ausgesprochen werden.



Legende:

SRS – System Requirements Specification (Spezifikation für Systemanforderungen)

SSP – System Security Policy (System-Sicherheitspolitik)

SEISP – System Electronic Information Security Policy (IT-Sicherheitspolitik)

SFS – System Functional Specification (Funktionale System-Spezifikation) (SSADM Stufen 1–3)

IIS/EIS – Internal/External Interface Specifications (Spezifikationen für interne/externe Schnittstellen)

MMI(L) – Logical Man-Machine Interface (Logische Mensch-Maschine-Schnittstelle)

FSS – Formal Security Specification (Formale Sicherheitsspezifikation)

SAD – Security Architectural Document (Sicherheitsarchitektur-Dokument)

MMI(P) – Physical Man-Machine Interface (Physische Mensch-Maschine-Schnittstelle)

SDS, SSDS, MDS, FTLS, DTLS – Feinentwurf

Abbildung 5.4.1 Schematischer Aufbau der Dokumentation

Kapitel 5.5 Beispiel 4, Prüfung des Entwurfs auf Korrektheit (E2)

Einleitung

5.5.1 Dieses Beispiel behandelt die Aufgaben des Evaluators in der Konstruktionsphase 3 des Entwicklungsprozesses – Feinentwurf. Der EVG war ein kundenspezifisches System. In den Sicherheitsvorgaben für den EVG war die Funktionalitätsklasse F-DI festgelegt.

5.5.2 Die Evaluation sollte begleitend zur Systementwicklung durchgeführt werden, was bedeutete, daß die meisten Evaluationsbeiträge anfangs nur in Entwurfsform vorlagen. Vor der Evaluation wurde eine ITSEF beauftragt, die Entwurfsdokumente auf Einhaltung der Anforderungen für E2 zu überprüfen.

5.5.3 Aus der Erstanalyse wurde deutlich, daß der EVG die Vorgaben der Evaluationsstufe in vielen Bereichen nicht würde erfüllen können. Der Antragsteller wurde daraufhin informiert, welche Schritte zu unternehmen seien, damit eine erfolgreiche Evaluation gewährleistet sei.

Relevante Evaluationsbeiträge

5.5.4 Als Beiträge zu dieser Arbeit standen die Architekturentwurfsdokumentation (Entwurf Stufe 1) und die Feinentwurfsdokumentation für den EVG zur Verfügung.

5.5.5 Die Feinentwurfsdokumentation umfaßte folgendes:

a) Subsystem-Entwurfsspezifikationen (Entwurf Stufe 2);

b) Subsystem-Schnittstellenspezifikationen (Entwurf Stufe 2);

c) Implementierungsspezifikationen (Entwurf Stufe 3).

Durchgeführte Arbeiten

5.5.6 Der Aufbau der EVG-Stufen wurde hinsichtlich der **Darstellung** anhand der Kriterien für ein klares, hierarchisches Beziehungsgefüge bewertet. Es zeigte sich, daß die Subsystem-Schnittstellenspezifikationen als Entwurfsdokument der Stufe 2 verfaßt waren, daß sie jedoch Informationen enthielten, die aus der Entwurfsarbeit der Stufe 3 stammten. Die Form der Informationen entsprach somit nicht den Kriterien der Evaluationsstufen, während der Informationsgehalt als angemessen bewertet wurde.

5.5.7 Die Beziehung zwischen den in der Dokumentation des Architekturentwurfs ausgewiesenen sicherheitsspezifischen Funktionen und den in den Subsystem-Entwurfsspezifikationen dargelegten Funktionen wurde durch manuelle Quervergleiche geprüft, um sicherzustellen,

a) daß alle sicherheitsspezifischen Funktionen im Feinentwurf enthalten waren;

b) daß die Intention des Architekturentwurfs im Feinentwurf korrekt beibehalten wurde.

5.5.8 Zur Überprüfung der Beziehung zwischen den in den Entwurfsspezifikationen der Subsysteme dargelegten sicherheitsspezifischen und sicherheitsrelevanten Funktionen und den sicherheitsspezifischen und sicherheitsrelevanten Komponenten der Implementierungsspezifikationen wurde eine Matrix für die Abbildbarkeit der Anforderungen erstellt. Dabei wurden einige Fehler festgestellt, und zwar insbesondere folgende:

a) Komponenten in den von den Evaluatoren als sicherheitsrelevant ausgewiesenen Implementierungsspezifikationen waren in den Subsystem-Entwurfsspezifikationen nicht aufgeführt (d. h. fehlende sicherheitsrelevante Funktionalität in den Darstellungen der höheren Stufen);

b) in den Entwurfsspezifikationen der Subsysteme aufgeführte sicherheitsspezifische Funktionen (z. B. Wiederaufbereitung) waren nicht in den Implementierungsspezifikationen enthalten.

5.5.9 Die Spezifikationen sämtlicher sicherheitsspezifischen und sicherheitsrelevanten Mechanismen und Komponenten wurden auf ausreichende Dokumentierung überprüft. Dabei wurde festgestellt, daß die zur Implementierung der sicherheitsspezifischen und sicherheitsrelevanten Komponenten benötigten Informationen nicht immer vorhanden waren. Beispiele sind

a) die unzureichende Detaillierung hinsichtlich Anwendung und Inhalt wichtiger Datenstrukturen und hinsichtlich der bei fehlgeschlagener Parametervalidierung zu ergreifenden Maßnahmen;

b) fehlende externe Verweise (z. B. Angabe verwendeter Bibliotheken und externer Systemkomponenten);

c) umgangssprachliche Beschreibungen sicherheitsrelevanter Funktionen, die nicht mit den entsprechenden Beschreibungen im Pseudocode übereinstimmen.

5.5.10 Die Schnittstellen zu sicherheitsspezifischen und sicherheitsrelevanten Komponenten wurden anhand der Dokumente für die Systemschnittstellenspezifikation manuell überprüft, und zwar dahingehend, ob alle Schnittstellen aufgeführt und korrekt angegeben waren. Auf Fehler wurde hier besonders geachtet, da für den Programmierer die Dokumente über die Systemschnittstellen die maßgebliche Richtschnur für die Anwendung der sicherheitsspezifischen und sicherheitsrelevanten Funktionen bildeten.

5.5.11 Die oben aufgeführten Fälle, in denen die Darstellung des EVG-Feinentwurfs nicht mit den Kriterien für die Evaluationsstufe übereinstimmte, waren in erster Linie durch die Evaluation des EVG anhand der in Entwurfsform vorliegenden Darstellungen bedingt. Die Evaluatoren stellten allerdings auch fest, daß der Feinentwurf nicht in völliger Übereinstimmung mit den Anforderungen von E2 abgefaßt wurde, und legten entsprechende Mängelberichte vor.

5.5.12 Die Evaluatoren konnten in dieser Phase der Evaluation keine akzeptierende Entscheidung für den Feinentwurf fällen. Da die Evaluatoren nur in Entwurfsform vorliegende Darstellungen des EVG prüfen konnten, wurde eine *nichtbeurteilende* Entscheidung ausgesprochen.

5.5.13 Endversionen der Feinentwurfsdarstellungen wurden vor Abschluß der Evaluation nochmals untersucht, woraufhin festgestellt wurde, daß die genannten Probleme beseitigt waren. Daraufhin wurde eine *akzeptierende* Entscheidung ausgesprochen.

Kapitel 5.6 Beispiel 5, Prüfung der Implementierung auf Korrektheit (E2)

Einleitung

5.6.1 Dieses Beispiel behandelt die Aufgaben des Evaluators in Konstruktionsphase 4 des Entwicklungsprozesses – Implementierung.

5.6.2 Der EVG war ein kundenspezifisches System. In den Sicherheitsvorgaben für den EVG war die Funktionalitätsklasse F-DI festgelegt.

Relevante Evaluationsbeiträge

5.6.3 Als Beiträge zu dieser Arbeit dienten

a) die Testdokumentation:

- Spezifikationen für Pakettests;
- Abnahmetestplan;
- Spezifikation für Aktivitäts-Schnittstellentests;
- Spezifikation für die Abnahme von Systemtests;
- Spezifikation für die Abnahme von Systemfunktionstests;
- Testablaufpläne;
- Testergebnisdateien;
- Beschreibung der Testwerkzeuge und des Benutzerhandbuchs;

b) eine Bibliothek von Testprogrammen und -werkzeugen, die von den Entwicklern zum Testen des EVG verwendet wurden.

5.6.4 Das Testen des EVG erfolgte in zwei Phasen:

a) Pakettests;

b) Abnahmetests.

5.6.5 Die Abnahmetests umfaßten folgende Phasen:

a) Aktivitäts-Schnittstellentests: Prüfung, ob sich die integrierten Komponenten wie im Entwurf festgelegt verhalten und ob die Integrität gemeinsam genutzter Daten erhalten bleibt;

b) Funktionstests: Prüfung, ob die integrierten Komponenten eine Systemdienstleistung wie im Entwurf festgelegt ausführen und ob die Anforderungen des Anwenders erfüllt werden;

c) Systemtests: eine vollständige Integration von Hardware und Software um nachzuweisen, daß das System als Ganzes in Übereinstimmung mit dem Systementwurf arbeitet und die Anforderungen des Anwenders erfüllt.

Durchgeführte Arbeiten

5.6.6 Die Bewertung der Korrektheit des EVG anhand der E2-Kriterien für die Implementierung erfolgte durch folgende Schritte für jede der oben angegebenen Phasen und Abschnitte:

a) Überprüfen der Testdokumentation;

b) Beobachten der Tests;

c) Überprüfen von Testberichten;

d) Wiederholen ausgewählter Tests.

5.6.7 Die Teststrategie des Entwicklers für den EVG entsprach einem kontrollierten Top-down-Ansatz, der alle in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen abdeckte. Bei den auf der untersten Stufe durchgeführten Tests, denen die Komponenten des EVG unterzogen wurden, handelte es sich nicht um Tests der einzelnen Module, sondern um Pakettests (als Paket wird eine Auswahl von Modulen bezeichnet, die eine zusammengehörige Menge von Dienstleistungen erbringen). Für E2 ist dies jedoch ausreichend, da nur nachzuweisen ist, daß die *Tests alle sicher-heitsspezifischen Funktionen ... umfassen.*

5.6.8 Die Zielsetzung des Entwicklers bei den Pakettests bestand darin, alle im Entwurf des Pakets bezeichneten Funktionsstränge durch hinreichende Tests abzudecken (bestätigt durch Verwendung eines In-line-Testroutinecodes, der während der Kompilierung ausgewählt werden konnte), um so eine vollständige Gesamtabdeckung zu erreichen. Die Bewertung der Integrationstests ergab jedoch, daß diese Zielsetzung nicht erfüllt wurde.

5.6.9 Es wurde festgestellt, daß die Abnahmetestdokumentation zu jedem Test eine ausführliche Beschrei-bung, einschließlich Zweck, Prozeduren und Ressourcen, enthielt.

5.6.10 Der Abnahmetestplan enthielt eine Anforderungs-Abbildbarkeitsmatrix (Requirements Traceability Matrix, RTM) auf hoher Ebene, in der Testphasen auf Anwenderanforderungen abgebildet wurden. Die einzelnen Abnahmetestspezifikationen enthielten jeweils eine detailliertere RTM. Die RTM wurden manuell dahingehend überprüft, ob alle sicherheitsspezifischen Funktionen hinreichend abgedeckt waren. Dabei wurde festgestellt, daß die RTM unvollständig waren.

5.6.11 Um sicherzustellen, daß die Testverfahren eingehalten wurden, wurde die Durchführung der Abnahmetests für einige der sicherheitsrelevanten Funktionen persönlich beobachtet. Dabei wurde auch um Wiederholung bereits abgeschlossener Tests ersucht.

5.6.12 Um sicherzustellen, daß alle Tests erfolgreich abgeschlossen worden waren, und um Schwächen bei der Entwicklung des EVG sichtbar zu machen, wurden die Abnahmetestberichte überprüft. Dabei wurden die folgenden häufig auftretenden Probleme festgestellt:

a) Implementierungsmodule, die Pakettests (scheinbar) erfolgreich absolviert hatten, ließen sich auf nachfolgenden Teststufen nicht mehr kompilieren;

b) der unzureichende Testumfang bei den Pakettests führte zu Fehlern auf nachfolgenden Teststufen;

c) es traten Systemabstürze mit unbestimmten Fehlerstatuscodes auf.

5.6.13 Diese Probleme wiesen auf Schwächen im Entwicklungsprozeß hin. Die Evaluatoren verfaßten einen einzelnen Mängelbericht, der alle diese Aspekte abdeckte. Der Entwickler konnte später nachweisen, daß man diese Probleme behoben hatte.

5.6.14 Die Evaluatoren legten weitere Tests für die Fehlersuche fest, die sie aufgrund der Komplexität der Testroutinen jedoch nicht selbst durchführen konnten. Um dieses Problem zu lösen, erhielt der Entwickler Testspezifikationen für zusätzlich durchzuführende Tests. Diese wurden anschließend von den Evaluatoren persönlich beobachtet.

5.6.15 Da die ITSEC-Korrektheitskriterien für die Implementierung erfüllt wurden, konnte eine *akzeptierende* Entscheidung ausgesprochen werden.

Kapitel 5.7 Beispiel 6, Prüfung des Betriebs auf Korrektheit (E2)

Einleitung

5.7.1 Dieses Beispiel gliedert sich in vier Unterbeispiele (6(a), 6(b), 6(c) und 6(d)), die jeweils einen Aspekt der Betriebsdokumentation oder der Betriebsumgebung betreffen.

Beispiel 6(a) – Prüfung der Unteraktivität Benutzerdokumentation (E2.27)

Einleitung

5.7.2 Dieses Unterbeispiel behandelt die Aufgaben des Evaluators zu Aspekt 1 der Betriebsdokumentation – Benutzerdokumentation. Der EVG war ein System. In den Sicherheitsvorgaben für den EVG war die Funktionalitätsklasse F-C2 festgelegt.

5.7.3 Im Unterabschnitt *Strenge und Tiefe des Nachweises* am Ende dieses Beispiels wird die zunehmende Strenge der Benutzerdokumentation beim Übergang von *darlegen/angeben* über *beschreiben* zu *erklären* interpretiert.

Relevante Evaluationsbeiträge

5.7.4 Als Beitrag zu dieser Arbeit dienten die Sicherheitsvorgaben und die Benutzeranleitungen für den EVG.

Durchgeführte Arbeiten

5.7.5 Um eine vollständige und konsistente Abdeckung der für den Endanwender relevanten sicherheitsspezifischen Funktionen zu gewährleisten, wurden die Benutzeranleitungen auf die sicherheitsspezifischen Funktionen in den Sicherheitsvorgaben abgebildet. Systemverwalterfunktionen wie etwa die Protokollauswertung wurden nicht als relevant betrachtet.

5.7.6 Die Evaluatoren führten eine Reihe von Besichtigungen vor Ort durch. Dadurch konnten sie sich einen genauen Einblick in die Funktionsweise des Systems verschaffen. Der Betrieb des Systems konnte anschließend mit den Beschreibungen in den Benutzeranleitungen verglichen werden (um ihre Korrektheit zu bewerten), und verbliebene Unklarheiten über den Zweck der Anleitungen ließen sich klären.

5.7.7 In den Benutzerhandbüchern wurde die Verwendung der Systemmenüs erläutert. Die Systemmenüs wurden auf korrekte Übereinstimmung mit den Benutzerhandbüchern überprüft.

5.7.8 Um sicherzustellen, daß mögliche Sicherheitslücken den Benutzern nicht aufgezeigt wurden, wurden die Benutzerhandbücher von den Evaluatoren gründlich überprüft.

Strenge und Tiefe des Nachweises – Einleitung

5.7.9 Dieser Unterabschnitt zeigt an einem Beispiel, wie sich die Anforderungen an Inhalt, Form und Nachweis auf den einzelnen Stufen jeweils ändern, wenn die Verben *darlegen/angeben* (state), *beschreiben* (describe) und *erklären* (explain) in den ITSEC verwendet werden, und führt hierzu positive und negative Aspekte an. Das gewählte Beispiel soll darauf hinweisen, wie gefährlich es ist, bei der Interpretation dieses ITSEC-Konzepts den Kontext unberücksichtigt zu lassen.

5.7.10 Die folgenden Unterschiede in den Anforderungen an Inhalt, Form und Nachweis in der Benutzerdokumentation werden in den ITSEC detailliert beschrieben:

a) Auf E1 und E2 muß die *Benutzerdokumentation ... die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind,* ***darlegen***, und die *Benutzerdokumentation muß* ***darlegen****, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt*.

b) Auf E3 und E4 muß die *Benutzerdokumentation ... die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind,* ***beschreiben***, und die *Benutzerdokumentation muß* ***beschreiben****, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt*.

c) Auf E5 und E6 muß die *Benutzerdokumentation ... die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind,* ***erklären***, und die *Benutzerdokumentation muß* ***erklären****, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt*.

5.7.11 In Absatz 0.12 der ITSEC werden *darlegen/angeben*, *beschreiben* und *erklären* wie folgt definiert: *Darlegen/Angeben bedeutet, daß die relevanten Fakten zur Verfügung gestellt werden müssen; beschreiben bedeutet, daß die Fakten zur Verfügung gestellt werden müssen und daß ihre relevanten Eigenschaften aufgezählt werden müssen; erklären bedeutet, daß die Fakten zur Verfügung gestellt, ihre relevanten Eigenschaften aufgezählt und Begründungen gegeben werden müssen.*

5.7.12 Der erforderliche Aufwand für die Überprüfung, ob die gelieferten Informationen allen Anforde-rungen an Inhalt, Form und Nachweis genügen, ändert sich daher mit der Evaluationsstufe.

5.7.13 In den Sicherheitsvorgaben für ein System könnte eine sicherheitsspezifische Funktion definiert sein, mit der sich die Zahl der Anmeldeversuche an einem Terminal begrenzen läßt. In diesem Fall wären folgende Anforderungen möglich:

a) Das System darf nicht mehr als drei fehlgeschlagene Anmeldeversuche hintereinander zulassen;

b) wenn drei aufeinanderfolgende Anmeldeversuche hintereinander fehlschlagen, muß der Bildschirm dunkelgeschaltet und die Tastatur gesperrt werden;

c) das System muß alle fehlgeschlagenen Anmeldeversuche protokollieren.

5.7.14 Die Auswirkungen der verschiedenen Evaluationsstufen werden im folgenden erläutert.

Interpretation auf E1 und E2

5.7.15 Auf E1 und E2 könnten die Benutzeranleitungen darlegen, daß der Benutzer nur drei Versuche hat, um sich an einem Terminal anzumelden, und daß nach drei Fehlversuchen der Bildschirm dunkelgeschaltet, die Tastatur gesperrt und jeder Fehlversuch vom System protokolliert wird. Dies ist eine sinnvolle Interpretation auf E1 und E2.

5.7.16 Die auf E1 und E2 durchgeführten Arbeiten wären ebenso detailliert wie im obigen Unterabschnitt *Durchgeführte Arbeiten* beschrieben.

Interpretation auf E3 und E4

5.7.17 Auf E3 und E4 könnten die Benutzeranleitungen beschreiben, daß ein Benutzer nur drei Anmeldeversuche hat und daß der Anmeldeprozeß nach drei Fehlversuchen

a) den Terminalbildschirm durch Senden einer Steuersequenz dunkelschaltet (zum Beispiel);

b) die Tastatur sperrt, indem ihr Eintrag in der Terminal-Konfigurationsdatei deaktiviert und ihre interne Terminaltabelle aktualisiert wird (zum Beispiel);

c) eine Nachricht in das **Protokoll** schreibt, die für den betreffenden Zwischenfall Stufe, Datum, Uhrzeit, Zwischenfalltyp (d. h. fehlgeschlagener Anmeldeversuch), Terminal-ID und eingegebenen Anwendernamen angibt. Eine Nachricht könnte beispielsweise lauten:

```
"WARNING: 12/08/91: 0935: LOGON FAILURE ON TTY03 BY J_SMITH".
("WARNUNG:  08.12.91:  0935:  FEHLGESCHLAGENER  ANMELDEVERSUCH  AN  TERM03  DURCH
J_SMITH".)
```

5.7.18 In diesem Fall sollen die Evaluatoren darauf hinweisen, daß die Punkte (a) und (b) Einzelheiten zur Implementierung enthalten, die für die Betriebsdokumentation nicht relevant sind. Punkt (c) enthält Angaben, die für eine Benutzeranleitung nicht relevant sind, die jedoch als *Beschreibung* in einem Systemverwalter-Handbuch geeignet wären.

5.7.19 Stattdessen soll die Benutzeranleitung den Prozeß der Anmeldung und die Vorgänge beschreiben. Beispiele sind:

a) Um sich beim System anzumelden, muß der Anwender zunächst durch Drücken einer Taste das Betriebssystem verständigen.

b) Das System fragt dann den Anwendernamen ab; die Eingabe wird am Bildschirm angezeigt.

c) Anschließend fragt das System das Paßwort des Anwenders ab; diese Eingabe wird nicht angezeigt.

d) Wenn Anwendername und Paßwort keine gültige Kombination bilden, zeigt das System die Nachricht "ERROR: PLEASE TRY AGAIN" (FEHLER: BITTE EINGABE WIEDER-HOLEN).

e) Das System fragt anschließend den Anwendernamen erneut ab (Schritt (b)). Drei Versuche sind zulässig. Hat der Anwender beim dritten Versuch keinen Erfolg, wird der Bildschirm dunkelgeschaltet und die Tastatur gesperrt. Das Terminal kann für fünf Minuten (oder einer anderen vom Systemverwalter festgesetzten Zeitspanne) nicht benutzt werden.

f) Nach erfolgreicher Anmeldung zeigt das System das Befehlsmenü für den Anwender an.

Interpretation auf E5 und E6

5.7.20 Auf E5 und E6 könnten die Benutzeranleitungen zusätzlich zu den oben genannten Informationen folgendes erklären:

a) Durch Dunkelschalten des Bildschirms wird der Eindruck einer Funktionsstörung erweckt, damit der Hacker keine weiteren Informationen erhält;

b) durch Sperren der Tastatur wird verhindert, daß der Hacker weitere Paßwörter ausprobieren kann;

c) durch Protokollieren des Ereignisses bekommt der Systemverwalter einen Warnhinweis, daß ein bestimmtes Terminal (und ebenso möglicherweise ein bestimmtes Anwenderkonto) angegriffen wird.

5.7.21 Auch hier sollen die Evaluatoren bemängeln, daß diese Informationen für eine Benutzeranleitung nicht relevant sind, obwohl sie an einen Sicherheitsadministrator gerichtete Begründungen des

Entwicklers enthalten. Man beachte auch den möglichen Kritikpunkt, daß in diesem Beispiel einem potentiellen Hacker wertvolle Informationen geliefert würden.

5.7.22 Absatz 5.7.19 bildet einen sinnvollen Ausgangspunkt für die Erläuterung des Anmeldevorgangs. Zusätzlich ist ein Absatz etwa wie folgt erforderlich:

> *Der Zweck dieser Vorgehensweise bei der Anmeldung ist, dem System zu bestätigen, daß Sie derjenige sind, für den Sie sich ausgeben; dadurch soll vor allem verhindert werden, daß sich eine andere Person an Ihrer Stelle im System anmelden kann. Die Zahl der Anmeldeversuche ist auf 3 beschränkt worden, damit zwar Sie selbst bei der Eingabe Ihres Paßworts einen echten Schreibfehler machen dürfen, ein unberechtigter Anwender aber nicht durch systematisches Probieren Ihr Paßwort erraten kann. Gelingt die Anmeldung selbst nach dreimaligem Versuch nicht, wird automatisch der Systemverwalter verständigt.*

5.7.23 Zusätzlich zu den auf E3 und E4 durchgeführten Arbeiten würden die Begründungen auch anhand der Erläuterungen der Sicherheitsvorgaben für Sicherheitsziele, Bedrohungen und sicherheitsspezifische Funktionen überprüft werden.

5.7.24 Es ist zu beachten, daß die Entwickler je nach der Zielgruppe, für die die Benutzeranleitungen bestimmt sind, ausführlichere Informationen zur Verfügung stellen können als in den ITSEC gefordert. Beispielsweise können die Entwickler auf E1 Erklärungen für unerfahrene Anwender mitliefern; dies kann in einen Entwicklungsvertrag als Bedingung aufgenommen werden.

Beispiel 6(b) – Prüfung der Unteraktivität Systemverwalter-Dokumentation (E2.30)

Einleitung

5.7.25 Dieses Unterbeispiel behandelt die Aufgaben zu Aspekt 2 der Betriebsdokumentation – Systemverwalter-Dokumentation. Der EVG war ein System. In den Sicherheitsvorgaben für den EVG war die Funktionalitätsklasse F-C2 festgelegt.

Relevante Evaluationsbeiträge

5.7.26 Als Beitrag zu dieser Arbeit dienten die Sicherheitsvorgaben und die Systemverwalter-Handbücher zum EVG.

Durchgeführte Arbeiten

5.7.27 Um eine vollständige und konsistente Behandlung der für den Systemverwalter relevanten sicherheitsspezifischen Funktionen zu gewährleisten, wurden die Systemverwalter-Handbücher auf die sicherheitsspezifischen Funktionen in den Sicherheitsvorgaben abgebildet.

5.7.28 Während der Besichtigungen vor Ort (siehe Absatz 5.7.6) erfuhren die Evaluatoren, wie das System vom Systemverwalter verwaltet werden könnte. Der Betrieb des Systems konnte anschließend mit den Beschreibungen in den Systemverwalter-Handbüchern verglichen werden (um ihre Korrektheit zu bewerten), und verbliebene Unklarheiten über den Zweck der Systemverwalter-Handbücher ließen sich klären.

5.7.29 Bei diesem konkreten System waren die Möglichkeiten des Systemverwalters, auf Anwenderinformationen zuzugreifen, stark eingeschränkt. Die Arbeit konzentrierte sich deshalb darauf sicherzustellen, daß die Prozeduren zur Kontrolle der Sicherheitsparameter detailliert genug waren.

5.7.30 Die Protokollkonfiguration wurde als ein unzureichend beschriebener Bereich herausgestellt. Die für die Installierung des Systems verwendeten Verfahren erlaubten eine Deinstallierung der Protokollmechanismen. Da in den Sicherheitsvorgaben sicherheitsspezifische Funktionen für die Protokollauswertung spezifiziert wurden, verfaßten die Evaluatoren einen Mängelbericht, um eine Änderung der Systemverwalter-Dokumentation zu gewährleisten, und zwar durch den Hinweis, daß die Protokollmechanismen so konfiguriert werden müssen, daß sie im System aktiv sind.

5.7.31 Die Vorschriften für die Identifikations- und Authentisierungsmechanismen wurden gründlich geprüft, um sicherzustellen,

a) daß die Verfahren für die Behandlung persönlicher Identifikationskarten konsistent waren;

b) daß Anwenderkonten mit einem eindeutigen Anwendernamen eingerichtet werden mußten.

5.7.32 Die Verfahren für die ordnungsgemäße Behandlung von Sicherungs- und Archivierungsmaterial wurden überprüft. Im Hinblick auf die Verwaltung des gesamten Archiv- und Sicherungsmaterials an demselben Ort wurde ein Mängelbericht verfaßt.

Beispiel 6(c) – Prüfung der Unteraktivität Auslieferung und Konfiguration (E2.34)

Einleitung

5.7.33 Dieses Unterbeispiel behandelt die Aufgaben zu Aspekt 1 der Betriebsumgebung – Auslieferung und Konfiguration. Der EVG war ein System. In den Sicherheitsvorgaben für den EVG war die Funktionalitätsklasse F-B1 festgelegt.

Relevante Evaluationsbeiträge

5.7.34 Als Beitrag zu dieser Arbeit dienten die Sicherheitsvorgaben und die Vorgehensweisen für die Auslieferung und Konfiguration des EVG.

Durchgeführte Arbeiten

5.7.35 Die Vorschriften für die Auslieferung konnten akzeptiert werden, da sie den im **nationalen Regelwerk** veröffentlichten Richtlinien entsprachen.

5.7.36 Jede in den Vorschriften genannte mögliche Konfiguration wurde überprüft, um sicherzustellen, daß sie keine Beeinträchtigung der Sicherheitsvorgaben verursachte.

5.7.37 Die Evaluatoren führten eine Besichtigung vor Ort durch, um die Installation des Systems zu beobachten. Sie beobachteten die Systemgenerierung, um die Einhaltung der dokumentierten Verfahren zu gewährleisten, und überprüften das Protokoll um sicherzustellen, daß die eigentliche Systemgenerierung im Protokoll unverfälscht wiedergegeben war.

5.7.38 Da die ITSEC-Korrektheitskriterien für Auslieferung und Konfiguration erfüllt wurden, konnte eine *akzeptierende* Entscheidung ausgesprochen werden.

Beispiel 6(d) – Prüfung der Unteraktivität Anlauf und Betrieb (E2.37)

Einleitung

5.7.39 Dieses Unterbeispiel behandelt die Aufgaben des Evaluators zu Aspekt 2 der Betriebsumgebung – Anlauf und Betrieb. Der EVG war ein System. Als Sicherheitsvorgabe für den EVG war die Funktionalitätsklasse F-C2 festgelegt.

Relevante Evaluationsbeiträge

5.7.40 Als Beitrag zu dieser Arbeit dienten die Sicherheitsvorgaben und die Vorgehensweisen für Anlauf und Betrieb des EVG.

Durchgeführte Arbeiten

5.7.41 Während der Besichtigungen vor Ort (siehe Absatz 5.7.6) erfuhren die Evaluatoren, wie der Anlauf und Betrieb des Systems durchgeführt wurde. Der Betrieb des Systems konnte anschließend mit den Beschreibungen in den Vorgehensweisen verglichen werden (um ihre Korrektheit zu bewerten), und verbliebene Unklarheiten über den Zweck der Anweisungen ließen sich klären.

5.7.42 Den Evaluatoren standen keine Beispielergebnisse von Selbsttestverfahren für sicherheitsspezifische Komponenten der Hardware zur Verfügung. Als Beispiel für eine sicherheitsspezifische Hardware-Komponente diente ein Hardware-Filter, das eine Terminal-Identifikationseinheit mit dem Netz verband. Während der Besichtigungen erfaßten die Selbsttestverfahren einen Hardware-Fehler in der Systemausstattung, womit sich für die Evaluatoren die Möglichkeit ergab, ein gewisses Vertrauen zu den Selbsttests zu entwickeln.

5.7.43 Sicherheitsspezifische Funktionen für die Beweissicherung beim Systemanlauf waren vorhanden. Der Antragsteller legte daher Beispiele von Protokollaufzeichnungen vor, die während der Anlauf- und Betriebsphase erstellt worden waren. Um eine korrekte Übereinstimmung zu gewährleisten, wurden diese Ergebnisse anhand konkreter Anlaufvorgänge überprüft. Die Funktionstests wurden eingehend geprüft, wobei eine ordnungsgemäße Abdeckung der sicherheitsspezifischen Funktionen festgestellt wurde.

5.7.44 Um sicherzustellen, daß keine potentiellen Sicherheitslücken in Form von Startoptionen eingebracht wurden, wurden die Vorgehensweisen von den Evaluatoren gründlich überprüft. In den Vorgehens-weisen wurde folgenden Aspekten keine besondere Beachtung geschenkt:

a) dem Zugang zum Rechnerraum;

b) der Konsolenausgabe.

5.7.45 Da die Verfahren zur Behandlung ungekennzeichneter Konsolenausgaben nicht beschrieben waren, wurde ein Mängelbericht erstellt.

5.7.46 Die Verfahren zum Trennen eines Host-Rechners vom Netz und zum Wiederanschließen ans Netz waren nicht ausreichend präzisiert. Während einer Besichtigung vor Ort konnte ein Bediener, der die schriftlichen Verfahrenshinweise befolgte, einen Host-Rechner nicht korrekt trennen. Dies führte zu einer Verletzung der örtlichen Sicherheitsvorschriften. Die Vorgehensweisen wurden daher in diesem Bereich als unzureichend betrachtet, und es wurde ein Mängelbericht erstellt.

5.7.47 Die Tatsache, daß jeder Anwender der Konsole die Möglichkeit hat, sicherheitsspezifische Prozesse zu beenden, war unzureichend dokumentiert. Ein Mängelbericht wurde verfaßt.

5.7.48 Die Möglichkeit, Beweissicherungsmechanismen bei laufendem System zu deaktivieren, war in den Vorgehensweisen unzureichend dokumentiert. Ein Mängelbericht wurde erstellt.

5.7.49 Da die Korrektheitskriterien der ITSEC für Anlauf und Betrieb nicht erfüllt wurden, konnte nur eine *ablehnende* Entscheidung ausgesprochen werden. Die Betriebsdokumentation wurde daraufhin vom Antragsteller und vom Entwickler gründlich überarbeitet und anschließend von den Evaluatoren erneut untersucht. Daraufhin konnte anhand der Kriterien in den ITSEC für Anlauf und Betrieb eine *akzeptierende* Entscheidung getroffen werden.

5.7.50 Die Evaluatoren prüften jedoch die Möglichkeit, ob die Deaktivierung von Beweissicherungsmechanismen und die Beendigung sicherheitsspezifischer Prozesse an der Konsole zu **potentiellen Schwachstellen** führen könnte. Diese Probleme wurden vermerkt und im Rahmen der unabhängigen **Schwachstellen**analyse der Evaluatoren untersucht.

Kapitel 5.8 Beispiel 7, Bewertung der Wirksamkeit (E3)

Einleitung

5.8.1 Dieses Kapitel enthält ein vollständig ausgearbeitetes Beispiel der Wirksamkeitskriterien auf E3. Das Beispiel ist rein fiktiver und theoretischer Natur. Es läßt die Anwendung der Korrektheitskriterien außer acht. Es soll daher davon ausgegangen werden, daß diese zu gegebener Zeit angewandt worden sind.

5.8.2 Dieses Beispiel soll in erster Linie veranschaulichen,

a) wie ein Antragsteller eine wohlbegründete Erklärung liefern kann, daß bekannte Schwachstellen in der Praxis nicht ausnutzbar sind;

b) welche Arbeiten von den Evaluatoren zur unabhängigen Überprüfung der Schwachstellenanalyse des Antragstellers durchgeführt wurden.

5.8.3 Da es sich hier um ein fiktives Beispiel handelt, wurden die in diesem Beispiel erörterten Schwachstellen nur zur Veranschaulichung der Analyse ausgewählt.

5.8.4 Nachdem die Hauptmerkmale der Sicherheitsvorgaben und des Architekturentwurfs des Beispielsystems beschrieben worden sind, werden die Kriterien 'Eignung' und 'Zusammenwirken der Funktionalität' angewandt. Diese beiden Kriterien sind darauf ausgerichtet, Schwachstellen in den Sicherheitsvorgaben bzw. im Architekturentwurf aufzuzeigen (siehe Teil 4, Kapitel 4.4). Die in dem Beispiel verwendeten Sicherheitsvorgaben sind so beschaffen, daß die Anwendung des Kriteriums 'Eignung der Funktionalität' keine Schwachstelle aufzeigt. Es wurde jedoch ein Architekturentwurf gewählt, der einen (teilweisen) Verstoß gegen die Kriterien 'Zusammenwirken der Funktionalität' illustrieren soll.

5.8.5 Anschließend werden weitere Beispiele für Konstruktions- und **operationelle Schwachstellen** vorgestellt und die Anwendung der Kriterien 'Bewertung der Konstruktionsschwachstellen und operationellen Schwachstellen', 'Analyse der Stärke der Mechanismen' und 'Benutzerfreundlichkeit' erläutert. Aufgrund der Einfachheit der in diesem Beispiel vorgestellten Sicherheitsvorgaben ist die Analyse der Stärke der Mechanismen und der Benutzerfreundlichkeit allerdings begrenzt.

Beschreibung der Sicherheitsvorgaben

Systembeschreibung

5.8.6 Das Beispielsystem befindet sich auf einem großen Gelände, das einem Wirtschaftsunternehmen gehört. Das Gelände ist vollständig von einem Schutzzaun umgeben, der gut bewacht ist. Alle Mitarbeiter gelten als vertrauenswürdig. Besucher dürfen das Betriebsgelände nur in Begleitung betreten.

5.8.7 Innerhalb des Betriebsgeländes gibt es verschiedene Bereiche, die zusätzlichen Schutz in Form einer Zugangskontrolle und anderer organisatorischer Sicherheitsmechanismen bieten. Es liegt eine geringe TEMPEST-Belastung und kryptographische Bedrohung vor. Die Terminals befinden sich in gesicherten Räumen, und Mitarbeiter werden durch die autorisierten Anwender daran gehindert, ein unbeaufsichtigtes Terminal in einem von ihnen betretenen Raum zu benutzen.

5.8.8 Auf dem Betriebsgelände befindet sich eine Vielzahl unterschiedlicher IT-Systeme, die zu unterschiedlichen Zeiten von verschiedenen Herstellern bezogen wurden und für eine Vielzahl von Zwecken, einschließlich der Transaktionsverarbeitung, der Abrechnung und der Unternehmensverwaltung, eingesetzt werden.

5.8.9 Jedes dieser Systeme, die als Endsysteme bezeichnet werden, ist an einer Systemnummer (S#) und einer Sicherheitsstufe (SL) zu erkennen. Sie alle liefern die notwendige Sicherheitsstufe für die eigenen Bedürfnisse (so sind beispielsweise manche Informationen managementvertraulich (Management in Confidence, MiC). Aufgrund der materiellen Sicherheit des Standorts, der Zahl der Anwender pro Endsystem, der erkannten Bedrohungen und der Sensitivität der Daten garantiert keines der Endsysteme mehr Schutz als ein Betriebssystem der ITSEC-Klasse F-C2.

5.8.10 In diesem Beispiel besitzt jedes Endsystem im allgemeinen seine eigenen I&A- und DAC-Funktionen, die der direkten Kontrolle des Systemverwalters für das betreffende Endsystem unterstehen. Außerdem sind alle Endsysteme als sternförmige Netze mit einem zentralen Host-Rechner (oder Cluster) zu betrachten, welcher eine geschlossene Anwendergruppe bedient, die in erster Linie unintelligente Terminals verwendet.

5.8.11 Die Anwenderterminals und die Host-Rechner, die in verschiedenen Gebäuden untergebracht sein können, waren früher über festgeschaltete Lichtwellenleiterkabel verbunden. Diese sind inzwischen durch ein Site-Wide Area Network (SWAN) ersetzt worden, das in diesem Beispiel behandelt wird. Das SWAN ist ein TCP/IP Token Ring-Netz, das aus einem "dual counter rotating backbone"-Netz und verschiedenen Teilnetzen besteht. Die Endsystemeinrichtungen sind über Zugangspunkte am Host-Rechner (Host Access Point, HAP) oder an den Terminals (Terminal Access Point, TAP) an das SWAN angeschlossen. Die TAP werden über RS232-Verbindungen zu Terminal-Servern (TS) geführt und von dort per Ethernet-Verbindung zu Routern, die in erster Linie mit den Teilnetzen, in einigen Fällen aber auch direkt mit dem Backbone-Hauptnetz verbunden sind. Die HAP sind direkt an einen Router angeschlossen. Hierbei handelt es sich um festgeschaltete Leitungen. Wenn ein Terminal eingeschaltet wird, startet das SWAN automatisch eine Anmeldesequenz. Wenn die Anwenderanmel-dung erfolgreich ist, wird am Terminal des Anwenders/der Anwenderin ein Menü der zulässigen Dienste angezeigt. Darin werden diejenigen Host-Rechner aufgeführt, zu denen der Anwender vom SWAN-Systemverwalter Zugang gewährt bekommen hat. Anschließend wird eine virtuelle Verbindung zwischen dem betreffenden Terminal und dem gewählten Host-Rechner aufgebaut. Der Anwender muß sich dann beim Host-Rechner anmelden.

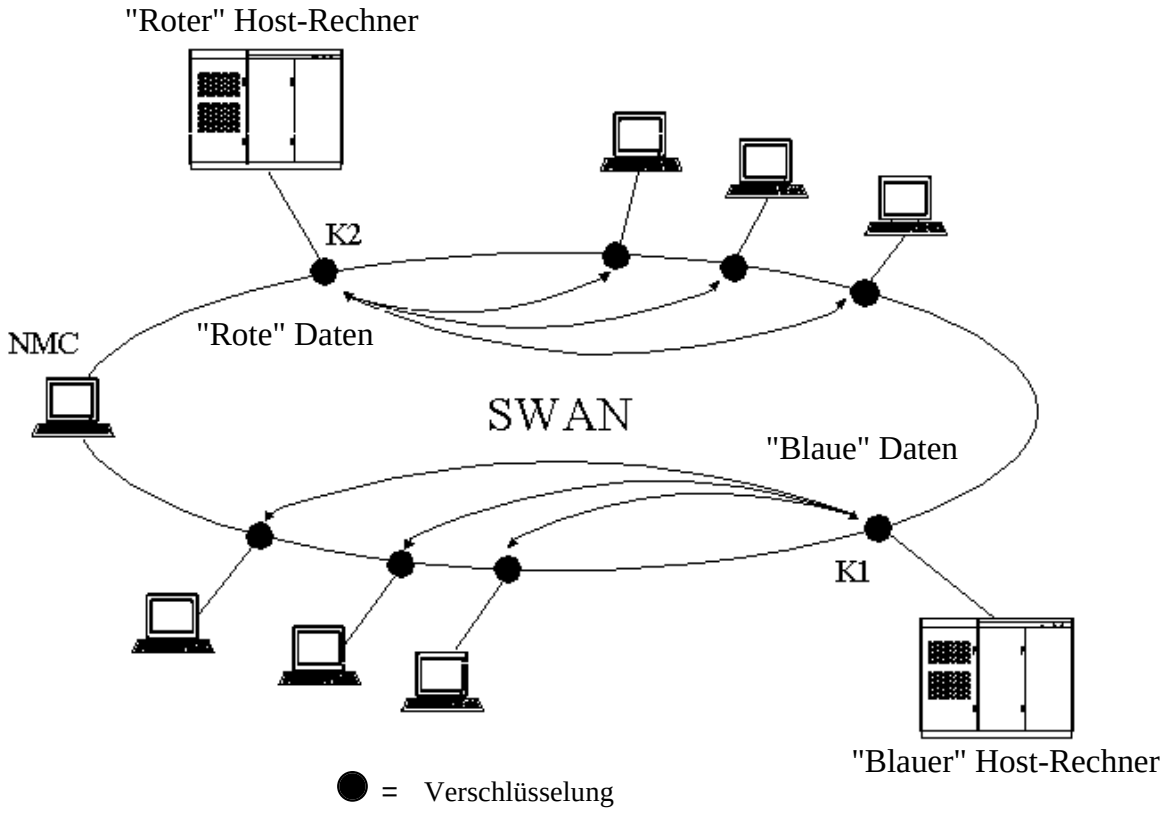
5.8.12 Sicherheitsprofile (auf welche Host-Rechner ein Anwender zugreifen darf) und andere Sicherheitsmechanismen werden im SWAN über eine von zwei Netzverwaltungszentralen (Network Management Centre, NMCs) zugeteilt, die I&A, DAC und MAC für das SWAN bereitstellen.

Sicherheitsziele

5.8.13 Das SWAN erbringt daher eine Vernetzungsdienstleistung für die Host-Rechner von Endsystemen und ihre Anwendergruppen. Es hat zwei Sicherheitsziele:

a) Schutz vor unberechtigtem Zugang zu einem Endsystem (S1);

b) Schutz der Vertraulichkeit von unterwegs befindlichen Informationen (S2).



Das SWAN sorgt für die Vernetzung verschiedener Rechnersysteme und ihrer Anwender. Eine *Endsystem-Zugangskontrolle* erfolgt über die Netzverwaltungszentrale (NMC), indem diese nur Zugang zu autorisierten Dienstleistungen im Netz gewährt. Ein Anwender, etwa im blauen System, müßte sich beim SWAN anmelden, eine autorisierte Dienstleistung auswählen und sich anschließend beim Host-Rechner anmelden. Eine der Vorgaben lautet, die verschiedenen Anwendergruppen voneinander getrennt zu halten, und da diese eventuell auf verschiedenen Stufen operieren (z. B. könnten die roten Daten managementvertraulich (MiC) sein, die blauen Daten dagegen offen), ist dies eine verbindliche Vorgabe. Zur Gewährleistung der *Vertraulichkeit der Übertragung* erfolgt eine Ende-zu-Ende-Verschlüsselung mit eindeutigen Schlüsseln für jedes Endsystem (d. h. K1 und K2 in der Abbildung). Durch materielle und organisatorische Kontrollen soll gewährleistet werden, daß die Anwender nur ihre eigenen Terminals benutzen können (anders ausgedrückt wäre ein Anwender des roten Systems nicht berechtigt, den Terminalraum des blauen Systems zu betreten und eines der dortigen Terminals zu benutzen).

Abbildung 5.8.1 Architekturentwurf des SWAN

Bedrohung der Sicherheit

5.8.14 Für die Sicherheit des SWAN bestehen folgende Bedrohungen:

a) Ein Anwender könnte sich beim Zugang zum SWAN für einen anderen Anwender ausgeben (T1).

b) Ein Anwender könnte eine Dienstleistung anfordern und/oder auf andere Weise zu nutzen versuchen, für den er/sie keine Nutzungsberechtigung besitzt (T2).

c) Ein Anwender könnte unterwegs befindliche Daten im Netz heimlich abhören oder auf andere Art abfangen (T3).

d) Ein Anwender könnte sich beim Zugang zu einem Host-Rechner für einen anderen Anwender ausgeben (T4).

Sicherheitspolitik

5.8.15 Die Sicherheitspolitik verlangt drei Formen der Zugriffskontrolle: MAC, gemeinsame HAP-Nutzung (siehe unten) und DAC.

5.8.16 MAC wird dann und nur dann erfüllt, wenn

$$S\#_H = S\#_T$$

$$SL_H = SL_T$$

wobei ($S\#_H$, SL_H) und ($S\#_T$, SL_T) die Systemnummer und die Sicherheitsstufe des Host-Rechners bzw. Terminals bezeichnen.

5.8.17 Die Strategie der gemeinsam HAP-Nutzung berücksichtigt den Fall, in dem einem Terminal Zugang zu mehr als einem Host-Rechner (H1 ... Hn) gewährt wird, und setzt voraus, daß

$$S\#_{H1} = S\#_{H2} = \ldots S\#_{Hn} = S\#_T$$

$$SL_{H1} = SL_{H2} = \ldots SL_{Hn} = SL_T$$

5.8.18 Im Rahmen dieser Einschränkungen läßt die DAC nur den Anschluß der vom betreffenden Endsystemverwalter gewünschten Einheiten der Endsystemausstattung zu.

Sicherheitsfunktionalität

5.8.19 Die Sicherheit im SWAN wird mit Hilfe von vier **Gegenmaßnahmen** (CM1 ... CM4) durchgesetzt:

a) Zur Authentisierung von Anwendern, die sich im Netz anmelden, wird eine I&A-Funktion verwendet (CM1);

b) die oben beschriebene Zugangskontrollpolitik wird von den NMCs durchgesetzt (CM2);

c) zwischen die Endsystemausstattung und die HAPs und TSs werden zugelassene Ver-/Entschlüsselungsgeräte eingefügt (CM3);

d) zur Authentisierung von Anwendern, die sich bei einem Host-Rechner anmelden, wird eine I&A-Funktion verwendet (CM4).

5.8.20 Die zwischen einem Host-Rechner und dem SWAN befindlichen Kryptogeräte arbeiten stets im Chiffriermodus – es gibt keinen Klartext-Bypass. Die zwischen der Terminalausstattung und dem Netz befindlichen Geräte verfügen über einen Bypass-Modus. Ein derartiges Gerät arbeitet anfänglich im Bypass-Modus. Dies ermöglicht eine Interaktion mit dem Netz im Klartext (d. h. zum und vom Netz gesendete Nachrichten werden nicht verschlüsselt). Sobald der Anwender eine Verbindung zum Host-Rechner aufgebaut hat, überträgt die Kryptoeinheit des Host-Rechners (Host computer Crypto-Unit, HCU) ein Signal zur Kryptoeinheit am Terminal (TCU), die ihrerseits die TCU vom Bypass- in den Chiffriermodus umschaltet. Nach Beendigung der Sitzung zwischen Anwender und Host-Rechner wird die Verbindung unterbrochen, und die TCU schaltet wieder auf den Bypass-Modus um. An beiden Kryptoeinheiten leuchtet eine Kontrollampe auf, solange sich die Einheit im Chiffriermodus befindet; sie erlischt, sobald wieder in den Klartextmodus umschaltet wird.

5.8.21 Die Schlüssel werden extern verwaltet, d. h. sie unterstehen dem Verwalter der Endsysteme und nicht dem SWAN-Verwalter. Pro System gibt es nur einen Kryptoschlüssel, der nur einmal existiert.

5.8.22 Die anwenderbestimmbare Zugangskontrollpolitik wird von den NMCs durchgesetzt.

5.8.23 Router- oder Terminal-Server-Software wird nicht als sicherheitsrelevant betrachtet.

Erforderliche Mindeststärke der Mechanismen

5.8.24 Die erforderliche Mindeststärke der Mechanismen ist *mittel*. Folglich (siehe Teil 6, Anhang 6.C) wird die Höchstzahl der einem Angreifer zur Verfügung stehenden Gelegenheiten, Fachkenntnisse und Betriebsmittel als *mittel* betrachtet.

5.8.25 Die Entwickler entscheiden sich für einen kryptographischen Mechanismus, der von der entsprechenden nationalen Behörde mit mindestens *mittel* bewertet wurde, einen mit *hoch* bewerteten Zugangskontrollmechanismus (für CM2) und für *niedrige* I&A-Mechanismen (für CM1 und CM4).

5.8.26 In den Sicherheitsvorgaben wird darauf hingewiesen, daß der kryptographische Mechanismus der kritische Mechanismus für das SWAN ist, da bei einem Versagen der Zugangskontrollmechanismen der Angreifer nur Zugang zu verschlüsselten Daten erhält, so daß beide Sicherheitsziele aufrechterhalten werden können.

Konfigurierbare Geräte

5.8.27 Es gibt ein Kryptogrundgerät, das durch Einschieben einer ein Anwendungsprogramm und den Kryptoschlüssel enthaltenden Schlüsselkarte als HCU oder TCU konfiguriert werden kann. Die Karten sind von unterschiedlicher Größe und Farbe, und ein eingebauter Teil des Schlüsselkartenschlitzes an der HCU ist mechanisch blockiert, so daß diese Geräte TCU-Karten physikalisch nicht annehmen. Dadurch lassen sich HCU und TCU leicht unterscheiden.

5.8.28 Paßwörter können auf eine Länge zwischen 8 und 12 Zeichen konfiguriert werden und werden automatisch generiert. Als Gültigkeitsdauer eines Paßworts können zwischen 1 und 60 Tagen konfiguriert werden. Beide Bereiche sind in den Sicherheitsvorgaben spezifiziert.

5.8.29 Weitere konfigurierbare Sicherheitsfunktionen sind nicht vorhanden.

Wirksamkeitsanalyse

Analyse der Eignung

5.8.30 Die ITSEC verlangen, daß der Antragsteller eine **Analyse der Eignung** vorlegt, in der die sicherheitsspezifischen Funktionen und Mechanismen den festgestellten Bedrohungen, denen sie entgegenwirken sollen, gegenübergestellt sind, und in der gezeigt wird, daß diesen Bedrohungen angemessen entgegen-gewirkt wird.

5.8.31 In diesem Beispiel befaßt sich die vom Antragsteller vorgelegte Analyse der Eignung mit jeder der in Absatz 5.8.14 aufgeführten Bedrohungen getrennt von den anderen Bedrohungen. Die Analyse zeigt mindestens eine Funktion oder einen Mechanismus auf, die/der der Bedrohung entgegenwirken kann. Der Antragsteller zieht die Zusammensetzung von Mechanismen nicht in Betracht, d. h. er berücksichtigt den Architekturentwurf des SWAN nicht (Abbildung 5.8.1), sondern begnügt sich mit der bloßen Aufzählung der Bedrohungen und der Gegenmaßnahmen, die in den Sicherheitsvorgaben genannt sind.

5.8.32 In diesem Beispiel demonstriert der Antragsteller den direkten Zusammenhang zwischen den Gegenmaßnahmen (Countermeasures, CM) und Bedrohungen (Threats, T) und den sicherheits-spezifischen Funktionen, und zwar wie folgt:

a) versuchter Zugang zum SWAN unter fremder Identität (*T1*) und die Anmeldefunktion des SWAN (*CM1*);

b) Anforderung oder anderweitige Erlangung des Zugangs zu einer nicht autorisierten Dienstleistung (*T2*) und die SWAN-Zugangskontrollfunktion (*CM2*);

c) Abhören oder sonstiges Abfangen von unterwegs befindlichen Daten im SWAN (*T3*) und die Kryptofunktion (*CM3*);

d) versuchter Zugang zu einem Host-Rechner unter fremder Identität (*T4*) und die Anmel-defunktion des Host-Rechners (*CM4*).

5.8.33 Die vom Antragsteller vorgelegte Analyse der Eignung schließt auch die in Abbildung 5.8.2 ge-zeigte Tabelle ein, die den Zusammenhang zwischen Sicherheitszielen, Gegenmaßnahmen und Bedrohungen demonstriert.

Abbildung 5.8.2 Analyse der Eignung

Sicherheitsziel	Gegenmaßnahme	Bedrohung
S1 – Host-Rechner Zugangsschutz	CM1 – SWAN-Anmeldung	T1 – SWAN-Zugang unter falscher Identität
S1 – Host-Rechner Zugangsschutz	CM2 – Host-Rechner Zugangs-kontrolle	T2 – Anforderung oder Erlangung des Zugangs zu nicht autorisierter Dienstleistung
S1 – Host-Rechner Zugangsschutz	CM4 – Host-Rechner Anmeldung	T4 – falsche Identitätsangabe für Host-Rechner
S2 – Netz vertraulich	CM3 – Kryptofunktion	T3 – Abfangen von Daten

5.8.34 Sowohl die Anmeldefunktion beim SWAN als auch beim Host-Rechner sind firmeneigene Systeme mit geheimem Paßwort. Der Antragsteller behauptet in seiner Analyse der Eignung, daß beide Funktionen geeignet seien, da ein Angreifer das geheime Paßwort der anderen Person kennen müsse. Außerdem wird geltend gemacht,

a) daß die Zugangskontrollfunktion des SWAN geeignet sei, da ein identifizierter Anwender nur zwischen Dienstleistungen auswählen dürfe, für die der Betreffende autorisiert sei;

b) daß die Kryptofunktion geeignet sei, da die Kryptoeinheit des Host-Rechners über keinen Bypass-Modus verfüge und stets Daten sende, die mit einem entsprechenden Algorithmus und Schlüssel chiffriert seien, der ausschließlich dem betreffenden Host-Rechner zugeordnet und nur den autorisierten Anwendern dieses Host-Rechners bekannt sei.

5.8.35 Demnach dürfte nur ein *autorisierter* Anwender, der unterwegs befindliche Daten im SWAN abhört oder auf andere Weise abfängt, zur Entschlüsselung der Daten in der Lage sein. Demzufolge sind also alle sicherheitsspezifischen Funktionen geeignet.

5.8.36 Man beachte, daß diese Argumente nicht auf die Stärke der Mechanismen oder das Zusammenwirken der Sicherheitsfunktionen bezogen sind.

5.8.37 Ein Beispiel für eine ungeeignete Funktion wäre die Verwendung einer DAC-Funktion, wenn die Gefahr besteht, daß jemand versucht, auf geheime Informationen zuzugreifen, für die er keine ausreichende Berechtigung besitzt. Dies liegt daran, daß die DAC-Funktion keine Möglichkeit hat, die Geheimhaltungs- bzw. Berechtigungsstufen des Objekts und der Subjekte festzustellen, mit denen sie arbeitet.

5.8.38 Wahlweise hätte das Eignungsargument auch in Form von Sicherheitszielen formuliert werden können. Dieser Ansatz ist unter Umständen vorzuziehen, wenn es sich um ein Produkt handelt oder wenn die Bedrohung detaillierter ausgedrückt wird, z. B. "es liegt eine terroristische Bedrohung vor":

a) Das Ziel des Endsystemzugangs (S1) wird durch Kombination der Anmeldefunktionen (für CM1 und CM4) und der Zugangskontrollfunktion (CM2) erreicht (aus den in Absatz 5.8.34 genannten Gründen).

b) Die Vertraulichkeit von unterwegs befindlichen Informationen (S2) wird durch den kryptographischen Mechanismus (für CM3) bewahrt (aus den in Absatz 5.8.34 genannten Gründen).

Analyse des Zusammenwirkens

5.8.39 Die ITSEC verlangen vom Antragsteller,

a) daß er eine Analyse aller potentiellen Beziehungen zwischen sicherheitsspezifischen Funktionen und Mechanismen vorlegt;

b) daß er nachweist, daß keine Möglichkeit besteht, eine sicherheitsspezifische Funktion oder einen Mechanismus zu veranlassen, mit den Zielen anderer sicherheitsspezifischer Funktionen oder Mechanismen zu kollidieren oder ihnen entgegenzuwirken.

5.8.40 Im Gegensatz zur Eignung der Funktionalität muß die **Analyse des Zusammenwirkens** die Zusammensetzung des Systems berücksichtigen, d.h., der Entwickler muß *alle möglichen Beziehungen zwischen den sicherheitsspezifischen Funktionen und Mechanismen* berücksichtigen.

5.8.41 In diesem Beispiel wird die Zugangskontrolle zum Endsystem verletzt, wenn ROTE Daten an einem BLAUEN Terminal angezeigt werden können. Die Vertraulichkeit der Übertragung wird verletzt, wenn die Kryptoschlüssel gefährdet werden, beide Kryptofunktionen am Terminal oder am Host-Rechner umgangen werden und die Übertragung "im Klartext" erfolgt oder andere "Nutz"-Informationen im Klartext übertragen werden.

5.8.42 Aus der vom Antragsteller durchgeführten Analyse des Zusammenwirkens geht folgendes hervor:

a) Wenn dem Anwender (Angreifer) die Anmeldung beim SWAN aus irgendeinem Grund nicht gelingt, kann er keine Nutzinformationen gewinnen.

b) Wenn sich der Anwender beim SWAN erfolgreich anmeldet, arbeiten die zwischen dem Terminal und dem SWAN befindlichen kryptographischen Geräte im Bypass-Modus, bis eine Verbindung mit einem Host-Rechner aufgebaut ist. Daher werden die SWAN-Authentisierungsdaten im Klartext über das SWAN übertragen.

c) Dem Anwender werden nur Dienstleistungen angeboten, (i) für die er eine Autorisierung besitzt und (ii) die der SWAN-Zugangskontrollpolitik entsprechen.

d) Anschließend wird eine Kryptoverbindung zwischen Terminal und Host-Rechner aufgebaut. Der Entwickler geht davon aus, daß nur gültige Schlüssel verwendet werden.

e) Anschließend meldet sich der Anwender beim Host-Rechner an. Wenn dies nicht gelingt, wird der Vorgang beendet: Am Terminal werden keine Nutzdaten angezeigt, und über das SWAN wurden keine anderen Nutzdaten übertragen (mit Ausnahme der SWAN-Authentisierungs-daten, siehe (b)).

f) Wenn der Anwender/die Anwenderin erfolgreich ist, kann er/sie anschließend *verschlüsselte* Informationen zwischen seinem/ihrem Terminal und dem Host-Rechner übertragen.

5.8.43 In der vom Antragsteller durchgeführten Analyse des Zusammenwirkens werden drei Szenarien vorgestellt, die aus Abbildung 5.8.3 zu ersehen sind.

Abbildung 5.8.3 Analyse des Zusammenwirkens

Szenarium	**Angezeigte Daten**	**Daten im SWAN**
Anwender kann sich nicht beim SWAN anmelden.	Keine	Keine
Anwender meldet sich erfolgreich beim SWAN an, kann sich aber nicht beim Host-Rechner anmelden.	Keine	I&A-Informationen *im Klartext*
Anwender meldet sich erfolgreich beim SWAN und bei einer *autorisierten* Host-Dienstleistung an.	BLAUE Daten	I&A-Informationen *im Klartext,* verschlüsselte Daten

5.8.44 Folglich kann der Antragsteller nachweisen,

a) daß die Funktionen SWAN I&A, Zugangskontrolle und Host I&A tatsächlich *zusammenwirken*, da in allen Szenarien niemals ROTE Daten im Klartext angezeigt werden;

b) daß die Verschlüsselungsgeräte jedoch *nicht völlig zusammenwirken*, da bei einigen Szenarien SWAN-Authentisierungsdaten im Klartext gesendet werden.

5.8.45 Der Antragsteller bringt daraufhin vor, die Überwindung von CM1 reiche für sich allein nicht aus, um eine Verletzung der Sicherheitsziele zu verursachen, da zwar SWAN-Authentisierungsdaten "im Klartext" gesendet würden, die kryptographischen Mechanismen (für CM3) und die Anmeldung beim Host-Rechner (für CM4) aber weiterhin die Sicherheitspolitik umsetzen.

5.8.46 Die Evaluatoren führen eine unabhängige Überprüfung der vom Antragsteller erstellten Analyse des Zusammenwirkens durch. Der offenkundige Mangel an Zusammenwirkung wird festgestellt, die Evaluatoren sprechen aber an dieser Stelle der Wirksamkeitsbewertung keine *ablehnende* Entscheidung aus.

5.8.47 Dieses fehlende Zusammenwirken stellt lediglich eine Schwachstelle dar, die die Evaluatoren unabhängig dahingehend überprüfen müssen, ob sie in der Praxis ausnutzbar ist. In diesem Stadium kann kein ablehnendes Urteil ausgesprochen werden, wenn sich nicht nachweisen läßt, daß diese Schwachstelle (in der Konstruktion) ausnutzbar ist. Dies läßt sich erst feststellen, wenn die Evaluatoren die Kriterien für die Schwachstellenbewertung angewandt und Penetrationstests durchgeführt haben.

Schwachstellenanalysen des Antragstellers

5.8.48 In Übereinstimmung mit den ITSEC (Absätze 3.26 bis 3.27 und 3.35 bis 3.36) stellt der Antragsteller den Evaluatoren eine Liste bekannter Schwachstellen in der Konstruktion und im Betrieb des EVG sowie eine Analyse der potentiellen Auswirkungen jeder bekannten Schwachstelle auf die Sicherheit des EVG zur Verfügung.

5.8.49 In diesem Beispiel hat der Antragsteller die Liste bekannter Konstruktionsschwachstellen und die Liste bekannter operationeller Schwachstellen zusammengefaßt und eine einzige Schwachstellenanalyse durchgeführt.

5.8.50 Operationelle Schwachstellen stehen mit materiellen und administrativen Vorgängen außerhalb des EVG in Zusammenhang. Sie können dem Angreifer die Gelegenheit und die Ressourcen verschaffen, mit denen dieser eine **Konstruktionsschwachstelle** ausnutzen oder einen direkten Angriff durchführen kann. Ebenso können sie dem Angreifer die Sicherheitsinformationen (z. B. eine Anwender-ID und ein Paßwort) liefern, die dieser benötigt, um sich als autorisierter Anwender auszugeben.

5.8.51 Die ITSEC verlangen vom Antragsteller, daß er nachweist, daß die Schwachstelle in der Praxis nicht ausgewertet werden kann, d.h.,

a) daß jede Schwachstelle ausreichend durch andere nicht beeinträchtigte Sicherheitsmechanismen geschützt ist, oder

b) daß die Schwachstelle für die Sicherheitsvorgaben irrelevant ist, daß sie in der Praxis nicht vorkommt oder daß ihr mit dokumentierten technischen, personellen, organisatorischen oder materiellen Gegenmaßnahmen außerhalb des EVG entgegengewirkt werden kann.

5.8.52 Die dem Antragsteller bekannten Konstruktionsschwachstellen und operationellen Schwachstellen sind in Abbildung 5.8.4 aufgeführt. In dieser Liste werden die Schwachstellen mit Bedrohungen (z. B. Bedrohung T1: Der Anwender könnte sich beim Zugang zum SWAN für einen anderen Anwender ausgeben, vielleicht als Folge des Abhörens von I&A-Daten des SWAN) und dem Sicherheitsziel in Zusammenhang gebracht, das verletzt werden kann, wenn die Schwachstelle in der Praxis ausnutzbar ist.

5.8.53 Um unter Verletzung der Sicherheitspolitik Zugriff auf Host-Rechnerdaten zu bekommen, muß ein Angreifer mit Erfolg ein *Angriffsszenarium* gegen die vier Gegenmaßnahmen (CM1 .. CM4) verwirklichen. Jede Gegenmaßnahme muß im Verlauf des Angriffsszenariums entweder durch einen direkten Angriff (z. B. einen Angriff, der auf die zugrundeliegenden Algorithmen, Prinzipien oder Eigenschaften der betreffenden Gegenmaßnahme abzielt) oder indirekt (z. B. durch Umgehen) überwunden werden.

5.8.54 Abbildung 5.8.5 zeigt die vom Antragsteller vorgenommene Analyse aller möglichen Angriffsszenarien, die eine Verletzung der Sicherheitsziele bewirken würden, d.h.

a) Schutz gegen unautorisierten Zugang zu einem Endsystem (S1);

b) Schutz der Vertraulichkeit der unterwegs befindlichen Informationen (S2).

5.8.55 Zu den Mitteln, mit denen die Gegenmaßnahmen CM1 .. CM4 überwunden werden können, gehört auch eine Darstellung der entsprechenden Bedrohungen T1 .. T4, die durch indirekte Angriffe auf diese Gegenmaßnahmen mit Hilfe der obengenannten Schwachstellen realisiert werden können (zum Beispiel V1, V2 sind indirekte Angriffe auf CM1).

5.8.56 Wenn ein Angreifer über einen gültigen Account auf dem Host-Rechner verfügt, hat er die Wahl, das Menü der autorisierten SWAN-Dienstleistungen normal zu verwenden oder V6 zu aktivieren. Wenn der Angreifer keinen gültigen Account auf dem Host-Rechner besitzt, kann er nur V6 einsetzen, weil das Vorhandensein des Ziel-Host-Rechners in dem Menü der autorisierten Dienstleistungen unter normalen Umständen impliziert, daß er über einen gültigen Account auf dem Host-Rechner verfügt. V6 setzt eine geheime Absprache mit dem SWAN-Sicherheitsadministrator, aber nicht mit dem Sicherheitsadministrator des Ziel-Host-Rechners voraus, womit sich die Notwendigkeit eines Angriff auf die Anmeldung beim Host-Rechner ergibt.

5.8.57 Obwohl nach den Plänen des Entwicklers die Gegenmaßnahmen in der Reihenfolge CM1, CM2, CM3 und CM4 überwunden werden sollen, besteht aufgrund der Konstruktion des SWAN die Möglichkeit, daß andere Angriffsszenarien existieren, die zu einer **ausnutzbaren Schwachstelle** führen könnten.

5.8.58 In diesem Beispiel zeigt die Analyse des Antragstellers keine Möglichkeit, den kryptographischen Mechanismus zu umgehen, so daß die einzige entdeckte Schwachstelle in der Deaktivierung durch einen Komplizen besteht. Für jedes der in Abbildung 5.8.5 gezeigten Angriffsszenarien muß der Angreifer daher die Gegenmaßnahme CM3 überwinden, um die Sicherheitsziele S1 und S2 verletzen zu können.

5.8.59 CM3 ist mit einer *mittleren* Stärke der Mechanismen (Strength of Mechanisms, SoM) gegenüber einem direktem Angriff bewertet und erfüllt die postulierte Mindeststärke für das SWAN. Ein Angreifer könnte versuchen, die Konstruktionsschwachstelle V4 auszunutzen, doch dies setzt eindeutig eine geheime Absprache mit einem vertrauenswürdigen Anwender des Ziel-Host-Rechners voraus, der mit Sicherheitsmaßnahmen außerhalb des EVG begegnet wird.

5.8.60 Die Analyse des Antragstellers zeigt somit, daß den in Abbildung 5.8.5 gezeigten bekannten Schwachstellen mit den kryptographischen Geräten (sowie Maßnahmen außerhalb des EVG) angemessen entgegengewirkt wird.

5.8.61 Da außer den obengenannten keine erkennbaren Möglichkeiten zur Umgehung von Gegenmaßnahmen innerhalb des Angriffsszenariums vorhanden sind, ist klar, daß bei der Analyse des Antragstellers sämtliche Kombinationen bekannter Schwachstellen berücksichtigt worden sind. Entsprechend sind die Evaluatoren aufgrund ihrer Kenntnis des EVG überzeugt, daß in der Analyse des Antragstellers keine unrealistischen Annahmen über die vorgesehene Betriebsumgebung getroffen sind.

Abbildung 5.8.4 Liste bekannter Konstruktionsschwachstellen und operationeller Schwachstellen			
ID	**Beschreibung**	**Bedrohung**	**Sicherheits-ziel**
V1	**Angreifer hört I&A-Daten des SWAN ab.** Der Angreifer hört das SWAN-Netz ab und verschafft sich die SWAN-Kennung und das Paßwort für einen Anwender des Ziel-Host-Rechners (des anzugreifenden Host-Rechners). Hierbei handelte es sich um die Schwachstelle, die bei der obigen Analyse des Zusammenwirkens der Funktionalität ermittelt wurde.	T1	S1
V2	**Break-Taste bei SWAN-Anmeldung.** Wenn während der Anmeldung beim SWAN die Break-Taste gedrückt wird, bewirkt dies eine Unterbrechung des Anmeldevorgangs nach 5 Minuten, sofern der Anwender keine Eingabe eintippt. Es erscheint eine Zeitsperrmeldung. Wenn der Anwender 10 Minuten lang nichts unternimmt, läuft die Zeitsperrmeldung ihrerseits ab, woraufhin das autorisierte Dienstleistungsmenü für den letzten Anwender angezeigt wird, der sich erfolgreich beim SWAN angemeldet hat. Dieser Anwender hätte ein Anwender des Ziel-Host-Rechners sein können.	T1	S1
V3	**Nicht autorisierte Dienste verfügbar.** Wenn die Zahl der autorisierten Dienstleistungen für den aktuellen Anwender kleiner ist als für den zuvor beim SWAN angemeldeten Anwender, stehen die zusätzlichen (nicht autorisierten) Dienstleistungen weiterhin zur Verfügung, obwohl sie nicht angezeigt werden.	T2	S1
V4	**Komplize deaktiviert Kryptofunktionen.** Wenn während der Anmeldung beim Host-Rechner die Break-Taste zweimal kurz hintereinander gedrückt wird, geht die TCU in den Bypass-Modus über, ohne daß dem NMC der Abbruch der Sitzung mit dem Host-Rechner signalisiert wird. Ein anschließendes Drücken der Break-Taste bewirkt dies zwar, doch aufgrund eines Fehlers in der HCU laufen alle weiteren Übertragungen zwischen dieser HCU und einer TCU im Klartext ab. Da die Anmeldung beim Host-Rechner durch die HCU geschützt wird, ist eine Deaktivierung der HCU nur durch einen autorisierten Anwender des betreffenden Host-Rechners möglich – daher ist ein Komplize erforderlich.	T3	S2
V5	**Komplize hat I&A-Daten des Host-Rechners abgefangen.** Durch Betätigen einer bestimmten Folge von Funktionstasten kann ein Anwender Zugang zur Paßworttabelle des HOST erhalten. Die Paßwörter sind verschlüsselt, können aber innerhalb weniger Tage entschlüsselt werden. Wie bei V4 (siehe oben) kann auch dieser Schritt nur von einem vertrauenswürdigen Anwender des Host-Rechners durchgeführt werden.	T4	S1
V6	**Angreifer erhält autorisierte Dienstleistung durch geheime Absprache.** Autorisierte Dienstleistungen werden für einen Anwender/eine Anwenderin auf seinen/ihren schriftlichen Antrag hin eingerichtet und von seinem/ihrem Vorgesetzten genehmigt. Die Daten werden auf Konsistenz mit denen anderer Anwender geprüft und vom NMC abgelehnt, wenn sie nicht der Zugangskontrollpolitik des SWAN entsprechen. Die Daten werden nach einem Vier-Augen-Prinzip eingegeben. Trotzdem ist es immerhin möglich, durch geheime Absprache dieselbe Systemnummer (S*#*) und Sicherheitsstufe (*SL*) wie für den Ziel-Host-Rechner zu verwenden, um ein neues System zu identifizieren, und DAC-Kontroll-mechanismen zu verwenden, um die Anwendergruppen der beiden Systeme zu trennen, wobei jedoch der Angreifer Zugang zu beiden erhält.	T2	S1

Abbildung 5.8.5 Antragstelleranalyse der Angriffsszenarien						
Lfd. Nr.	**Beschreibung**	**CM1 (niedrig)**	**CM2 (hoch)**	**CM3 (mittel)**	**CM4 (niedrig)**	**Verletzung**
1	Angreifer überwindet CM1, verwendet das SWAN-Autorisierungsmenü normal, überwindet CM3 und meldet sich erfolgreich beim Host-Rechner an	V1 oder V2	Menü verwenden	V4	Anmeldung beim Host als autoris. Anwender	S1, S2
2	Angreifer überwindet CM1, verwendet das SWAN-Autorisierungsmenü normal und überwindet anschließend sowohl CM3 als auch CM4	V1 oder V2	Menü verwenden	V4	V5	S1, S2
3	Angreifer überwindet CM1 .. CM4 mittels irgendeiner Kombination der obigen Schwachstellen	V1 oder V2	V6 oder V3	V4	V5	S1, S2
4	Angreifer überwindet CM1 .. CM3 und führt anschließend eine erfolgreiche Anmeldung beim Host-Rechner durch	V1 oder V2	V3	V4	Anmeldung beim Host als autoris. Anwender	S1, S2
5	Angreifer meldet sich erfolgreich beim SWAN an und überwindet anschließend CM2 .. CM4	SWAN-Anmeldung als autoris. Anwender	V6 oder V3	V4	V5	S1, S2
6	Angreifer meldet sich erfolgreich beim SWAN an, überwindet CM2 und CM3 und meldet sich anschließend erfolgreich beim Host-Rechner an	SWAN-Anmeldung als autoris. Anwender	V3	V4	Anmeldung beim Host als autoris. Anwender	S1, S2
7	Angreifer meldet sich erfolgreich beim SWAN an, wählt eine autorisierte Dienstleistung und überwindet anschließend CM3 und CM4	SWAN-Anmeldung als autoris. Anwender	autorisierte Dienstleistung wählen	V4	V5	S1, S2
8	Angreifer meldet sich erfolgreich beim SWAN an, wählt eine autorisierte Dienstleistung, überwindet CM3 und meldet sich anschließend erfolgreich beim Host-Rechner an	SWAN-Anmeldung als autoris. Anwender	autorisierte Dienstleistung wählen	V4	Anmeldung beim Host als autoris. Anwender	S2

Unabhängige Schwachstellenanalyse der Evaluatoren

5.8.62 Die ITSEC verlangen von den Evaluatoren die Durchführung einer eigenen Schwachstellenanalyse unter Berücksichtigung der aufgelisteten und der sonstigen während der Evaluation gefundenen bekannten Schwachstellen (sowohl operationelle Schwachstellen als auch Konstruktionsschwachstellen).

5.8.63 In dem gesamten Beispiel wurde davon ausgegangen, daß die Korrektheitskriterien bereits auf den EVG angewandt worden sind. Im Sinne dieses Beispiels wird davon ausgegangen, daß bei der Anwendung der Korrektheitskriterien eine potentielle Schwachstelle entdeckt wurde, die für Analysezwecke als Konstruktionsschwachstelle betrachtet wurde. Diese Schwachstelle war in der vom Antragsteller gelieferten Liste der bekannten Schwachstellen noch nicht ausgewiesen. Sie ist in Abbildung 5.8.6 dargestellt.

Abbildung 5.8.6 Bei der Bewertung der Korrektheit ermittelte Konstruktionsschwachstellen

ID	Beschreibung	Bedrohung	Sicherheits-ziel
V7	**Anwender deaktiviert Kryptofunktionen.** Wie V4, doch wenn der Angreifer Anwender des Ziel-Host-Rechners ist, fungiert er als sein eigener Komplize. Dieser Fall tritt beispielsweise dann ein, wenn der Angreifer Anwender eines Systems mit managementvertraulichen Daten ist, bei dem ein autorisierter Zugang nur von einem sicherheitsgeprüften Terminalraum aus möglich ist, der Angreifer sich aber von seinem (nicht sicherheitsgeprüften) Büro aus Zugang zum System verschaffen möchte.	T3	S2

5.8.64 Aus dieser Konstruktionsschwachstelle folgt, daß ein Anwender, der sich erfolgreich bei einem ROTEN Host-Rechnersystem anmeldet, Gegenmaßnahme CM3 überwinden kann, ohne daß eine geheime Absprache nötig ist. Diese Schwachstelle wirkt sich auf die Angriffsszenarien 1, 4, 6 und 8 in der Evaluatoranalyse der Angriffssequenzen aus, die nun wie in Abbildung 5.8.7 dargestellt aussehen. Von Belang für die Evaluatoren war, daß die Schwachstellenanalyse des Antragstellers folgendes zeigte:

a) CM1 und CM4 werden mit einer *niedrigen* Stärke der Mechanismen (SoM) angegeben und sind für sich allein nicht hinreichend (man beachte, daß nur die Mechanismen für CM2 (*hoch*) und CM3 (*mittel*) der postulierten Mindeststärke für den EVG entsprechen (*mittel*)).

b) Der Mechanismus für CM3 ist der einzige Mechanismus in den Angriffsszenarien 1, 2, 7 und 8, der der postulierten Mindest-SoM für das SWAN entspricht (Angriffsszenarium 8 verläßt sich ganz auf CM3 zur Aufrechterhaltung der Sicherheitspolitik).

c) Wenn der Mechanismus für CM2 überwunden werden kann, ist der Mechanismus für CM3 der einzige andere Mechanismus in den Angriffsszenarien 3, 4, 5 und 6, der der postulierten Mindest-SoM für das SWAN entspricht.

Abbildung 5.8.7 Evaluatoranalyse der Angriffsszenarien						
Lfd. Nr.	**Beschreibung**	**CM1 (niedrig)**	**CM2 (hoch)**	**CM3 (mittel)**	**CM4 (niedrig)**	**Verletzung**
1’	Angreifer überwindet CM1, verwendet das SWAN-Autorisierungsmenü normal, überwindet CM3 und meldet sich erfolgreich beim Host-Rechner an	V1 oder V2	autoris. Dienst-leistung wählen	V4 oder V7	Anmeldung beim Host als autoris. Anwender	S1, S2
4’	Angreifer überwindet CM1 .. CM3 und führt anschließend eine erfolgreiche Anmeldung beim Host-Rechner durch	V1 oder V2	V3	V4 oder V7	Anmeldung beim Host als autoris. Anwender	S1, S2
6’	Angreifer meldet sich erfolgreich beim SWAN an, überwindet CM2 und CM3 und meldet sich anschließend erfolgreich beim Host-Rechner an	SWAN-An-meldung als autoris. Anwender	V3	V4 oder V7	Anmeldung beim Host als autoris. Anwender	S1, S2
8’	Angreifer meldet sich erfolgreich beim SWAN an, wählt eine autorisierte Dienstleistung, überwindet CM3 und meldet sich anschließend erfolgreich beim Host-Rechner an	SWAN-An-meldung als autoris. Anwender	autorisiert e Dienst-leistung wählen	V4 oder V7	Anmeldung beim Host als autoris. Anwender	S2

5.8.65 Es ist nicht möglich, anhand der Schwachstellenbewertungen eine endgültige Entscheidung zu treffen (siehe Abschnitt *Evaluatorentscheidungen*, Teil 4, Kapitel 4.4), bis die Evaluatoren nachweisen können, ob diese zusätzliche Konstruktionsschwachstelle (oder eine andere der obigen Schwach-stellen) in der Praxis ausnutzbar ist (durch Penetrationstests).

Stärke der Mechanismen

5.8.66 Obwohl der Antragsteller alle Mechanismen bewertet hat (siehe Absatz 5.8.25), zeigt seine Schwachstellenanalyse, daß der einzige kritische Mechanismus der von CM3 ist (dies wurde auch durch die unabhängige Schwachstellenanalyse der Evaluatoren bestätigt).

5.8.67 Gegenmaßnahme CM3 ist kryptographisch, und die Bewertung der Stärke ihres kryptographischen Mechanismus fällt ebenso wie die Schlüsselverwaltungsverfahren nicht in den Anwendungsbereich der ITSEC. Die Evaluatoren können nur unter Bezugnahme auf die nationale Sicherheitsbehörde überprüfen, ob der kryptographische Mechanismus die Bewertung der postulierten Mindeststärke der Mechanismen für das SWAN erfüllt.

5.8.68 Die Evaluatoren müssen bei der zuständigen nationalen Sicherheitsbehörde im Zusammenhang mit der Online-Kryptoanalyse (für einen Angriff auf die Trennung der Endsysteme erforderlich, da ein Verbindungsweg mit dem Host-Rechner eingerichtet werden muß) und der Offline-Kryptoanalyse (zum Abhören) anfragen, ob die SoM der Kryptofunktionen, einschließlich der Schlüsselverwaltungs-verfahren, zumindest mit *mittel* bewertet würde.

5.8.69 Für dieses Beispiel wird angenommen, daß beide Fragen zu bejahen sind, und da der kritische Mechanismus ein kryptographischer Mechanismus ist, wird von den Evaluatoren kein Penetrations-test im Hinblick auf einen direkten Angriff oder eine operationelle Schwachstelle durchgeführt. Folg-lich können die Evaluatoren in bezug auf das Kriterium "Stärke der Mechanismen" eine *akzeptierende* Entscheidung aussprechen.

5.8.70 In diesem Beispiel gibt es nur einen kritischen Mechanismus, der beiden Sicherheitszielen gemein ist. In anderen Fällen, in denen es mehrere Sicherheitsziele gibt, könnte der kritische Mechanismus für jedes Ziel unterschiedlich sein.

5.8.71 Darüber hinaus ist ein kryptographischer Online-Angriff sehr schwierig, wenn nicht gar unmöglich, ohne daß die Schlüsselverwaltungsprozeduren unterlaufen werden und so "falsche" Schlüssel verwen-det werden können. Bei einem Offline-Angriff wie im Falle des Angriffsszenariums 8’ wäre es eventu-ell möglich, den Schlüssel aus der Analyse des chiffrierten Textes herzuleiten. In diesem Beispiel ist die SoM des Algorithmus und der Schlüsselverwaltungsverfahren stark genug, um dies zu verhindern.

5.8.72 In der vom Antragsteller durchgeführten Analyse der Stärke der Mechanismen wird ausführlich be-gründet, weshalb der Zugangskontrollmechanismus (CM2) des SWAN als starker Mechanismus be-schrieben wird, d. h. als ein Mechanismus, der nicht anfällig für direkte Angriffe ist (siehe Teil 6, An-hang 6.C). Dies kommt in der Analyse des Antragstellers zum Ausdruck, wo diesem Mechanismus eine *hohe* Stärke zuerkannt wird.

Benutzerfreundlichkeit

5.8.73 Bei diesem Aspekt der Wirksamkeit wird geprüft, ob der EVG in einer Weise konfiguriert oder genutzt werden kann, die unsicher ist, die aber von einem Systemverwalter oder Endanwender des EVG berechtigterweise für sicher gehalten würde.

5.8.74 Die vom Antragsteller durchgeführte Analyse der Benutzerfreundlichkeit muß die möglichen Betriebs-arten des EVG aufzeigen, darunter auch den Betrieb nach einer Funktionsstörung oder einem Bedienungsfehler, ihre Konsequenzen und ihre Auswirkungen auf die Aufrechterhaltung eines sicheren Systembetriebs. Sie muß außerdem nachweisen,

a) daß menschliches Versagen oder ein sonstiger Bedienungsfehler, durch den sicherheitsspezifi-sche Funktionen oder Mechanismen deaktiviert oder ausgeschaltet werden, leicht zu erkennen ist;

b) daß für den Fall, daß der EVG in einer Weise konfiguriert oder benutzt werden kann, die un-sicher ist (d.h. die sicherheitsspezifischen Funktionen und Mechanismen des EVG erfüllen die Sicherheitsvorgaben nicht), wohingegen ein Endanwender oder Systemverwalter des EVG diesen berechtigterweise für sicher halten würde, diese Tatsache ebenfalls leicht zu erkennen ist.

5.8.75 Die bekannten unsicheren Zustände des EVG sind im Angriffsszenarium aufgeführt. Ihre bloße Existenz weist darauf hin, daß es *durchaus* möglich ist, den EVG auf eine unsichere Weise zu benutzen oder zu konfigurieren (*Angreifer erhält autorisierte Dienstleistung durch geheime Absprache* ist ein Konfigurationsproblem). Die Frage lautet daher, ob in einem solchen Fall ein Systemverwalter oder Endanwender den EVG berechtigterweise für sicher halten würde.

5.8.76 Der Antragsteller versichert, daß dem Verhalten des EVG nach einer Funktionsstörung oder einem Bedienungsfehler, einschließlich der Konsequenzen und Auswirkungen auf die Aufrechterhaltung eines sicheren Systembetriebs, bereits nachgegangen worden ist – andernfalls wäre die Liste der Schwachstellen des Antragstellers unvollständig. Anders ausgedrückt müßte man sich im Falle der

Einbringung einer neuen Schwachstelle in dieser Phase (z. B. ein elektrisches Versagen der Kryptofunktionen) erneut mit den Kriterien für die Schwachstellenbewertung befassen.

5.8.77 In Anbetracht der vorausgegangenen Analysen in diesem Beispiel befaßt sich dieses Kriterium nur mit der Frage, ob es möglich ist zu erkennen, ob die kritischen Mechanismen des EVG versagt haben. Wenn ein kritischer Mechanismus versagt, befindet sich der EVG in einem unsicheren Zustand, oder er ist in Gefahr, in einen solchen Zustand zu geraten. Das Kriterium in den ITSEC verlangt lediglich, daß der EVG dies erkennt.

5.8.78 Der Antragsteller weist darauf hin, daß jedes Kryptogerät mit einer Kontrollampe ausgestattet ist, die aufleuchtet, sobald die betreffende Einheit im Chiffriermodus arbeitet, und erlischt, sobald sie sich im Klartextmodus befindet. Den Evaluatoren ist bekannt, daß diese Geräte ordnungsgemäß funktionieren (für dieses Beispiel wird angenommen, daß die Korrektheitskriterien erfolgreich angewandt worden sind). Die Lampen müssen an den HCU aller aktiven Host-Rechner permanent leuchten und dadurch klar zu erkennen geben, daß sowohl die Trennung der Endsysteme als auch die Vertraulichkeit der Datenübertragung gewährleistet ist.

5.8.79 Es ist jedoch zu beachten, daß diese Analyse komplexer werden kann, wenn weitere Funktionen (z. B. Beweissicherungsfunktionen) Bestandteil der Sicherungsvorgaben sind.

Penetrationstests

5.8.80 An diesem Punkt der Evaluation des SWAN haben die Evaluatoren alle Aktivitäten zur Prüfung auf Korrektheit abgeschlossen und hinsichtlich der Korrektheit des SWAN eine abschließende *akzeptierende* Entscheidung ausgesprochen. Aufgrund einer potentiellen Schwachstelle, die bei der Bewertung der Korrektheit festgestellt wurde, wiesen die Evaluatoren ausdrücklich auf eine Konstruktionsschwachstelle hin, die vom Antragsteller nicht erkannt wurde und daher in seiner Schwachstellenanalyse nicht enthalten war.

5.8.81 Wie in Teil 4, Kapitel 4.4 erläutert, können die Evaluatoren keine endgültige Entscheidung über die Wirksamkeit fällen, bevor die Penetrationstests abgeschlossen sind. Ziel der Penetrationstests ist es (laut Definition in den ITSEC) zu bestätigen oder zu widerlegen, daß die bekannten Schwachstellen in der Praxis wirklich ausgewertet werden können.

5.8.82 In diesem Beispiel wurde durch die Penetrationstests der Evaluatoren für das SWAN bestätigt, daß der Angreifer, wenn er Anwender eines Host-Rechners ist, die Kryptogeräte deaktivieren kann (V7), ohne über spezielle Kenntnisse oder Werkzeuge verfügen zu müssen (den Evaluatoren gelang dies ohne Hilfe und innerhalb von Minuten). Im Rückblick auf die unabhängige Schwachstellenanalyse der Evaluatoren zeigt Abbildung 5.8.7, daß die Angriffsszenarien 1', 4', 6' und 8' in ihrer Gesamtheit von dieser Schwachstelle betroffen sind.

5.8.83 Der kryptographische Mechanismus ist der einzige kritische Mechanismus im SWAN. Wenn in den Angriffsszenarien 1' und 8' der kryptographische Mechanismus versagt, ist das Sicherheitsziel S2 unmittelbar gefährdet, und Sicherheitsziel S1 wird dann nur durch *niedrige* Mechanismen verteidigt, die der postulierten Bewertung der Mindeststärke der Mechanismen des SWAN (*mittel*) nicht gerecht werden.

5.8.84 In den Angriffsszenarien 4' und 6' muß der Angreifer jedoch auch CM2 überwinden (mit *hoch* bewertet), um das Sicherheitsziel S2 zu verletzen; die Ergebnisse der Penetrationstests der Evaluatoren für das SWAN zeigen jedoch, daß CM2 von einem Angreifer ohne Hilfe und innerhalb weniger Tage überwunden werden könnte (aufgrund einer Konstruktionsschwachstelle V3).

5.8.85 Somit ist die Schwachstelle V7 in der Praxis ausnutzbar, weshalb die Evaluatoren in bezug auf die Analyse der Konstruktionsschwachstellen eine *ablehnende* Entscheidung aussprechen; und daher wird in bezug auf die Wirksamkeit des EVG eine endgültig *ablehnende* Entscheidung ausgesprochen.

Kapitel 5.9 Beispiel 8, Prüfung der Sicherheit beim Entwickler (E2 und E4)

Einleitung

5.9.1 In diesem Beispiel werden zwei Unterbeispiele (8(a) und 8(b)) vorgestellt, die jeweils einen Aspekt der Entwicklungsumgebung auf unterschiedlichen Evaluationsstufen behandeln.

Beispiel 8(a) – Prüfung der Sicherheit beim Entwickler (E2)

Einleitung

5.9.2 Dieses Unterbeispiel behandelt die Aufgaben zu Aspekt 3 der Entwicklungsumgebung – Sicherheit beim Entwickler. Dieses Beispiel soll in erster Linie veranschaulichen, wie die Sicherheit beim Entwickler untersucht werden kann. Für den Schutz der Entwicklungsumgebung wurden materielle und organisatorische Sicherheitsmaßnahmen eingesetzt.

ITSEC-Anforderungen an Inhalt und Form

5.9.3 *E2.21 Das Dokument über die Sicherheit der Entwicklungsumgebung muß die geplanten Schutzmaßnahmen bzgl. der Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumente darlegen. Materielle, organisatorische, personelle und andere Sicherheitsmaßnahmen, die durch den Entwickler eingesetzt werden, müssen dargelegt werden.*

ITSEC-Anforderungen an Nachweise

5.9.4 *E2.22 Die Information über die Sicherheit der Entwicklungsumgebung muß darlegen, wie die Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumentation gewährleistet werden.*

ITSEC-Aufgaben des Evaluators

5.9.5 *E2.23 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist nach Fehlern in den Verfahren zu suchen.*

Relevante Evaluationsbeiträge

5.9.6 Als Beitrag zu dieser Arbeit dienen die vom Antragsteller gelieferten Informationen über die Sicherheit der Entwicklungsumgebung und die Sicherheitsvorgaben des Produkts oder Systems, die die vermuteten oder tatsächlichen Bedrohungen aufweisen.

Durchgeführte Arbeiten

5.9.7 Die Informationen über die Sicherheitsmaßnahmen wurden in der Sicherheitsdokumentation des Entwicklers *dargelegt*. Die Dokumentation wurde von den Evaluatoren untersucht (durch Lesen und Verstehen). Insbesondere überprüften die Evaluatoren,

a) ob die materiellen Sicherheitsmaßnahmen geeignet waren, die Entwicklungsumgebung vor böswilligen Angriffen zu schützen;

b) ob die organisatorischen Sicherheitsmaßnahmen angemessen waren, um die Integrität des EVG zu schützen und die Vertraulichkeit der zugehörigen Dokumentation zu bewahren.

5.9.8 Die Evaluatoren hatten die Möglichkeit, den Entwicklungsort zu besichtigen und die Anwendung der vom Antragsteller angegebenen Sicherheitsmaßnahmen zu bestätigen, und zwar

a) durch Bewertung sonstiger vorgelegter Dokumente im Hinblick auf die Einhaltung der für die Sicherheitsmaßnahmen vorgesehenen Verfahren;

b) durch Befragung des Entwicklungspersonals, um herauszufinden, ob sie mit den Verfahren vertraut waren und diese in der Praxis anwandten.

5.9.9 Um des weiteren zu überprüfen, ob die dokumentierten Verfahren angewandt wurden, führten die Evaluatoren anschließend folgendes durch:

a) Überprüfung der Anwendung der materiellen Sicherheitsmaßnahmen;

b) Überprüfung der Anwendung der organisatorischen Sicherheitsmaßnahmen.

Beispiel 8(b) – Prüfung der Sicherheit beim Entwickler (E4)

Einleitung

5.9.10 Dieses Unterbeispiel behandelt die *Aufgaben zu Aspekt 3 der Entwicklungsumgebung – Sicherheit beim Entwickler*. Dieses Beispiel soll in erster Linie veranschaulichen, wie die Sicherheit beim Entwickler geprüft werden kann. Für den Schutz der Entwicklungsumgebung wurden materielle, organisatorische und technische Sicherheitsmaßnahmen eingesetzt.

ITSEC-Anforderungen an Inhalt und Form

5.9.11 *E4.21 Das Dokument über die Sicherheit der Entwicklungsumgebung muß die geplanten Schutzmaßnahmen bzgl. der Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumente darlegen. Materielle, organisatorische, personelle und andere Sicherheitsmaßnahmen, die durch den Entwickler eingesetzt werden, müssen beschrieben werden.*

ITSEC-Anforderungen an Nachweise

5.9.12 *E4.22 Die Information über die Sicherheit der Entwicklungsumgebung muß beschreiben, wie die Integrität des EVG und die Vertraulichkeit der zugehörigen Dokumentation gewährleistet werden.*

ITSEC-Aufgaben des Evaluators

5.9.13 *E4.23 Es ist zu überprüfen, ob die dokumentierten Verfahren angewendet werden. Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist nach Fehlern in den Verfahren zu suchen.*

Relevante Evaluationsbeiträge

5.9.14 Als Beitrag zu dieser Arbeit dienen die vom Antragsteller gelieferten Informationen über die Sicherheit der Entwicklungsumgebung sowie die Sicherheitsvorgaben des Produkts oder Systems, die die vermuteten oder tatsächlichen Bedrohungen aufweisen.

Durchgeführte Arbeiten

5.9.15 Die Informationen zu den Sicherheitsmaßnahmen wurden in der Sicherheitsdokumentation des Entwicklers *beschrieben.* Die Dokumentation wurde von den Evaluatoren untersucht (durch Lesen und Verstehen). Insbesondere überprüften die Evaluatoren,

a) ob die materiellen Sicherheitsmaßnahmen geeignet waren, die Entwicklungsumgebung vor böswilligen Angriffen zu schützen;

b) ob die organisatorischen Sicherheitsmaßnahmen angemessen waren, um die Integrität des EVG zu schützen und die Vertraulichkeit der zugehörigen Dokumentation zu bewahren;

c) ob die technischen Sicherheitsmaßnahmen angemessen waren, um die Integrität des EVG zu schützen und die Vertraulichkeit der zugehörigen Dokumentation zu bewahren.

5.9.16 Während der Vorlaufphase der Evaluation wurde ein Problem innerhalb des Konfigurationskontroll-systems festgestellt. Jedes Mitglied des Entwicklungsteams konnte den von einem anderen Mitglied des Entwicklungsteams erzeugten Quellcode ohne Autorisierung ändern. Das Problem wurde durch Aktivierung der Zugangskontrollfunktionen des Konfigurationskontrollsystems behoben, so daß jeder Entwickler nur noch seinen eigenen Quellcode ändern konnte.

5.9.17 Die Evaluatoren hatten die Möglichkeit, den Entwicklungsort zu besichtigen und die Anwendung der vom Antragsteller angegebenen Sicherheitsmaßnahmen zu bestätigen, und zwar:

a) durch Bewertung sonstiger vorgelegter Dokumente im Hinblick auf die Einhaltung der für die Sicherheitsmaßnahmen vorgesehenen Verfahren;

b) durch Befragung des Entwicklungspersonals, um herauszufinden, ob sie mit den Verfahren vertraut waren und diese in der Praxis anwandten.

5.9.18 Um des weiteren zu prüfen, ob die dokumentierten Verfahren angewandt wurden, führten die Evaluatoren anschließend folgendes durch:

a) Überprüfung der materiellen Sicherheitsmaßnahmen durch Testen. Die Evaluatoren überprüften, ob keine Möglichkeit zum Unterlaufen der verwendeten Verfahren bestand;

b) Überprüfung der organisatorischen Sicherheitsmaßnahmen durch Testen. Die Evaluatoren überprüften die Eignung der verwendeten Verfahren;

c) Überprüfung der technischen Sicherheitsmaßnahmen durch Testen. Die Evaluatoren überprüften die Eignung der verwendeten Verfahren nach Maßgabe des werkzeuggestützten Kon-figurationskontrollsystems.

Teil 6 Hinweise für andere Beteiligte

Inhalt

Abbildungen

Kapitel 6.1 Einleitung

Zielsetzung dieses Teils

6.1.1 Dieser Teil soll Antragstellern, Entwicklern, Herstellern, Anwendern und Systemakkreditierern, die mit der Sicherheit in der Informationstechnik (IT) befaßt sind, als Richtschnur dienen. Damit soll diesem Personenkreis die Möglichkeit gegeben werden, das ITSEM möglichst wirkungsvoll einzusetzen, und es soll ihnen zu einem besseren Verständnis des Evaluations- und Zertifizierungsprozesses verholfen werden.

6.1.2 Der wirksame Einsatz der IT ist ein wichtiger Faktor für den Erfolg eines Unternehmens; die Abhängigkeit von der IT nimmt ebenso wie die Vielseitigkeit ihrer Nutzung in allen Bereichen von Handel und Industrie immer weiter zu. Die Anwendung der IT ist jedoch auch mit potentiellen Risiken verbunden. Daher ist es wichtig, möglichst von Anfang an auf die Sicherheit zu achten und entsprechende Schutzmaßnahmen zu treffen. Eine Unterlassung kann gravierende Folgen haben, so z. B. den Verlust von **Werten**, die Schädigung des geschäftlichen Ansehens, die Nichterfüllung gesetzlicher Vorschriften oder eine mangelnde Anpassung an die Gegebenheiten des Marktes oder gar einen Zusammenbruch des Betriebs.

6.1.3 Die Anwender können nicht immer eine detaillierte Analyse der von einem Produkt oder System gebotenen Sicherheit durchführen und möchten sich daher auf den gegebenen Grad seiner Vertrauenswürdigkeit verlassen können.

6.1.4 Um attraktive Produkte oder Systeme anbieten zu können, müssen neue Leistungsmerkmale eingeführt werden; diese sollen jedoch zum günstigsten Zeitpunkt der Markteinführung und mit kontrollierten Fertigungskosten angeboten werden.

6.1.5 Aus den obigen Absätzen ergeben sich folgende Fragen:

a) Ist es zweckmäßig, Sicherheit ohne Vertrauenswürdigkeit zu bieten?

b) Ist es möglich, Vertrauenswürdigkeit ohne eine Evaluation zu erreichen?

c) Kann eine Evaluation ohne allzu hohe Zusatzkosten durchgeführt werden?

6.1.6 Sicherheit soll als inhärentes Qualitätsmerkmal eines Produkts oder Systems betrachtet werden, und der Evaluationsprozeß ist das Hilfsmittel, mit dem die Vertrauenswürdigkeitsstufe der Sicherheit eines Produkts oder Systems ermittelt werden kann.

Zusammenhang zwischen diesem Teil und den anderen Teilen des ITSEM

6.1.7 Dieser Teil richtet sich an alle Beteiligten, die mit der Sicherheit in der Informationstechnik laut Definition in Teil 1 des ITSEM befaßt sind, und beschreibt die Aufgaben und Tätigkeiten dieser Beteiligten im Evaluationsprozeß.

6.1.8 Spezifische Hinweise für Beteiligte, die am Zertifizierungsprozeß beteiligt sind (ITSEF, Antragsteller und **Zertifizierungsstelle**), sind in Teil 2 des ITSEM und in der Dokumentation des **nationalen Regelwerks** enthalten.

6.1.9 Spezifische Hinweise für die am Evaluationsprozeß beteiligten Evaluatoren (ITSEF) sind in Teil 4 des ITSEM zu finden.

6.1.10 Dieser Teil enthält Hinweise zu Aspekten der IT-Sicherheit, die in den anderen Teilen des ITSEM nicht behandelt werden:

a) Vorbereitung auf die Evaluation: Es werden Hinweise gegeben, die gewährleisten sollen, daß die am Evaluations- und Zertifizierungsprozeß beteiligten Stellen ausreichend auf eine wirksame Evaluation vorbereitet sind.

b) Vor oder während der Evaluation: Es werden Hinweise zum Entwicklungsprozeß gegeben.

c) Nach der Evaluation: Es werden Hinweise zur Verwendung der Evaluationsergebnisse gegeben.

d) Nach der Zertifizierung: Es werden Hinweise zur Verwendung des **Zertifikats/Zertifizierungsreports** gegeben.

e) Nach der Evaluation und Zertifizierung: Es werden Hinweise für Änderungen an einem evaluierten System oder Produkt gegeben.

Aufbau und Zusammenfassung dieses Teils

6.1.11 Dieser Teil besteht aus mehreren Kapiteln und Anhängen. Diese einleitenden Bemerkungen bilden Kapitel 6.1.

6.1.12 Die mit der IT-Sicherheit befaßten Beteiligten und ihre Verantwortlichkeiten werden in Kapitel 6.2 beschrieben.

6.1.13 Kapitel 6.3 enthält Hinweise für Sicherheitsanbieter (d. h. Antragsteller, Entwickler und Hersteller).

6.1.14 Kapitel 6.4 enthält Hinweise für Sicherheitsanwender (d. h. Anwender und Systemakkreditierer).

6.1.15 Anhang 6.A enthält Hinweise für Antragsteller und Entwickler zur Bereitstellung von **Evaluationsbeiträgen** für die Evaluatoren.

6.1.16 Anhang 6.B richtet sich an Antragsteller und Systemakkreditierer und enthält ein Beispiel für die Ableitung von Sicherheitsvorgaben.

6.1.17 Anhang 6.C enthält Hinweise zu Mechanismen und zur Wirksamkeit.

6.1.18 Anhang 6.D richtet sich an Antragsteller und Systemakkreditierer und beschreibt die **Auswirkungsanalyse** als Mittel zur Bestimmung der Auswirkungen von Änderungen an einem evaluierten System oder Produkt auf die Zertifizierung.

6.1.19 Anhang 6.E enthält allgemeine Hinweise für Entwickler von Evaluationswerkzeugen.

6.1.20 Anhang 6.F richtet sich an Antragsteller, Systemintegrierer und Systemakkreditierer, die mit dem Zusammenfügen früher evaluierter EVG befaßt sind.

Kapitel 6.2 Mit der IT-Sicherheit befaßte Beteiligte

Einleitung

6.2.1 Folgende Beteiligte sind mit der IT-Sicherheit befaßt (siehe Teil 1 des ITSEM):

a) Antragsteller, die eine Evaluation beantragen, die Sicherheitsvorgaben für ein zu evaluierendes Produkt oder System festlegen, die Kosten der Evaluation tragen und das Zertifikat/den Zertifizierungsreport entgegennehmen.

b) Entwickler (einschließlich Systemintegrierer), die das zu evaluierende Produkt oder System herstellen und die für die Evaluation geforderten Evaluationsbeiträge liefern.

c) ITSEFs, die das Produkt oder System evaluieren.

d) Nationale Zertifizierungsstellen, die den Evaluationsprozeß überwachen und die Zertifikate/Zertifizierungsreporte herausgeben.

e) Hersteller, die evaluierte Produkte verkaufen und vertreiben.

f) Anwender, die zum Schutz ihrer Werte ein evaluiertes Produkt oder System einsetzen.

g) Systemakkreditierer, die für die Sicherheit eines evaluierten Systems verantwortlich sind.

6.2.2 Eine einzelne Stelle kann mehrere Rollen wahrnehmen und beispielsweise als Antragsteller und Entwickler, Antragsteller und Hersteller oder Anwender und Systemakkreditierer usw. auftreten.

6.2.3 Die Angabe spezifischer Hinweise für ITSEFs und nationale Zertifizierungsstellen fällt nicht in den Rahmen dieses Teils.

Verantwortlichkeiten der beteiligten Stellen

6.2.4 Die Zielsetzungen der beteiligten Stellen lassen sich wie folgt einteilen:

a) die Gewährleistung, daß ein EVG angemessene Sicherheit bietet;

b) die Reduzierung oder Kontrolle der Kosten für diese Sicherheit;

c) die Bereitstellung der geforderten Sicherheit innerhalb eines angemessenen zeitlichen Rahmens.

6.2.5 In vielen Fällen muß ein Kompromiß zwischen diesen Zielsetzungen gefunden werden.

6.2.6 Der Antragsteller ist verantwortlich für

a) die Bestimmung der Sicherheitsvorgaben;

b) die Definition des EVG;

c) die Bereitstellung der für die Evaluation angeforderten Evaluationsbeiträge;

d) die Verwendung des Zertifikats/Zertifizierungsreports;

e) die Pflege der Evaluationsbewertung.

6.2.7 Der Entwickler ist verantwortlich für

a) die Spezifikation des EVG;

b) die Produkt- oder Systementwicklung;

c) die Erstellung der für die Evaluation angeforderten Evaluationsbeiträge;

d) die Pflege des Produkts oder Systems;

e) den Schutz seines Know-Hows und der firmeneigenen Informationen.

6.2.8 Der Hersteller ist verantwortlich für

a) den Produktvertrieb;

b) die Produktwerbung;

c) die Beratung;

d) die Produktinstallation.

6.2.9 Der Anwender ist verantwortlich für

a) die Produkt- oder Systemauswahl;

b) den Produkt- oder Systemanlauf;

c) den Produkt- oder Systemeinsatz;

d) die Produkt- oder Systemkonfigurierung.

6.2.10 Der Systemakkreditierer ist verantwortlich für

a) die Festlegung der System-Sicherheitspolitik;

b) die Festlegung der Regeln für eine Systemänderung;

c) die Einschätzung der geforderten Vertrauenswürdigkeitsstufe;

d) die Zulassung eines Systems für den betrieblichen Einsatz.

6.2.11 Diese Liste ist nicht verbindlich, da unterschiedliche Organisationen wohl auch die Verantwortlichkeiten unterschiedlich zuweisen.

6.2.12 Eine ITSEF kann bei der Spezifikation oder Realisierung des EVG beratend tätig sein, darf aber keine Ratschläge geben, die ihre Unabhängigkeit beeinträchtigen würden (siehe Teil 4, Kapitel 4.2).

Kapitel 6.3 Hinweise für Antragsteller, Entwickler und Hersteller (Sicherheitsanbieter)

Einleitung

6.3.1 Sicherheitsanbieter sind Beteiligte, die einen Beitrag zum Evaluationsprozeß liefern (d. h. Antragsteller und Entwickler) sowie Beteiligte, die Sicherheitsdienstleistungen erbringen (d. h. Vertreiber). Dieses Kapitel behandelt die folgenden Themen:

a) Bestimmung der Sicherheitsvorgaben (relevant für Antragsteller);

b) Starten von Produktevaluationen (relevant für Antragsteller und Hersteller);

c) Bereitstellung und Verwaltung von Evaluationsbeiträgen (relevant für Antragsteller und Entwickler);

d) den Entwicklungsprozeß (relevant für Entwickler);

e) spezielle Entwicklungstechniken (relevant für Entwickler);

f) Verwendung von ETR und Zertifikaten/Zertifizierungsreporten (relevant für Entwickler);

g) Zertifikatspflege (relevant für Antragsteller und Entwickler);

h) Vertrieb zertifizierter Produkte (relevant für Hersteller);

i) Installierung und Konfigurierung von Produkten (relevant für Hersteller);

j) Integration von Produkten (relevant für Hersteller und Entwickler);

k) Beratung (relevant für Hersteller).

Bestimmung der Sicherheitsvorgaben

6.3.2 Es ist Sache des Antragstellers, die Sicherheitsvorgaben für einen EVG zu liefern. Die Zielsetzungen von Sicherheitsvorgaben sind folgende:

a) die Bereitstellung einer Spezifikation der Sicherheitsfunktionalität des EVG;

b) das Herstellen eines Bezugs zwischen dem EVG und der Umgebung, in der er eingesetzt werden soll;

c) die Bereitstellung der Grundlage für die Evaluation.

6.3.3 Zur Zielgruppe der Sicherheitsvorgaben können daher folgende Beteiligte gehören:

a) der Entwickler des EVG – die Sicherheitsvorgaben definieren die Sicherheitsanforderungen des EVG;

b) die Evaluatoren – die Sicherheitsvorgaben bilden die Basis, anhand derer der EVG bewertet wird;

c) der Hersteller oder der Anwender des EVG – die Sicherheitsvorgaben legen die Sicherheitsziele des EVG für die Beteiligten fest, die für die Verwaltung, die Beschaffung, die Installation, die Konfigurierung und den Betrieb des EVG zuständig sind.

6.3.4 Wie in den ITSEC (Absätze 2.4 – 2.26 und 4.11) dargelegt, wird der geforderte Inhalt der Sicherheitsvorgaben dadurch bestimmt, ob es sich beim EVG um ein System oder ein Produkt handelt. Der Inhalt läßt sich wie folgt zusammenfassen:

a) entweder eine System-Sicherheitspolitik oder eine Produktbeschreibung;

b) eine Spezifikation der geforderten sicherheitsspezifischen Funktionen;

c) eine Definition geforderter Sicherheitsmechanismen (optional);

d) die postulierte Bewertung der Mindeststärke der Mechanismen;

e) die angestrebte Evaluationsstufe.

6.3.5 Die Sicherheitsvorgaben bilden die Grundlage für die Evaluation und unterliegen selbst der Evaluation.

6.3.6 Die Erstellung von Sicherheitsvorgaben für einen EVG, die den Kriterien in den ITSEC entsprechen, setzt die genaue Anwendung eines methodischen Ansatzes voraus. Insbesondere sollen die Sicherheitsvorgaben mit Hilfe eines Top-Down-Ansatzes definiert werden, bei dem folgende Punkte der Reihe nach zu berücksichtigen sind:

a) die Eingrenzung des Bereichs: Risikoanalyse;

b) Betriebsspezifikationen: Sicherheitspolitik;

c) Funktionsspezifikationen: die sicherheitsspezifischen Funktionen;

d) Implementierungsspezifikationen: die erforderlichen Mechanismen und die Mindeststärke der Mechanismen;

e) Evaluationsspezifikationen: die angestrebte Evaluationsstufe.

6.3.7 Weitere Hinweise zum Inhalt der Sicherheitsvorgaben sowie ein Top-Down-Ansatz für ihre Erstellung sind in Anhang 6.B zu finden.

Starten von Produktevaluationen

6.3.8 Der Einsatz von Standardlösungen ist für die Erfüllung der allgemeinen Anforderungen häufig kostengünstiger. Dies kann für die Sicherheitsanforderungen ebenso gelten wie für beliebige andere Anforderungen.

6.3.9 Vom sicherheitstechnischen Standpunkt aus betrachtet kann ein Produkt folgendes sein:

a) ein Sicherheitsprodukt, das für einen spezifischen Sicherheitszweck als einzigen oder primären Zweck entwickelt wurde (z. B. ein Produkt, das die Identifikation und **Authentisierung** auf einem Desktop-PC implementiert);

b) ein sicheres Produkt, das auf die Gewährleistung einer spezifischen Sicherheitsstufe als Ergänzung zu seiner wesentlich umfangreicheren Funktionalität ausgerichtet ist (z. B. ein Betriebssystem).

6.3.10 Die Entscheidung, ein Sicherheitsprodukt oder ein sicheres Produkt zu entwickeln oder zu vermarkten, kann unter anderem von folgenden Faktoren abhängen:

a) von den Anwendern wahrgenommene Bedrohungen ihrer Werte (z. B. Viren-Angriffe);

b) nationale oder internationale gesetzliche Anforderungen (z. B. das US Computer Security Act);

c) nationale oder internationale Normen (z. B. Bereitstellung von Sicherheit in X.400 oder X.500);

d) eine Marktnische (z. B. Zugangskontrollgeräte für Personal Computer).

6.3.11 Die wirtschaftlichen Rahmenbedingungen spielen stets eine ausschlaggebende Rolle bei der Entscheidung. Der Antragsteller muß eine ganze Reihe von Fragen berücksichtigen, die für die Marktfähigkeit des Produkts relevant sind. Diese Fragen können beispielsweise wie folgt lauten:

a) Wer sind die potentiellen Kunden?

b) Warum ist Sicherheit für diese potentiellen Kunden von Bedeutung?

c) Welche Sicherheitsstufe (hinsichtlich Funktionalität und Vertrauenswürdigkeit) wird von diesen potentiellen Kunden verlangt?

6.3.12 Die Anforderungen und Auswirkungen der Produktzertifizierung werden ebenfalls berücksichtigt:

a) Soll die Evaluation und Zertifizierung im Rahmen eines anerkannten Regelwerks angestrebt werden?

b) Welche wirtschaftlichen und gesetzlichen Auswirkungen bringt eine solche Entscheidung mit sich (z. B. Ausfuhrkontrolle)?

6.3.13 Ausgehend von bestimmten Annahmen zu den obigen Punkten soll der Antragsteller einen Geschäftsplan für sein Produkt erstellen, wobei auch die voraussichtlichen Wettbewerber in diesem Bereich zu berücksichtigen sind.

Lieferung und Verwaltung von Evaluationsbeiträgen

6.3.14 Der Antragsteller ist für die Bereitstellung der den Evaluatoren während des Evaluationsprozesses zur Verfügung stehenden Evaluationsbeiträge zuständig.

6.3.15 Der Begriff *Evaluationsbeitrag* bezeichnet all das (einschließlich des EVG selbst), was den Evaluatoren für die Evaluation zugänglich gemacht werden muß. Hierzu gehören auch immaterielle Beiträge wie die Unterstützung der Evaluatoren (z. B. gegebenenfalls durch Schulung) und der Zugang zu Rechnern.

6.3.16 Der Zweck der Evaluationsbeiträge besteht darin, den Evaluatoren die Evaluation des EVG zu ermöglichen. Dieser Zweck wird von verschiedenen Arten von Evaluationsbeiträgen auf unterschiedliche Weise erfüllt. Dazu gehören

a) Evaluationsbeiträge, die einen Nachweis der Wirksamkeit oder Korrektheit bieten, z. B. eine informelle Beschreibung des Zusammenhangs zwischen Quellcode und Feinentwurf;

b) Evaluationsbeiträge, mit denen die Evaluatoren einen zusätzlichen Nachweis der Wirksamkeit oder Korrektheit erbringen können, z. B. der Zugang zu dem entwickelten EVG;

c) Evaluationsbeiträge, die die Effizienz der Arbeit der Evaluatoren insgesamt verbessern, z. B. die technische Unterstützung durch den Entwickler.

6.3.17 Ausführliche Hinweise für Antragsteller und Entwickler zu Inhalt und Verwaltung der Evaluationsbeiträge sind in Anhang 6.A zu finden.

6.3.18 Der Antragsteller soll sicherstellen, daß die Vereinbarungen mit dem Entwickler

a) so genau abgefaßt sind, daß gewährleistet ist, daß die Evaluatoren die erforderlichen Evaluationsbeiträge erhalten;

b) so verbindlich sind, daß gewährleistet ist, daß unzureichende Evaluationsbeiträge eine Nicht-erfüllung der vertraglichen Vereinbarungen bedeuten.

6.3.19 Es ist Sache des Antragstellers, den Evaluatoren sämtliche erforderlichen Evaluationsbeiträge zur Verfügung zu stellen, die von Subunternehmern erstellt werden oder die mit von Dritten hergestellten Produkten in Zusammenhang stehen (z. B. Quellcode).

6.3.20 Werden die erforderlichen Evaluationsbeiträge nicht innerhalb eines angemessenen Zeitrahmens oder nicht in angemessener Qualität geliefert, kann dies zu einer Unterbrechung der Evaluation bis zur Bereitstellung geeigneter Evaluationsbeiträge führen, da eine Fortführung der Evaluation unter Umständen nicht möglich ist.

6.3.21 Der Entwickler muß alle erwarteten Evaluationsbeiträge bis zu den bei Beginn der Evaluation vereinbarten Terminen liefern. Um dieser Verpflichtung nachzukommen, soll der Entwickler

a) die Übereinstimmung zwischen der Liste der Evaluationsbeiträge und dem von ihm erstellten Entwicklungsplan bestätigen;

b) die Übereinstimmung zwischen der Liste der Evaluationsbeiträge und den von ihm erzielten Ergebnissen des Entwicklungsprozesses bestätigen;

c) die Übereinstimmung zwischen dem zu erwarteten Grad an Information und den von ihm angewandten Entwicklungsmethoden bestätigen.

6.3.22 Gelegentlich kann der Fall eintreten, daß der Entwickler zwar der Evaluation und der Lieferung der Evaluationsbeiträge an die ITSEF zustimmt, daß er aber den Zugriff des Antragstellers auf firmeneigene Informationen einschränken möchte. Der Entwickler soll zur gegebenen Zeit sicherstellen, daß Art und Umfang der firmeneigenen Informationen bestimmt wird, und er soll Grundregeln für ihren Schutz festlegen.

6.3.23 Vor einer Evaluation soll der Antragsteller in Übereinstimmung mit den nationalen Gesetzesvorschriften

a) alle erforderlichen Rechtsansprüche auf den EVG und sonstige Evaluationsbeiträge im Hinblick auf die Evaluation begründen und der ITSEF und der Zertifizierungsstelle die diesbezüglichen Rechte übertragen (ihr Schadloshaltung zusichern);

b) (gegebenenfalls) die schriftliche Zustimmung des Entwicklers zu etwaigen besonderen Verein-barungen über die Beschränkung des Zugriffs auf firmeneigene Informationen einholen.

6.3.24 Im Anschluß an die Entscheidung, ein Produkt oder ein System evaluieren zu lassen, soll sich der Entwickler bereit erklären, die ihm übertragenen Verantwortlichkeiten im Rahmen des Evaluationsprozesses zu übernehmen.

Der Entwicklungsprozeß

6.3.25 Vom Entwickler wird die Bereitstellung von Evaluationsbeiträgen zum Nachweis der Erreichung der angestrebten Vertrauenswürdigkeitsstufe erwartet (siehe Anhang 6.A). Dieser Nachweis soll im Rahmen des Entwicklungsprozesses erbracht werden bzw. im Anschluß an die Entwicklung, wenn die Evaluation nicht das ursprüngliche Ziel war.

6.3.26 Die ITSEC gehen von einer Gliederung des Entwicklungsprozesses in die folgenden vier Phasen aus:

a) Die Anforderungsphase:

Bei einem System fällt diese Phase in die Zuständigkeit des Antragstellers (häufig ist jedoch der Entwickler eines Produkts zugleich auch der Antragsteller einer Evaluation). Für den Entwickler ist es wichtig, daß in dieser Phase die gesamten Sicherheitsanforderungen und ihre Logik genau definiert und analysiert und so die Stärken und Schwächen des vorgesehenen Produkts oder Systems bestimmt werden.

b) Die Architekturphase:

In dieser Phase werden die Sicherheitsanforderungen zur Entwicklung einer Sicherheitsarchitektur und zur Festlegung eines Katalogs von Sicherheitsfunktionen herangezogen. Besonders zu beachten ist dabei die Trennung der sicherheitsspezifischen und sicherheitsrelevanten Funktionen von den anderen Funktionen.

c) Die Feinentwurfsphase:

Diese Phase ist eine Verfeinerung der Architekturphase, in der die Funktionalität der einzelnen Komponenten sichtbar wird. Besonders zu beachten sind dabei die Stärken und Schwächen der in Frage kommenden Programmiersprachen im Zusammenhang mit den geforderten Sicherheitsfunktionen und -mechanismen.

d) Die Implementierungsphase:

Während dieser Phase implementiert der Entwickler die Funktionen, die für die in der Entwurfsphase beschriebenen Sicherheitseigenschaften sorgen. Besonders zu beachten ist dabei die Anwendung der Entwicklungsregeln; außerdem sollen Inspektionen oder Stufentests Bestandteil der verwendeten Entwicklungsmethodik sein.

Außerdem folgt der Entwickler einem vordefinierten Testplan. Besonders zu beachten sind dabei der Aspekt der Vollständigkeit des Testplans und die Aufzeichnung der durchgeführten Tests und der entsprechenden Ergebnisse, die als Beiträge zur Evaluation bereitzustellen sind.

6.3.27 Die folgenden allgemeinen Hinweise bieten in allen obengenannten Phasen Hilfestellung bei der Erfüllung der Kriterien in den ITSEC:

a) Die Entwickler sollen einem strukturierten Ansatz folgen, um die Erstellung eines Codes zu unterstützen, der leicht zu lesen, einfach zu pflegen und innerhalb der Verfeinerungsstufen problemlos zu verfolgen ist.

b) Durch Analysieren der Entwurfsinformationen und des Quellcodes einer sicherheitsrelevanten Komponente kann ein Angreifer unter Umständen eine Möglichkeit entdecken, ein Sicherheitsziel zu verletzen. Die Entwickler sollen ihre firmeneigenen Informationen daher schützen.

c) Entwicklern wird empfohlen, den Programmierern die direkte Verantwortung für die von ihnen zu entwickelnden Programme zu übertragen. Hierdurch wird das Verständnis für die Sicherheitsanforderungen im Verlauf der Entwicklung gefördert.

d) Entwickler sollen im Rahmen des Prozesses zur Identifizierung potentieller Sicherheitsprobleme und Funktionsstörungen ein gegenseitiges Kontrollverfahren beschließen.

Spezielle Entwicklungstechniken

Einleitung

6.3.28 Dieser Abschnitt enthält für Entwickler bestimmte Hinweise zu speziellen Entwicklungstechniken, die für die höheren Vertrauenswürdigkeitsstufen relevant sind.

Werkzeuggestützte Konfigurationskontrollsysteme

6.3.29 Auf den höheren Evaluationsstufen wird von den Entwicklern die Verwendung eines werkzeuggestützten Konfigurationskontrollsystems verlangt. Dieser Unterabschnitt enthält Hinweise zur Auswahl und Entwicklung derartiger Systeme.

6.3.30 Das Konfigurationsmanagementsystem soll gewährleisten, daß für den EVG in sämtlichen Phasen seines Lebenszykluses eine klare, vollständige und unverfälschte **Darstellung** vorhanden ist. Diese Darstellung soll alle an der Konfiguration vorgenommenen Änderungen widerspiegeln.

6.3.31 Ein werkzeuggestütztes Konfigurationskontrollsystem soll eine klar definierte Konfigurationsmanagementpolitik durchsetzen und folgendes umfassen:

a) die Abbildbarkeit jeder am EVG aufgrund einer genehmigten Änderungsanforderung vorgenommenen Änderung;

b) die Abbildbarkeit von Ursache und Wirkung aller im EVG aufgrund einer Änderung aufgetretenen Funktionsstörungen;

c) die Analyse der Auswirkungen von Änderungen auf unverändert gebliebene Komponenten;

d) die Festlegung der Verantwortlichkeiten für die Änderungskontrolle;

e) die Kontrolle des Zugangs zu EVG-Software-Modulen während ihrer Entwicklung;

f) die Abstimmung der Implementierung von EVG-Änderungen und der Aktualisierung der EVG-Dokumentation;

g) die Erstellung etwaiger Vorversionen des EVG;

h) die Protokollierung implementierter Kontrollverfahren;

i) die Protokollierung der Beweissicherungsverfahren für den EVG-Status.

6.3.32 Es muß Vertrauen in die kontrollierte Implementierung des EVG aufgebaut werden. Alle Änderungen am EVG sollen autorisiert und kontrolliert erfolgen, damit sichergestellt ist, daß sie die Fähigkeit der sicherheitsspezifischen und sicherheitsrelevanten Funktionen, die System-Sicherheitspolitik oder Produktbeschreibung umzusetzen, nicht beeinträchtigen. In diesem Zusammenhang kann der Einsatz digitaler Signaturen hilfreich sein.

Formale Methoden

6.3.33 Die Anwendung formaler Methoden, die von den ITSEC auf den höheren Stufen zwingend vorgeschrieben ist, bereitet den Entwicklern aufgrund ihrer Neuartigkeit mitunter Schwierigkeiten. Dieser Unterabschnitt enthält Hinweise zur Auswahl formaler Techniken und Werkzeuge.

6.3.34 *Zugrundeliegende formale Spezifikation und Beschreibungstechniken*: Auf Stufe E6 verlangen die ITSEC eine formale Beschreibung der Architektur des EVG und eine formale Spezifikation der sicherheitsspezifischen Funktionen.

6.3.35 Nach den ITSEC-Anforderungen für E6 kann ein formaler Vergleich zwischen der formalen Beschreibung der Architektur und dem zugrundeliegenden formal spezifizierten Sicherheitsmodell vorgenommen werden. Dieser Vergleich ist nicht immer einfach: Formale Techniken werden gegenwärtig in erster Linie für die Beschreibung und den Nachweis statischer Eigenschaften von EVG eingesetzt. In diesem Fall bedarf es einer Kombination aus formalen und informellen Techniken (wie in Absatz E6.6 in den ITSEC dargelegt).

6.3.36 Ein weiterer Vergleich kann zwischen der formalen Spezifikation der sicherheitsspezifischen Funktionen und ihrer Umsetzung im EVG vorgenommen werden. Eine präzise formale Spezifikation der Funktionalität des EVG beinhaltet die Anwendung einer mathematischen Notation und ist daher abstrakt. Es handelt sich um eine funktionale oder semantische Definition der Funktion eines Systems, ohne daß dargelegt wird, auf welche Weise dies verwirklicht werden soll. Anhand einer formalen Spezifikation der Funktionalität des EVG können Eigenschaften des EVG formal dargelegt und nachgewiesen werden. Zusätzlich dient sie als genauer Standard für die Implementierung.

6.3.37 Eine formale Darstellungsform einer Spezifikation ist in einer formalen Notation geschrieben, die auf wohlbegründeten mathematischen Konzepten aufbaut (ITSEC Absatz 2.76). Für die meisten formalen Notationen werden die Konstrukte der mathematischen Logik (Prädikatenkalkül und in jüngster Zeit modale Logik) und die Mengenlehre herangezogen.

6.3.38 Es gibt drei sich gegenseitig ergänzende Techniken oder Methoden der formalen Beschreibung. Operationelle Definitionen bedienen sich eines abstrakten Interpretierers zur Definition des EVG. Diese sind am wenigsten abstrakt und ähneln Implementierungen. Begriffliche Beschreibungen bilden den EVG direkt auf seine Bedeutung ab. Axiomatische oder Gleichungsdefinitionen beschreiben Eigenschaften des EVG.

6.3.39 Es wird empfohlen, daß Entwickler sich bei der Auswahl der Techniken für die formale Spezifikation und Beschreibung an folgenden Überlegungen orientieren:

a) Stufen: Damit die Systementwickler oder Anwender die formale Beschreibung je nach Wunsch mit einem hohen oder einem niedrigen Detaillierungsgrad betrachten können, soll die Beschreibung in Stufen eingeteilt sein, die vom Top-Level-Kontrollfluß bis zu den Einzelheiten jeder Operation reichen.

b) Modular: Mit Ausnahme der obersten Stufe der formalen Beschreibung sollen alle Stufen modular sein. Auf diese Weise kann der Entwurf jeder Operation isoliert betrachtet werden.

c) Knapp: Die Notation soll die Möglichkeiten bieten, die erforderlichen Begriffe in knapper Form auszudrücken. Eine umständliche oder langatmige Notation bläht die Beschreibung unnötig auf.

d) Verständlich: Die Notation der formalen Spezifikation muß leicht verständlich sein.

e) Abstrakt: Die formale Beschreibung soll keine Problemstellungen erzwingen, die eigentlich erst in der Implementierungsphase behandelt werden müssen. Zwar ist der Top-Level-Kontrollfluß für den Systementwurf entscheidend, doch ist es häufig so, daß auf niedrigeren Stufen die Ordnung bestimmter Ereignisse unerheblich ist.

f) Solide: Damit formale Nachweise der Korrektheit geführt werden können, soll die Beschreibungstechnik über eine solide mathematische Grundlage verfügen.

6.3.40 *Werkzeuge für die formale Spezifikation*: Kurz ausgedrückt werden diese als Werkzeuge zur Implementierung – und Techniken zur Anwendung – mathematischer Logik bezeichnet. Diese Werkzeuge und Techniken sind darauf ausgerichtet, schlüssig zu beweisen, daß der EVG seine Spezifikation genau erfüllt. Formale Methoden, die durch ein Werkzeug unterstützt werden, müssen genauer definiert werden durch

a) eine formal spezifizierte Syntax und Semantik für die verwendeten Notationen;

b) Algorithmen zur Manipulation von Formeln der Sprachen;

c) eine Menge von Prüfregeln, mit denen die Korrektheit (Vollständigkeit und Eindeutigkeit) der Spezifikation abgeleitet werden kann;

d) eine Rahmenstruktur zur Verfeinerung einer Spezifikation in eine konkrete Implementierung.

6.3.41 Die *Ausdrucksfähigkeit der formalen Spezifikationssprachen*, die von einem Werkzeug verwendet werden, muß ausreichen, um die Sicherheitspolitik und die Komponenten eines IT-Systems, die diese Politik umsetzen, formal zu beschreiben, z.B. hinsichtlich invarianter Prädikate. Für die formale Spezifikationssprache müssen Konzepte zur Aufgliederung der Entwurfsspezifikation in hierarchisch geordnete Spezifikationsstufen vorhanden sein, damit eine Entwurfsspezifikation von der Top-Level-Spezifikation des EVG bis hinunter zu den Programmspezifikationen auf den unteren Stufen verfeinert werden kann.

Verwendung von ETR und Zertifikaten/Zertifizierungsreports

6.3.42 In einigen nationalen Regelwerken sind Zertifikate/Zertifizierungsreports offizielle Erklärungen einer staatlichen Einrichtung und unterliegen daher den für diese amtlichen Veröffentlichungen geltenden Bestimmungen. Anwender von ETR und Zertifikaten/Zertifizierungsreports müssen sich an die in Teil 2 des ITSEM aufgeführte zuständige nationale Stelle wenden.

6.3.43 Der Antragsteller ist verpflichtet, auf seine Ansprüche an Evaluationsergebnissen zu verzichten, durch die die firmeneigenen Informationen des Entwicklers gefährdet würden. Wird eine Evaluation nicht bestanden, darf der Antragsteller das Ergebnis nicht in einer den Interessen des Entwicklers zuwiderlaufenden Weise verwenden.

6.3.44 Nach Abschluß einer Evaluation wird der ETR der Zertifizierungsstelle zur Verfügung gestellt. Während des Evaluations- und Zertifizierungsprozesses ist der ETR ein Zwischendokument und stellt nicht die endgültige Entscheidung dieses Prozesses dar.

6.3.45 Der ETR wird dem Antragsteller zugänglich gemacht. Er wird unbeschadet des offiziellen Zertifikats/Zertifizierungsreports in vertraulicher Form und mit der Maßgabe freigegeben, daß er auf einen beschränkten Personenkreis der Belegschaft des Antragstellers beschränkt bleibt und nicht ohne Zustimmung der Zertifizierungsstelle an Dritte weitergegeben werden darf. Der ETR sollte mit *Evaluation-in-Confidence* (vertrauliche Evaluationsunterlagen) gekennzeichnet sein.

6.3.46 Falls der Antragsteller Bedenken im Hinblick auf Aussagen im ETR oder im Zertifikat/Zertifizierungsreport hat, kann er diese mit der ITSEF bzw. der Zertifizierungsstelle besprechen.

6.3.47 Die Zertifizierungsstelle prüft den ETR, um herauszufinden, inwieweit die Sicherheitsvorgaben durch den EVG erfüllt werden und ob die ITSEFs die Evaluation in Übereinstimmung mit den Anforderungen des ITSEM durchgeführt hat; anschließend kann die Zertifizierungsstelle die postulierte Evaluationsstufe bestätigen. Ihre Schlußfolgerungen werden im Zertifikat/Zertifizierungsreport festgehalten.

6.3.48 Die Verwendung der Evaluationsergebnisse und der Zertifikate/Zertifizierungsreports soll durch spezifische Anforderungen des nationalen Regelwerks eingeschränkt werden.

Pflege von Zertifikaten/Zertifizierungsreports

6.3.49 Ein Zertifikat/Zertifizierungsreport bezieht sich nur auf das Release/die Version des EVG, das/die evaluiert wurde; alle Änderungen an einem zertifizierten EVG unterliegen den für die Reevaluation festgelegten Vorschriften (ausführliche Hinweise sind in Anhang 6.D zu finden).

6.3.50 Der Antragsteller darf ein Produkt nur auf der Grundlage eines gültigen Zertifikats/Zertifizierungsreports als zertifiziertes Produkt auf den Markt bringen und muß gewährleisten, daß zur Verhinderung nichtautorisierter Änderungen für die Evaluationsstufe geeignete Konfigurationsmanagementverfahren vorhanden sind. Die Evaluatoren werden unter Umständen aufgefordert, das Evaluationsmaterial für eine spätere **Reevaluation** zu archivieren.

6.3.51 Wenn ein EVG oder seine Betriebs- oder Entwicklungsumgebung später geändert wird, ist es Sache des Antragstellers, die Art der Änderung zu klassifizieren und die Auswirkungen auf das Zertifikat/den Zertifizierungsreport zu bestimmen.

6.3.52 Die Art der Änderung bestimmt, ob der Antragsteller die Zertifizierungsstelle von ihr in Kenntnis setzen muß. Für den Antragsteller kann sich auch die Notwendigkeit ergeben, Vorkehrungen für eine Reevaluation zu treffen.

6.3.53 Die an dem Pflegeprozeß beteiligten Entwickler sollen die Schaffung eines speziellen Sicherheitsteams in Erwägung ziehen, das eine Auswirkungsanalyse aller geplanten oder implementierten Änderungen durchführt.

6.3.54 Der Pflegeprozeß kann durch die bei der Entwicklung verfolgte Strategie der Zuweisung individueller Verantwortlichkeiten unterstützt werden (siehe 6.3.27.c) und kann einen Reviewprozeß umfassen, der zur Vorbereitung der für die Reevaluation des EVG benötigten Informationen dient und unter anderem folgendes umfaßt:

a) eine Zusammenfassung der Änderungen seit dem letzten evaluierten Release;

b) eine Beschreibung aller sicherheitsrelevanten Änderungen und die Sicherheitsanalyse dieser Änderungen.

6.3.55 Antragsteller und Entwickler werden dazu angehalten, die Frage der Reevaluation und die Zertifikatspflege bereits während der Entwicklung des EVG und der Vorbereitung auf die ursprüngliche Evaluation zu berücksichtigen.

Vertrieb zertifizierter Produkte

6.3.56 Antragsteller, Entwickler und Hersteller sind unter Umständen am Vertrieb zertifizierter Produkte interessiert.

6.3.57 Vertreiber zertifizierter Produkte sind verpflichtet,

a) das Zertifikat/den Zertifizierungsreport zum Produkt vorzulegen, wenn dies von potentiellen Anwendern verlangt wird;

b) keine irreführenden Aussagen zum Produkt zu machen (z. B. zu behaupten, ein Produkt sei zertifiziert, obwohl dies nicht stimmt, oder die Vorzüge des Produkts übertrieben darzustellen);

c) bekannte Probleme zertifizierter Produkte potentiellen Anwendern mitzuteilen;

d) falls eine **Schwachstelle** in einem zertifizierten Produkt festgestellt wird, bestehenden Anwendern dies mitzuteilen;

e) bei Änderungen an einem zertifizierten Produkt das neue Produkt erst nach Aktualisierung der Zertifizierung/des Zertifizierungsreports für zertifiziert auszugeben.

6.3.58 Das wichtigste Dokument für den Hersteller beim Verkauf eines Produkts sind die Sicherheitsvorgaben.

Installieren und Konfigurieren eines Produkts

6.3.59 Die Installation und Konfiguration erfolgt im allgemeinen durch den Entwickler, den Hersteller oder (bei einfachen Produkten) den Anwender.

6.3.60 Die mit der Installation und Konfiguration der Produkte betrauten Personen sollen

a) die Auslieferungsanweisungen des Produkts genau befolgen;

b) die Konfigurationsoptionen entsprechend der Konfigurationsdokumentation des Produkts auswählen und die vollzogenen Schritte aufzeichnen, damit die Produktkonfiguration anschließend bekannt ist;

c) das entsprechende Verfahren zur Überprüfung der Authentizität des EVG befolgen und festgestellten Abweichungen nachgehen.

6.3.61 In dieser Phase ist die Dokumentation zur *Betriebsumgebung* für den Hersteller von größtem Nutzen.

Integrieren von Produkten

6.3.62 Es kommt häufig vor, daß mehrere evaluierte Produkte zu einem kombinierten Produkt oder System zusammengefügt werden müssen. Dies führt bei Produkten oft zu Problemen.

6.3.63 Auf Wunsch kann der Entwickler neue Sicherheitsvorgaben für das integrierte Produkt oder System erstellen und eine Evaluation anhand der neuen Sicherheitsvorgaben veranlassen. In diesem Fall kommen die Hinweise für die **Wiederverwendung** in Teil 4, Kapitel 4.3 und 4.6, zur Anwendung. Nach erfolgreicher Zertifizierung kann der Hersteller geltend machen, daß das integrierte Produkt oder System anhand der neuen Sicherheitsvorgaben zertifiziert worden ist.

6.3.64 Als Alternative dazu braucht der Hersteller lediglich zu überprüfen, ob das integrierte Produkt oder System alle in den Sicherheitsvorgaben aller Einzelprodukte genannten Voraussetzungen erfüllt, ohne eine Evaluation veranlassen zu müssen. In diesem Fall kann der Hersteller geltend machen, daß jedes Produkt anhand der eigenen Sicherheitsvorgaben zertifiziert worden ist, er darf aber keine Behauptungen hinsichtlich der Sicherheitsvorgaben des integrierten Systems oder Produkts aufstellen. Insbesondere darf er keine Behauptungen darüber aufstellen, wie gut die zertifizierten Produkte zusammenarbeiten werden.

6.3.65 Anhang 6.F enthält ein einfaches Modell für das Zusammenfügen von zwei bereits früher evaluierten Komponenten. Dieses Beispiel ist für alle diejenigen von Interesse, die sich mit der Frage der Systemintegration befassen.

Erteilen von Ratschlägen

6.3.66 Anwender, die die Anschaffung evaluierter Produkte in Erwägung ziehen, fragen in vielen Fällen den Entwickler, den Hersteller oder die ITSEFs um Rat.

6.3.67 Wer Ratschläge erteilt, ist verpflichtet,

a) nur unparteiische Ratschläge zu erteilen; das heißt, die Ratschläge sollen den Belangen des Anwenders dienen; jede Beteiligung des Beratenden an einem bestimmten Produkt muß dem Anwender mitgeteilt werden;

b) keine Ratschläge außerhalb seines Kompetenzbereichs zu erteilen.

Kapitel 6.4 Hinweise für Sicherheitsanwender

Einleitung

Hintergrund

6.4.1 Dieses Kapitel enthält Hinweise für Sicherheitsanwender, d. h. Antragsteller, Systemakkreditierer und Anwender von evaluierten Systemen und Produkten. Es behandelt folgende Themen:

a) Sicherheitsevaluation (eine grundlegende Einführung, die für Anwender von Interesse ist);

b) Anwender und Evaluation (für Anwender von Interesse);

c) Definition der Anforderungen (für Systemakkreditierer von Interesse);

d) Systemabnahme (für Systemakkreditierer von Interesse);

e) Pflege der Akkreditierung (für Systemakkreditierer von Interesse).

6.4.2 Im vorliegenden Kapitel soll keine umfassende Einführung in Sicherheitskonzepte gegeben werden; diese werden in zahlreichen anderen Veröffentlichungen behandelt [GASSER]. Es soll lediglich die Bedeutung der Sicherheitsevaluation und ihre Konsequenzen für Anwender und Systemakkreditierer erläutern.

Anwender

6.4.3 Anwender lassen sich in folgende Kategorien einteilen:

a) Endanwender , die ein IT-System für ihre normale Arbeit einsetzen;

b) Bediener, die für den Anlauf, das Herunterfahren, die Datensicherung und andere Routineaufgaben im Rahmen der Systemkontrolle verantwortlich sind;

c) Systemverwalter, die für die Erstellung von Anwender-ID, die Systemkonfiguration, die Zuweisung von Dateizugriffsrechten und ähnliche anspruchsvolle Kontrollfunktionen verant-wortlich sind.

6.4.4 Diese Aufgaben bedingen eine unterschiedlich große Einflußnahme auf die Sicherheit eines IT-Systems, die von überhaupt keiner Einflußnahme bis zu einer für die Wahrung der Systemsicherheit eminent wichtigen Einflußnahme reichen kann.

Systemakkreditierer

6.4.5 Ein Systemakkreditierer ist eine Person oder eine Organisation, die für die Sicherheit eines Systems, einschließlich seiner materiellen, personellen und organisatorischen Sicherheitseigenschaften, sowie für die von einem IT-System bereitgestellten technischen Eigenschaften verantwortlich ist.

6.4.6 Als Systemakkreditierer kommen folgende Personen in Frage:

a) Eigentümer von Daten, d.h. diejenigen, die die in einem IT-System zu speichernden Daten besitzen und Gewißheit haben möchten, daß das System sicher ist;

b) der bereichsinterne Sicherheitsbeauftragte, der für die gesamte IT-Sicherheit innerhalb eines Teilbereichs einer großen Organisation verantwortlich ist;

c) eine nationale Organisation, die dafür verantwortlich ist, daß Informationen, die für die nationale Sicherheit von Bedeutung sind, geschützt werden.

6.4.7 Bei der Bewertung der Sicherheit eines Systems stützt sich ein Systemakkreditierer in der Regel auf eine betriebsinterne Sicherheitspolitik, die für eine Abteilung oder Organisation oder in manchen Fällen nur für das betroffene System festgelegt sein kann. In dieser Sicherheitspolitik sollen sämtliche für das System geltenden Sicherheitsregeln oder -bestimmungen aufgezeigt werden, auch etwaige Nicht-IT-Anforderungen, die zu erfüllen sind.

6.4.8 Um Vertrauen in die Sicherheit eines Systems zu schaffen, führt ein Systemakkreditierer ein Verfahren in der Art einer High-Level-Evaluation durch, womit er nachweist, daß die Kombination aus IT-, materiellen, personellen und organisatorischen Maßnahmen die wirksame Umsetzung der für das System geltenden Sicherheitspolitik ermöglicht.

6.4.9 Die detaillierte technische Evaluation der IT-Komponenten eines Systems wird in der Regel von einer ITSEF durchgeführt. Ein Systemakkreditierer muß so viel vom Evaluations- und Zertifizierungsprozeß eines IT-Systems verstehen, daß die Ergebnisse der Evaluation für die Akkreditierung herangezogen werden können.

6.4.10 Ein Systemakkreditierer ist am Lebenszyklus eines sicheren Systems in erster Linie in den folgenden drei Phasen beteiligt:

a) während der anfänglichen Festlegung der Anforderungen;

b) wenn für die Betriebsbereitschaft des Systems eine Abnahme erforderlich ist;

c) wenn ein System verändert oder aufgerüstet wird.

Sicherheitsevaluation

6.4.11 Es ist unmöglich, praktisch einsetzbare IT-Systeme herzustellen, die absolut sicher sind. Dies ist durch die Komplexität der IT-Systeme bedingt wie auch durch die Vielzahl der Bedrohungen, denen sie begegnen müssen.

6.4.12 Es besteht jedoch die Möglichkeit, ein gewisses Vertrauen in die Sicherheit eines Rechnersystems zu schaffen. Die bevorzugte Lösung besteht in der eingehenden Prüfung des Systementwurfs und der Dokumentation durch eine unabhängige Stelle, Evaluationsstelle für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT Security Evaluation Facility, ITSEF) genannt, um Sicherheitsschwachstellen aufzudecken. Diese Prüfung wird als Sicherheitsevaluation bezeichnet. Ein System besteht diese Evaluation, wenn festgestellt wird, daß es keine ausnutzbaren Sicherheits-schwachstellen aufweist; andernfalls besteht es die Evaluation nicht.

6.4.13 Wenn ein System eine Sicherheitsevaluation bestanden hat, bietet es zwar mit großer Wahrscheinlichkeit einen gewissen Grad von Sicherheit, jedoch kann es aus folgenden Gründen nicht als absolut sicher angesehen werden:

a) Es können Schwachstellen vorhanden sein, die von den Evaluatoren aufgrund der ihnen zur Verfügung stehenden Informationen nicht entdeckt worden sind;

b) das System kann auf eine unsichere Weise genutzt, bedient, verwaltet oder konfiguriert werden;

c) einige der Bedrohungen in der Betriebsumgebung wurden unter Umständen nicht in die Sicherheitsvorgaben aufgenommen.

6.4.14 Ein evaluiertes System soll daher als etwas betrachtet werden, das bei der Aufrechterhaltung der Sicherheit einer Organisation eine Rolle spielt, jedoch nicht die gesamte Verantwortung für die Sicherheit trägt. Auch die verschiedenen Anwender müssen ihren Beitrag dazu leisten.

Anwender und evaluierte Systeme

Allgemeines

6.4.15 Aus sicherheitstechnischer Sicht können Anwender in zwei Kategorien eingeteilt werden: vertrauens-würdige und nicht vertrauenswürdige Anwender.

6.4.16 Systemverwalter werden in der Regel als besonders vertrauenswürdige Anwender angesehen, da auf-grund der besonderen Systemprivilegien, die sie für ihre Arbeit benötigen, und des ihnen gewährten Zugangs zum System die Sicherheit dieses Systems entscheidend davon abhängt, ob sie ihre Pflichten zuverlässig erfüllen.

6.4.17 Endanwender werden in der Regel als weniger vertrauenswürdig angesehen und erhalten daher nur beschränkt Zugang zu den die Sicherheit betreffenden Systemfunktionen; außerdem kommt ihnen nur eine begrenzte Rolle bei der Aufrechterhaltung der Systemsicherheit zu.

Vertrauenswürdige Anwender

6.4.18 Die folgenden Beispiele betreffen sicherheitsbezogene Aufgaben, die von vertrauenswürdigen Anwendern übernommen werden können:

a) Erstellen und Löschen von Anwender-ID;

b) Konfigurieren des Systems;

c) Auswählen von Dateizugangsberechtigungen;

d) Überprüfen von Protokollaufzeichnungen zur Aufspürung versuchter Sicherheitsverletzungen.

6.4.19 Ein evaluiertes System soll mit der entsprechender Systemverwalter-, Auslieferungs-, Konfigurations-, Anlauf- und Betriebsdokumentation ausgestattet sein. Während der Evaluation haben die ITSEF-Evaluatoren die vorhandene Dokumentation auf ihre Richtigkeit überprüft und nachgeprüft, ob mit ihr bei genauer Befolgung die Sicherheit aufrechterhalten werden kann. Daher sollen vertrauenswürdige Anwender bei der Erfüllung ihrer Sicherheitsaufgaben diese Dokumentation genau befolgen.

6.4.20 Ein evaluiertes System verfügt stets über Sicherheitsvorgaben, in denen die erforderliche Betriebsumgebung zur Gewährleistung der Sicherheit in Übereinstimmung mit den Evaluationsergebnissen definiert ist. Vertrauenswürdige Anwender sind für die Pflege dieser Betriebsumgebung verantwortlich, damit die durch die Evaluationsergebnisse bestätigte Stufe der Vertrauenswürdigkeit aufrechterhalten werden kann.

Nicht vertrauenswürdige Anwender

6.4.21 Die folgenden Beispiele betreffen sicherheitsbezogene Aufgaben, die von nicht vertrauenswürdigen Anwendern übernommen werden können:

a) Anmelden beim System;

b) Abmelden vom System;

c) Auswählen von Paßwörtern;

d) Auswählen von Zugriffsberechtigungen für eigene Dateien.

6.4.22 Diese Aufgaben sind zwar für die Sicherheit nicht so wichtig wie die der vertrauenswürdigen Anwender, jedoch kann eine unsachgemäße Durchführung die Sicherheit der Anwenderdaten oder sogar die des gesamten Systems gefährden.

6.4.23 Ein evaluiertes System soll mit einer Benutzerdokumentation ausgestattet sein. Während der Evaluation haben die ITSEF-Evaluatoren die vorhandene Dokumentation auf ihre Richtigkeit überprüft und nachgeprüft, ob mit ihr bei genauer Befolgung die Sicherheit aufrechterhalten werden kann. Daher sollen nicht vertrauenswürdige Anwender bei der Erfüllung ihrer Aufgaben diese Dokumentation genau befolgen.

Bestimmung der Anforderungen

6.4.24 Während der anfänglichen Bestimmung der Anforderungen kann ein Systemakkreditierer im Hinblick auf die zu verwendende Sicherheitspolitik um Rat gefragt oder bei der Entwicklung der Sicherheits-vorgaben für ein IT-System hinzugezogen werden.

6.4.25 Für gewöhnlich wird ein Systemakkreditierer in diesem Stadium gebeten, den bei der Entwicklung des Systems zu verwendenden Ansatz zu genehmigen; daher kann sich die Notwendigkeit ergeben, in einem frühen Projektstadium eine umfassende Sicherheitsbewertung vorzunehmen.

6.4.26 Eine Bewertung der Sicherheit eines Systems auf hoher Stufe erfolgt in der Regel mit den Mitteln der Risikoanalyse, wobei alle denkbaren Bedrohungen den vorhandenen **Gegenmaßnahmen** gegenüber-gestellt werden. Es gibt eine ganze Reihe von Verfahren auf Anwender- und Behördenseite, die für die Durchführung dieser Analyse herangezogen werden können wie etwa [BDSS], [CRAMM], [GISA2], MARION und MELISA. Diese Verfahren sind speziell auf die funktionale Sicherheit ausgerichtet und bieten wenig oder keine Anhaltspunkte für den erforderlichen Grad des Vertrauens in die Korrektheit und Wirksamkeit der Gegenmaßnahmen. Sie behandeln jedoch auch Aspekte von Gegenmaßnahmen der Nicht-IT-Sicherheit, die für einen Systemakkreditierer von Interesse sind.

6.4.27 Der Systemakkreditierer hat zu gewährleisten, daß die gesamte Palette der von der Risikoanalyse aufgezeigten Gegenmaßnahmen vorhanden ist und daß diese Gegenmaßnahmen zur Erfüllung der Sicherheitspolitik wirksam zusammenarbeiten. Diese Analyse entspricht der Bewertung der Wirksamkeit, die im Rahmen einer IT-Evaluation anhand der ITSEC durchgeführt wird, schließt aber auch Nicht-IT-Gegenmaßnahmen ein.

6.4.28 Einige der Gegenmaßnahmen werden von IT-Komponenten des Systems zur Verfügung gestellt; ihre Sicherheitseigenschaften werden entweder in einer Sicherheitsvorgabe für alle IT-Aspekte oder in mehreren Sicherheitsvorgaben für getrennte Systemkomponenten definiert. Im letzteren Fall hat der Systemakkreditierer dafür zu sorgen, daß die IT-Komponenten im System wirksam zusammen-arbeiten.

6.4.29 Der Systemakkreditierer muß zusätzlich zur Festlegung der erforderlichen Sicherheitsfunktionalität den geforderten Grad der Vertrauenswürdigkeit oder des Vertrauens in die Systemsicherheit bestimmen. Derzeit verwendete Verfahren bedienen sich einer qualitativen Bewertung des Risikos, dem das System ausgesetzt ist, um einen geforderten Grad an Vertrauen zuzuweisen.

6.4.30 Diese Richtlinien können zwar auch in anderen Bereichen verwendet werden, sie wurden aber für militärische Anwendungen entwickelt und sind primär nur mit dem Geheimhaltungsaspekt der Sicherheit befaßt. Wenn sie auch für andere Sicherheitsaspekte und andere Einsatzbereiche als Richtschnur dienen sollen, sind weitere Arbeiten erforderlich.

6.4.31 Besonders problematisch für Systemakkreditierer ist die Bestimmung der erforderlichen Evaluationsstufe für IT-Komponenten eines Systems, bei dem der Systementwurf mehrere Komponenten umfaßt.

6.4.32 Unter Umständen müssen die Systemakkreditierer für Anwender sicherer Systeme Schulungen veranstalten.

6.4.33 Systemakkreditierer müssen Zugriff auf eine Vielzahl von Informationen über das System haben, wozu in der Regel folgende gehören:

a) Systemspezifikationen;

b) auf das System und auf höhere Stufen bezogene Sicherheitspolitik;

c) Definitionen von Nicht-IT-Sicherheitsfunktionen;

d) Sicherheitsvorgaben für IT-Komponenten;

e) Dokumentation über die Betriebsverfahren für das System, auch für die IT-Komponenten;

f) Zertifikate/Zertifizierungsreports (und eventuell ETR) für vorevaluierte Komponenten.

Systemabnahme

6.4.34 Bei der Entwicklung eines Systems oder der Evaluation der zugehörigen IT-Komponenten können sich Änderungen ergeben und Schwachstellen aufgedeckt werden. Im Verlauf der Evaluation festgestellte Probleme werden mit Hilfe des Mechanismus der Erstellung eines **Mängelberichts** gemeldet, der im nationalen Regelwerk festgelegt ist.

6.4.35 Systemakkreditierer müssen die sicherheitstechnischen Auswirkungen gemeldeter Mängel und geplanter Änderungen berücksichtigen. Nach Abschluß der Evaluation(en) wird der Systemakkreditierer an der Entscheidung darüber, ob ein System in Betrieb genommen werden kann, mitbeteiligt. In beiden Fällen muß der Systemakkreditierer ein Urteil darüber abgeben, ob die geforderte Sicherheitsstufe erreicht worden ist oder erreicht werden wird.

6.4.36 Dazu kann es erforderlich sein, daß Teile der im vorausgegangenen Abschnitt beschriebenen Analyse wiederholt werden, allerdings mit präziseren Informationen über die tatsächliche oder geplante Implementierung des Systems.

6.4.37 Der Systemakkreditierer hat festzustellen, ob **ausnutzbare Schwachstellen** in den IT-Komponenten (die im ETR dokumentiert sind) durch bereits vorhandene Nicht-IT-Maßnahmen angemessen abgedeckt sind oder ob weitere Nicht-IT-Maßnahmen hinzukommen müssen, bevor das System in Betrieb genommen werden kann.

Pflege der Systemakkreditierung

6.4.38 Während der Nutzungsdauer eines Systems werden Änderungen an seiner Konfiguration, seinen Komponenten und seiner operationellen Nutzung vorgenommen. Diese Änderungen müssen von einer Akkreditierstelle dahingehend bewertet werden, ob die Sicherheitsanforderungen weiterhin erfüllt sind.

6.4.39 Anhang 6.D befaßt sich mit der Frage, wie festgestellt werden kann, ob bei bereits evaluierten IT-Komponenten eine Reevaluation erforderlich ist. Vom Systemakkreditierer ist ein analoges Verfahren anzuwenden, in das jedoch auch die Nicht-IT-Aspekte des Systems einbezogen werden müssen.

Anhang 6.A Evaluationsbeiträge

Einleitung

6.A.1 Im vorliegende Anhang, der insbesondere für Antragsteller und Entwickler bestimmt ist, sind die Anforderungen der ITSEC an Evaluationsbeiträge zusammengefaßt und erläutert.

Verantwortung für Evaluationsbeiträge

6.A.2 Die Verantwortung für die Bereitstellung aller geforderten Evaluationsbeiträge liegt beim Antragsteller. Allerdings werden die meisten Evaluationsbeiträge vom Entwickler erstellt und geliefert (sofern der Antragsteller nicht der Entwickler ist). Daher empfiehlt es sich, in den Vertrag zwischen Antragsteller und Entwickler auch genaue Einzelheiten darüber aufzunehmen, was der Entwickler zu erstellen hat und welche Folgen ein Versäumnis, ordnungsgemäße Evaluationsbeiträge zu erstellen, haben wird.

6.A.3 Im Rahmen einer Einzelvereinbarung zwischen Antragsteller und ITSEF müssen gegebenenfalls folgende Details geklärt werden:

a) Datenträger und Format maschinenlesbarer Evaluationsbeiträge;

b) der Zeitplan für die Erstellung der Evaluationsbeiträge;

c) die Anzahl der vorzulegenden Ausfertigungen der Evaluationsbeiträge;

d) die Sachlage bei Evaluationsbeiträgen in Entwurfsform;

e) Vereinbarungen über andere in Verbindung mit dem EVG zu verwendende Produkte;

f) Vereinbarungen über die Besprechung der Entwicklungsumgebung mit dem Entwickler;

g) Zutritt zum Betriebs- und zum Entwicklungsort;

h) Art und Dauer der Entwickleruntersützung, einschließlich Rechnerzugang und von den Evaluatoren benötigte Räumlichkeiten.

6.A.4 In vielen Fällen müssen die Evaluatoren die Möglichkeit des Zugriffs auf Informationen von Unterauftragnehmern oder Dritten haben. In den zu treffenden Vereinbarungen sollen solche Fälle berücksichtigt werden.

6.A.5 Die Betriebskosten und -risiken (z.B. Verluste oder Schäden durch Feuer, Wasser, Diebstahl usw.) für sämtliche Evaluationsbeiträge sind vom Antragsteller zu tragen, es sei denn, mit den Evaluatoren ist ausdrücklich etwas anderes vereinbart worden. Dabei ist zu beachten, daß bei manchen Evaluationsbeiträgen wie etwa neuen oder Sonderzwecken dienenden Gerätetypen der Wieder-beschaffungswert nicht so ohne weiteres ermittelt werden kann und diese somit durchaus ein Versicherungsrisiko darstellen können, das nicht an die Evaluatoren weitergeben werden kann.

Behandlung von Evaluationsbeiträgen

In Entwurfsform vorgelegte Evaluationsbeiträge

6.A.6 Für Evaluationen werden stabile und offiziell herausgegebene Versionen der Evaluationsbeiträge benötigt. Gelegentlich kann es jedoch für die Evaluatoren von Nutzen sein, auch Einblick in Entwurfsversionen bestimmter Evaluationsbeiträge zu bekommen wie etwa

a) Testunterlagen, die ihnen eine frühzeitige Bewertung von Tests und Testprozeduren ermöglichen;

b) Quellcode oder Hardware-Konstruktionszeichnungen, die ihnen die Möglichkeit geben, die Anwendung der Standards des Entwicklers zu bewerten.

6.A.7 Evaluationsbeiträge in Entwurfsform werden am ehesten dann vorgelegt, wenn die Evaluation eines EVG parallel zu seiner Entwicklung erfolgt. Sie können jedoch auch bei der nachfolgenden Evaluation eines Produkts oder Systems vorgelegt werden, wenn der Entwickler zusätzliche Arbeiten durchführen muß, um einen von den Evaluatoren festgestellten Mangel zu beheben (z.B. einen **Fehler** in der Konstruktion) oder um einen Sicherheitsnachweis zu erbringen, der in der vorhandenen Dokumentation nicht erbracht wird (z.B. die Wirksamkeit betreffende Evaluationsbeiträge im Falle eines Produkts oder Systems, das ursprünglich nicht mit Blick auf eine Evaluation entwickelt wurde).

6.A.8 Zugegebenermaßen sind Entwickler im allgemeinen nur ungern bereit, Evaluationsbeiträge im Entwurfsstadium an Evaluatoren weiterzugeben. Allerdings liegt es im Interesse des Antragstellers, Entwürfe bereitzustellen, da der Entwickler frühzeitig Rückmeldungen über sicherheitsbezogene Mängel oder Fehler bekommen kann, wodurch sich ein etwaiger späterer Nachbesserungsaufwand verringert.

Konfigurationskontrolle

6.A.9 Für eine Evaluation nach E1 braucht der Antragsteller nur eine Konfigurationsliste vorzulegen, aus der die Version des zu evaluierenden EVG hervorgeht. Wenn als Evaluationsstufe E2 oder eine höhere Stufe angestrebt wird, müssen die von den Evaluatoren benötigten Evaluationsbeiträge

a) einer laufenden Konfigurationskontrolle unterzogen werden;

b) eindeutig identifiziert sein (z.B. durch die Versionsnummer).

6.A.10 Diese Anforderung gilt für alle materiellen Evaluationsbeiträge, einschließlich beispielsweise aller verlangten Nachweise der Wirksamkeit oder Korrektheit, wie etwa einer Beschreibung der Art und Weise, wie der Architekturentwurf eines EVG die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung stellen wird.

6.A.11 An den Evaluationsbeiträgen sollen möglichst wenig Änderungen vorgenommen werden. Geänderte Evaluationsbeiträge müssen den Evaluatoren so früh wie möglich zugeleitet werden.

Die Sicherheitsvorgaben

6.A.12 Die Festlegung der Sicherheitsvorgaben ist Sache des Antragstellers. Ziel der Sicherheitsvorgaben ist es,

a) eine Spezifikation der Sicherheitsfunktionalität eines EVG zur Verfügung zu stellen;

b) einen EVG mit der Betriebsumgebung, für die er bestimmt ist, in Bezug zu bringen;

c) die Grundlage für die Evaluation zu schaffen.

6.A.13 Die vorgesehene Zielgruppe von Sicherheitsvorgaben sind daher

a) der Entwickler des EVG: in den Sicherheitsvorgaben sind die Sicherheitsanforderungen des EVG definiert;

b) die Evaluatoren: die Sicherheitsvorgaben liefern die Basiswerte, anhand derer der EVG evaluiert wird;

c) der Anwender eines EVG (d.h. die für die Verwaltung, die Beschaffung, die Installierung, die Konfigurierung und den Betrieb des EVG verantwortlichen Personen): in den Sicherheitsvorgaben sind alle erforderlichen Informationen für die Bewertung der Eignung des EVG für eine geplante Anwendung enthalten.

6.A.14 Welche Anforderungen an den Inhalt und an die Spezifikationsform eines EVG gestellt werden, hängt davon ab, ob der EVG ein System oder ein Produkt ist und welche Evaluationsstufe angestrebt wird. Zusammenfassend lassen sich diese wie folgt darstellen:

- System-Sicherheitspolitik *oder* Produktbeschreibung;
- eine Spezifikation der geforderten sicherheitsspezifischen Funktionen;
- eine Definition der erforderlichen Sicherheitsmechanismen (optional);
- die postulierte Mindeststärke der Mechanismen;
- die angestrebte Evaluationsstufe.

Evaluationsbeiträge

Allgemeines

6.A.15 Die allgemeinen Anforderungen an Evaluationsbeiträge sind in Abbildung 6.A.1 und 6.A.2 aufgeführt. Einige zusätzliche Anforderungen an Evaluationsbeiträge sind in den ITSEC impliziert, jedoch nicht explizit beschrieben. In der Regel werden insbesondere folgende die Entwicklungsumgebung im allgemeinen betreffende Evaluationsbeiträge benötigt:

a) Zugang zu früheren Evaluationsergebnissen (z.B. für die Reevaluation eines EVG oder wenn ein evaluiertes Produkt eine Komponente des EVG ist);

b) Zutritt zum Entwicklungsort, einschließlich Zugriff auf die Entwicklungswerkzeuge, sowie Räumlichkeiten für die Befragung (einiger Mitarbeiter) des Entwicklungsteams;

c) Zugang zum EVG in seiner Betriebsumgebung;

d) technische und logistische Unterstützung seitens des Entwicklers.

6.A.16 Es besteht keine Notwendigkeit, für jeden die Wirksamkeit betreffenden Evaluationsbeitrag ein getrenntes Dokument zu erstellen. Es ist durchaus möglich und in manchen Fällen vorzuziehen, daß nur ein einziges Dokument vorliegt, das die Wirksamkeit in ihrer Gesamtheit abdeckt.

Verwendung von Produkten als Komponenten eines EVG

6.A.17 Aus einer ganzen Reihe von Alternativen kann eine zur Bereitstellung von Evaluationsbeiträgen für ein Produkt gewählt werden, das eine sicherheitspezifische oder sicherheitsrelevante Komponente darstellt. So können/kann beispielsweise

a) die Ergebnisse einer früheren Evaluation des Produkts vorgelegt werden;

b) das Produkt genauso behandelt werden wie der übrige Teil des EVG; in diesem Fall sollen die entsprechenden produktspezifischen Evaluationsbeiträge mitgeliefert werden.

6.A.18 Die für eine bestimmte Evaluation gewählte Vorgehensweise muß für die Zertifizierungsstelle, den Antragsteller und die Evaluatoren akzeptierbar sein. Für die Fälle, in denen vorhandene Evaluationsergebnisse wiederverwendet werden sollen, sind zusätzliche Hinweise in Teil 4, Kapitel 4.6, zu finden.

Entwicklungsumgebung

6.A.19 Die Evaluatoren benötigen Unterlagen über die Konfigurationskontrolle, die Programmiersprachen und Compiler sowie über die im Verlauf der Entwicklung eines EVG verwendete oder praktizierte Sicherheit beim Entwickler. Außerdem benötigen sie Unterlagen allgemeinerer Art über die während der Entwicklung des EVG verwendeten Prozeduren, Methoden, Werkzeuge und Standards wie z.B.

a) einen Qualitätsplan einschließlich Entwicklungsprozeduren;

b) detaillierte Angaben über die verwendeten Entwicklungsmethoden;

c) detaillierte Angaben über die verwendeten Entwicklungswerkzeuge;

d) Software-Codierstandards.

6.A.20 Die Evaluatoren benötigen einen Nachweis über die Einhaltung von Prozeduren und Standards sowie einen Nachweis darüber, daß die Methoden und Werkzeuge korrekt angewendet worden sind, wie z.B.

a) den Konfigurationsmanagementplan;

b) Konfigurationskontrollaufzeichnungen;

c) das Protokoll der Entwurfsreviews.

6.A.21 Außerdem kann sich die Notwendigkeit eines oder mehrerer gezielter Besuche der Evaluatoren beim Entwickler zur Besprechung der Entwicklungsumgebung ergeben. Die Gesprächsthemen bei solchen Besuchen sind in Abbildung 6.A.3 aufgelistet.

6.A.22 Die Evaluatoren haben keinen Zugang zu Unterlagen, die ausschließlich Finanz-, Vertrags- oder Personalangelegenheiten betreffen (mit Ausnahme der Personalangelegenheiten, die in den Rahmen der Kriterien in den ITSEC für die Sicherheit beim Entwickler fallen).

Betriebsumgebung

6.A.23 Die Evaluatoren benötigen Unterlagen über die Verwendung, die Verwaltung, die Auslieferung, die Konfiguration, den Anlauf und den Betrieb des EVG.

6.A.24 Die Evaluatoren müssen Zugang zu dem betriebsbereiten EVG haben, um Penetrationstests durchführen zu können. Handelt es sich bei dem EVG um ein System, müssen die Evaluatoren, soweit möglich, auch Zutritt zum Betriebsort haben, damit sie

a) mit Vertretern der Anwender die Betriebsprozeduren betreffende Aspekte besprechen können;

b) Penetrationstests in der Betriebsumgebung durchführen können.

6.A.25 Handelt es sich bei dem EVG um ein Produkt, müssen die Evaluatoren Zugang zu einer Betriebsimplementierung dieses Produkts haben, um Penetrationstests durchführen zu können. Der Antragsteller kann den EVG entweder am Entwicklungsort bereithalten, oder die erforderlichen Einrichtungen können stattdessen den Evaluatoren leihweise zur Verfügung gestellt und die Penetrationstests bei der ITSEF durchgeführt werden.

Hilfestellung bei der Evaluation

6.A.26 Die Evaluatoren können im Rahmen einer Evaluation die Hilfe des Antragstellers und des Entwicklers in Logistik-, Beratungs- und Schulungsfragen in Anspruch nehmen.

6.A.27 Eine namentlich benannte Person in der Organisation des Entwicklers soll als Ansprechpartner für die gesamte Unterstützungsleistung durch den Entwickler fungieren. Diese Person oder ersatzweise benannte Personen

a) soll/sollen in der Lage sein, umgehend Hilfestellung zu leisten;

b) sollen in der Lage sein, gegebenenfalls mit anderen Mitarbeitern des Entwicklers Kontakt aufzunehmen, falls detaillierte Informationen zu bestimmten Aspekten des EVG benötigt werden.

6.A.28 In welchem Umfang insgesamt Hilfestellung benötigt wird, hängt von der jeweiligen Evaluation ab. Zu den Faktoren, die darauf Einfluß haben, gehören die angestrebte Evaluationsstufe, die Größe und Komplexität des Systems und die Frage, ob der Entwickler und/oder der Antragsteller bereits über Erfahrungen mit der Entwicklung evaluierter Systeme und Produkte verfügen. Einige Aspekte des Evaluationsprozesses, wie etwa die Durchführung von Tests anhand des EVG, erfordern eine intensivere Hilfestellung.

6.A.29 Was die Art der Hilfestellung betrifft, könnte folgendes in Betracht kommen:

a) Schulungsmaßnahmen;

b) informelle Besprechungen;

c) Rechnerzugang und -unterstützung;

d) Büroräume.

6.A.30 Eine informelle Schulung, vorzugsweise durch jemand aus dem Entwicklerteam, kann in einer Reihe von Anwenderbereichen erforderlich werden, in denen keine umfassende Dokumentation zur Verfügung steht, wie etwa

a) der Hardware und dem/den Betriebssystem(en), die für den EVG und seine Entwicklung verwendet werden;

b) den verwendeten Entwicklungsmethoden;

c) den verwendeten Entwicklungswerkzeugen.

6.A.31 Normalerweise wird vom Entwickler nicht erwartet, daß er formale Schulungskurse speziell für die Evaluatoren durchführt. Die Evaluatoren können jedoch auf Wunsch an Schulungen teilnehmen, die für andere Mitarbeiter angeboten werden, etwa wenn

a) Entwicklerpersonal z.B. in einer bestimmten Entwicklungsmethode ausgebildet wird;

b) Anwenderkurse z.B. zum Thema Sicherheitsverwaltung des EVG angeboten werden.

6.A.32 Informelle Gespräche mit dem Entwickler können für jeden Aspekt des EVG erforderlich werden. Im Normalfall können die Evaluatoren den Entwickler bitten, ihnen eine Kurzbeschreibung eines bestimmten Teils des EVG zur Verfügung zu stellen und anschließend ihre Fragen zu beantworten.

6.A.33 Die Evaluatoren müssen Zugang zu einem geeigneten Rechner bzw. Rechnern haben, in erster Linie zur Durchführung von Tests mit dem EVG. Der Begriff "Rechner" in diesem Kontext schließt alle Einrichtungen ein, die vom Entwickler für die Montage und zum Testen des EVG verwendet werden.

6.A.34 Handelt es sich bei dem EVG um ein System, müssen die Evaluatoren auch, soweit möglich, Zugang zu dem/den für den Betrieb des EVG verwendeten Rechner(n) haben (siehe Absätze 6.A.23 bis 6.A.25).

6.A.35 Die Evaluatoren müssen während eines Teils der Zeit, in der sie zusätzliche Tests (zu denen des Entwicklers) oder Penetrationstests durchführen, speziellen Rechnerzugang haben.

6.A.36 Die Dauer des Rechnerzugangs hängt von der Beschaffenheit des einzelnen EVG ab.

6.A.37 Der Rechnerzugang betrifft normalerweise den Entwicklungs- oder Betriebsort. In einigen Fällen kann es jedoch zweckmäßig sein, an einem anderen Ort Zugangsmöglichkeiten zu schaffen, beispielsweise durch Auslieferung eines Rechners an eine ITSEF.

6.A.38 Wenn die Evaluatoren einen Rechner benutzen, kann es sein, daß sie Hilfestellung bei Grundoperationen benötigen, wie etwa beim Hochfahren des Rechners, beim Erstellen von Sicherungskopien des EVG, Lauftests usw. .

6.A.39 Büroräume zur ausschließlichen Verfügung der Evaluatoren sollen dem Bedarf entsprechend zur Verfügung gestellt werden, wenn die Evaluatoren am Entwicklungs- oder Betriebsort arbeiten. Diese Räume sollen genügend Platz für die benötigte Anzahl von Personen bieten und folgendes enthalten:

a) Grundausstattung an Büromöbeln einschließlich Telefon;

b) sichere Aufbewahrungsmöglichkeiten für Informationen einer für den EVG angemessenen Geheimhaltungsstufe.

6.A.40 Bekanntlich kann aufgrund der geltenden Vorschriften der allgemeine Zutritt zum Entwicklungs- oder Betriebsort ohne Begleitung untersagt sein. Die Evaluatoren müssen jedoch während ihrer Arbeit an einem Standort gelegentlich auch für sich allein sein können; deshalb müssen Regelungen getroffen werden, daß die Evaluatoren während des Aufenthalts in diesem Büro unbeaufsichtigt bleiben dürfen.

Abbildung 6.A.1 Evaluationsbeiträge (Wirksamkeit)	
EVALUATIONSBEITRAG	**ALLE EVALUATIONSSTUFEN**
Analyse der Eignung: **eine Prüfung, aus der hervorgeht, daß die sicherheitsspezifischen Funktionen und Mechanismen des EVG den in den Sicherheitsvorgaben aufgezeigten Bedrohungen für die Sicherheit des EVG auch tatsächlich entgegenwirken**	✓
Analyse des Zusammenwirkens: **eine Prüfung, aus der hervorgeht, daß die sicherheitsspezifischen Funktionen und Mechanismen des EVG in einer sich wechselseitig unterstützenden und ein integriertes und wirksames Ganzes bildenden Weise zusammenwirken**	✓
Analyse der Stärke der Mechanismen: **eine Prüfung, aus der die Fähigkeit des EVG als Ganzes hervorgeht, direkten Angriffen aufgrund von Mängeln in den ihm zugrundeliegenden Algorithmen, Prinzipien oder Eigenschaften standzuhalten; bei dieser Bewertung muß der Aufwand an Ressourcen berücksichtigt werden, den ein Angreifer benötigt, um einen erfolgreichen Angriff durchzuführen**	✓
Liste der bekannten Konstruktionsschwachstellen: **eine Liste der potentiellen Konstruktionsschwachstellen des EVG (vom Entwickler identifiziert) plus eine Begründung, weshalb sie nicht ausnutzbar sind**	✓
Analyse der Benutzerfreundlichkeit: **eine Prüfung, aus der hervorgeht, daß der EVG nicht in einer Art und Weise konfiguriert oder eingesetzt werden kann, die unsicher ist, die der Systemverwalter oder der Endanwender des EVG aber begründeterweise für sicher halten**	✓
Liste der bekannten Schwachstellen in der operationellen Nutzung: **eine Liste der potentiellen Schwachstellen beim Betrieb des EVG (vom Entwickler identifiziert) plus eine Begründung, weshalb sie nicht ausnutzbar sind**	✓

Abbildung 6.A.2 Evaluationsbeiträge (Korrektheit)

Evaluationsbeitrag	Evaluationsstufe					
	E1	E2	E3	E4	E5	E6
Anforderungen						
Die Sicherheitsvorgaben für den EVG	✓	✓	✓	✓	✓	✓
Definition eines zugrundeliegenden formal spezifizierten Sicherheitsmodells oder Verweis darauf				✓	✓	✓
Informelle Interpretation des zugrundeliegenden Modells hinsichtlich der Sicherheitsvorgaben				✓	✓	✓
Architektur						
Informelle Beschreibung der Architektur des EVG	✓	✓	✓			
Semiformale Beschreibung der Architektur des EVG				✓	✓	
Formale Beschreibung der Architektur des EVG						✓
Feinentwurf						
Informelle Beschreibung des Feinentwurfs		✓	✓			
Semiformale Beschreibung des Feinentwurfs				✓	✓	✓
Implementierung						
Testdokumentation	(✓)	✓	✓	✓	✓	✓
Bibliothek der zum Prüfen des EVG verwendeten Testprogramme und Werkzeuge	(✓)	✓	✓	✓	✓	
Bibliothek der zum Prüfen des EVG verwendeten Testprogramme und Werkzeuge, einschließlich Werkzeuge, die zur Auffindung von Inkonsistenzen zwischen Quellcode und ausführbarem Code verwendet werden können, wenn sicherheitsspezifische oder sicherheitsrelevante Quellcodekomponenten vorhanden sind (z.B. ein Disassembler und/oder ein Debugger)						✓
Quellcode oder Hardware-Konstruktionszeichnungen für alle sicherheitsspezifischen und sicherheitsrelevanten Komponenten			✓	✓	✓	✓
Informelle Beschreibung der Übereinstimmung zwischen Quellcode oder Hardware-Konstruktionszeichnungen und dem Feinentwurf			✓	✓	✓	
Informelle Beschreibung der Übereinstimmung zwischen Quellcode oder Hardware-Konstruktionszeichnungen und dem Feinentwurf und der formalen Spezifikation sicherheitsspezifischer Funktionen						✓

Anmerkung: (✓) - optionale Evaluationsbeiträge

Abbildung 6.A.2 Evaluationsbeiträge (Korrektheit)

Evaluationsbeitrag	Evaluationsstufe					
	E1	E2	E3	E4	E5	E6
Konfigurationskontrolle						
Konfigurationsliste mit Angabe der für die Evaluation bestimmten Version des EVG	✓	✓	✓	✓	✓	✓
Informationen über das Konfigurationskontrollsystem		✓	✓			
Informationen über das Konfigurationskontrollsystem und seine Werkzeuge				✓	✓	✓
Protokollinformationen über die Modifikation aller der Konfigurationskontrolle unterliegenden Teile des EVG				✓		
Protokollinformationen über die Modifikation aller der Konfigurationskontrolle unterliegenden Objekte des EVG					✓	✓
Informationen über das Abnahmeverfahren			✓	✓	✓	✓
Informationen über das Integrationsverfahren					✓	✓
Programmiersprachen und Compiler						
Beschreibung aller verwendeten Implementierungssprachen			✓	✓	✓	✓
Beschreibung aller verwendeten Compiler				✓	✓	✓
Quellcode für alle verwendeten Laufzeitbibliotheken					✓	✓
Sicherheit beim Entwickler						
Informationen über die Sicherheit der Entwicklungsumgebung		✓	✓	✓	✓	✓
Betrieb						
Benutzerdokumentation	✓	✓	✓	✓	✓	✓
Systemverwalterdokumentation	✓	✓	✓	✓	✓	✓
Auslieferungs- und Konfigurationsdokumentation	✓	✓	✓	✓	✓	✓
Anlauf- und Betriebsdokumentation	✓	✓	✓	✓	✓	✓

Abbildung 6.A.3 Diskussionspunkte der Entwicklungsumgebung

ENTWICKLUNGSKONFIGURATIONSKONTROLLE

Anwendungsbereich:	Die Prozeduren (manuell und automatisiert) zur Kontrolle und Abbildbarkeit von Projektmaterial
Themen:	Rechnerorganisation - Verzeichnisstruktur - Software-Bibliothek und Zugriffskontrolle Änderungskontrolle Freigabeprozeduren

PROGRAMMIERSPRACHEN UND COMPILER

Anwendungsbereich:	Die zur Implementierung verwendeten Programmiersprachen
Themen:	Definition der Sprachen Implementierungsabhängige Optionen Compiler

ENTWICKLUNGSSICHERHEIT

Anwendungsbereich:	Sicherheit der Entwicklungsumgebung, d.h. Schutz des EVG und der Vertraulichkeit der zugehörigen Dokumente
Themen:	Materielle Maßnahmen Organisatorische Maßnahmen Personelle Maßnahmen

ENTWICKLUNGSMETHODEN

Anwendungsbereich:	Die verschiedenen Entwicklungphasen und der verwendete Ansatz
Themen:	Projekthintergrund und aktueller Sachstand Erstellte Darstellungen Entwurfsprozeß Codierphase Testpolitik

ENTWICKLUNGSWERKZEUGE

Anwendungsbereich:	Die während der Entwicklung verwendeten Werkzeuge (anwendereigene und speziell angefertigte)
Themen:	Entwicklungsrechner, Systemmanagement Compiler/Binder/Debugger Systemgenerierungsprozeduren Testroutinen

ENTWICKLUNGSPROZEDUREN

Anwendungsbereich:	Die während der Entwicklung verwendeten Kontrollen
Themen:	Projektmanagementprozeduren Qualitätssicherungsprozeduren Technische Sicherungsprozeduren

ENTWICKLUNGSNORMEN

Anwendungsbereich:	Die während der Entwicklung angewandten Normen
Themen:	Entwurfsnormen Codiernormen Dokumentationsnormen

Anhang 6.B Schreiben von Sicherheitsvorgaben

Einleitung

6.B.1 Der vorliegende Anhang enthält für den Antragsteller einer Evaluation bestimmte Hinweise für das Schreiben von Sicherheitsvorgaben. Anhand bildlicher Darstellungen wird beschrieben, wie die Sicherheitsvorgaben des SWAN-Systems (das in Teil 5 des ITSEM erläutert wird) umformuliert werden können.

Der Zweck von Sicherheitsvorgaben

6.B.2 Das Ziel, das vom Antragsteller bei der Festlegung von Sicherheitsvorgaben verfolgt wird, besteht darin, eine vollständige und konsistente Grundlage für die Evaluation zu schaffen. Die Sicherheitsvorgaben sind ein umfangreiches Dokument (oder eine Reihe von Dokumenten), das unter anderem folgendes enthält:

a) die Sicherheitsziele des Produkts oder Systems (EVG);

b) die vom EVG zur Abwehr der wahrgenommenen Bedrohungen eingesetzten Gegenmaßnahmen.

6.B.3 Demzufolge stellen Sicherheitsvorgaben die auf einem hohen Abstraktionsniveau beschriebenen Sicherheitsanforderungen an den EVG dar.

6.B.4 Darüber hinaus sind die Sicherheitsvorgaben Bestandteil der Vertragsgrundlage zwischen Antragsteller und ITSEF und enthalten Angaben wie etwa die Evaluationsstufe, die während der gesamten Evaluation relevant sind.

6.B.5 Aus der Sicht des Entwicklers sind die Sicherheitsvorgaben integraler Bestandteil der EVG-Spezifikation auf einem hohen Abstraktionsniveau. Dementsprechend müssen die Sicherheitsvorgaben für den Entwickler eine eindeutige Angabe der Fähigkeiten und möglichen Verwendungszwecke des EVG enthalten.

6.B.6 Die Sicherheitsvorgaben können organisatorische, funktionale und technische Aspekte enthalten. Sie können sich auch mit anderen durch die Anforderungen bedingten Aspekten wie etwa Unterstützungsleistungen befassen.

6.B.7 Die Sicherheitsvorgaben stellen eine Spezifikation für die sicherheitsspezifischen Teile der Implementierung dar. Sie sollen zu einem möglichst frühen Zeitpunkt des Entwicklungszykluses geschrieben werden, damit eine begleitende Evaluation frühzeitig während der Entwicklung begonnen werden kann. Dies ist jedoch nur dann möglich, wenn die Sicherheitsvorgaben ausreichend stabil sind.

6.B.8 Die Sicherheitsanforderungen müssen in den Sicherheitsvorgaben zwar getrennt spezifiziert werden, jedoch erfolgt die Verfeinerung der Sicherheits- und der Nicht-Sicherheitsanforderungen zur gleichen Zeit.

6.B.9 Bei einer nachfolgenden Evaluation ergibt sich, wenn der EVG vor Festlegung der Sicherheitsvorgaben entwickelt worden ist, die Notwendigkeit der "Rückwärtsentwicklung" aller benötigten Informationen.

6.B.10 Der Antragsteller ist zwar für die Bereitstellung der Sicherheitsvorgaben zuständig, er ist aber unter Umständen kein Fachmann für alle Sicherheitsaspekte. Daher empfiehlt sich, daß der Antragsteller beim Schreiben von Sicherheitsvorgaben Hilfestellung gewährt bekommt. Eine solche Hilfestellung kann von Entwicklern geleistet werden, die über die entsprechende Qualifikation für die Erstellung

der von ihnen zu implementierenden Spezifikation verfügen. Allerdings könnte auch eine ITSEF zu Rate gezogen werden, wenn es um Inhalt und Form der Sicherheitsvorgaben geht.

6.B.11 Für Käufer eines Systems (d.h. die Anwender, auf deren Anforderungen das System zugeschnitten sein soll) sollen die Sicherheitsvorgaben als Grundlage für ihre Kaufentscheidung dienen.

6.B.12 Es ist Aufgabe der Evaluatoren herauszufinden, ob der EVG mit den Sicherheitsvorgaben übereinstimmt. Darüber hinaus müssen die Evaluatoren abschätzen, ob die EVG-Spezifikation im Kontext der anderen Evaluationsbeiträge gültig ist.

Der Inhalt von Sicherheitsvorgaben

6.B.13 Damit Sicherheitsvorgaben ihrer Rolle im Rahmen einer Evaluation gerecht werden, müssen sie

a) genaue Angaben über die Sicherheitsanforderungen des EVG enthalten;

b) die vorgesehenen Gegenmaßnahmen angeben, mit denen die wahrgenommenen Bedrohungen der von dem EVG geschützten Werte abgewehrt werden können.

6.B.14 Zu diesem Zweck schreiben die ITSEC vor, daß

a) Sicherheitsanforderungen in einer Sicherheitspolitik (für Systeme) oder einer Produktbeschreibung (für Produkte) erfaßt werden;

b) zur Erfüllung der Sicherheitsanforderungen Funktionen festgelegt werden; diese werden als sicherheitsspezifische Funktionen bezeichnet;

c) für den Fall, daß zur Erfüllung einer Sicherheitsanforderung ein bestimmtes technisches Verfahren vorgeschrieben ist, z.B. die Verwendung eines speziellen Algorithmus für die Paßwortverschlüsselung, dieses als erforderlicher Sicherheitsmechanismus aufgeführt wird;

d) eine postulierte Mindeststärke der Mechanismen vorgegeben wird, die *niedrig*, *mittel* oder *hoch* ist;

e) für den EVG eine angestrebte Evaluationsstufe spezifiziert ist.

6.B.15 Es ist zu bedenken, daß je nach gewählter Evaluationsstufe die Spezifikation der sicherheitsspezifischen Funktionen unter Umständen in semiformaler oder formaler Form erfolgen muß.

Risikoanalyse

6.B.16 Bei der Spezifikation sicherheitsspezifischer Funktionen muß ein Kompromiß zwischen dem Bedürfnis, Werte zu schützen, und dem erforderlichen Aufwand für einen solchen Schutz (z.B. finanzieller, personeller, betrieblicher und technischer Art) geschlossen werden. Dieser Kompromiß wird durch einen Risikoanalyseprozeß gesteuert.

6.B.17 Darüber hinaus werden bei der Konstruktion eines EVG sowohl die Anforderungen an den EVG als auch etwaige relevante Einschränkungen bezüglich des EVG (z.B. Gesetze, Anweisungen, Technologie, Werte, Kosten usw.) berücksichtigt.

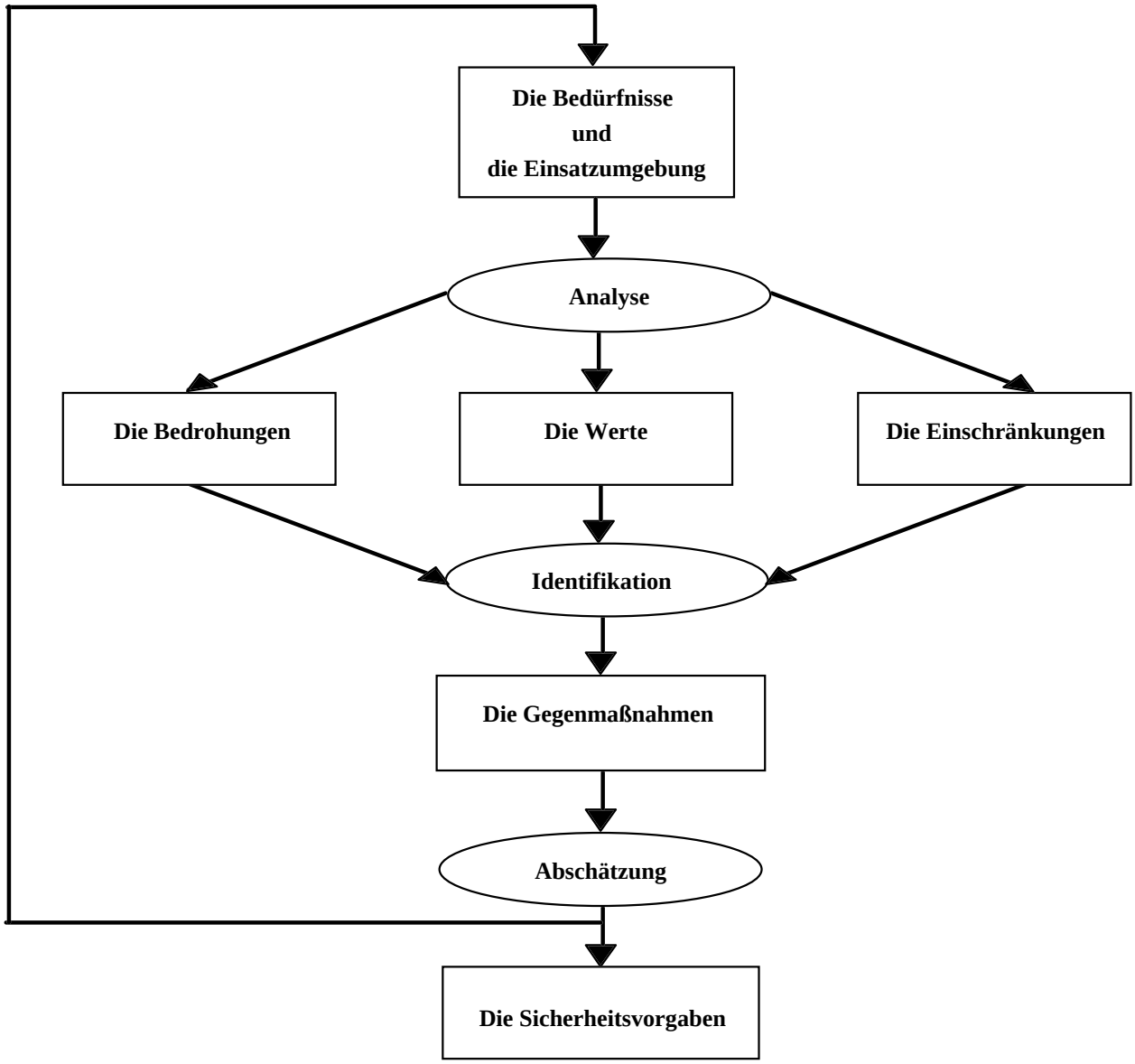


Abbildung 6.B.1 Das Verfahren der Risikoanalyse

6.B.18 Durch die Risikoanalyse werden die Bedrohungen ermittelt, denen die von dem EVG geschützten Werte ausgesetzt sind. Für jede Bedrohung wird die Wahrscheinlichkeit der Gefährdung eines Wertes abgeschätzt.

6.B.19 Die Risikoanalyse soll bei der Entwicklung des EVG als eine der ersten Aktivitäten durchgeführt werden.

6.B.20 Da die Entwicklung jedoch selten ein linearer Prozeß ist, kommt es wahrscheinlich zu einer regelmäßigen Überarbeitung und Änderung der Sicherheitsvorgaben. Solche Änderungen sind ein Problem für Evaluatoren und machen die Evaluationsergebnisse häufig ungültig.

6.B.21 Der Risikoanalyseprozeß steuert die Erstellung der Sicherheitsvorgaben, indem er sich zunächst mit den Werten, Bedrohungen und Gegenmaßnahmen befaßt, woraus sich letzten Endes die Sicherheitsvorgaben ergeben.

6.B.22 Eine Risikoanalyse besteht aus einer ganzen Reihe von Aktivitäten, die den Spezifikationen und Anforderungen entsprechend durchgeführt werden (siehe Abbildung 6.B.1). Zu diesen gehören folgende:

a) die Problemanalyse (sie befaßt sich mit der Betriebsumgebung und den Bedürfnissen);

b) die Identifikation von Optionen (sie befaßt sich mit Werten, Bedrohungen und Einschränkungen);

c) die Lösungsabschätzung (sie befaßt sich mit der Angemessenheit, der Durchführbarkeit und den Kosten von Gegenmaßnahmen);

d) die Entscheidungsintegration (sie befaßt sich mit Wahlmöglichkeiten und der Berichterstattung).

6.B.23 Varianten dieses Prozesses werden in den Standardmethodologien ([CRAMM], MARION, MELISA, [GISA2]) beschrieben. Sie sind eine nützliche Hilfe bei der Erstellung von Verzeichnissen der Ressourcen, Bedrohungen und der verschiedenen Klassen von Gegenmaßnahmen.

6.B.24 Mangels einer entsprechenden Methodik kann es zweckdienlich sein, generische Spezifikationen zu verwenden. Die vordefinierten Funktionalitätsklassen in den ITSEC und die Sicherheitsmodelle für offene Systeme nach ISO sind Beispiele dafür.

System-Sicherheitspolitik oder Produktbeschreibung

Allgemeines

6.B.25 Die Sicherheitsvorgaben beginnen mit einer Beschreibung der Bedrohungen, der Ziele und der Betriebsumgebung des EVG. Bei einem System geschieht dies im Rahmen einer System-Sicherheitspolitik, bei einem Produkt im Rahmen einer Produktbeschreibung.

6.B.26 Die Sicherheitspolitik oder Produktbeschreibung gibt an, wer was mit den Einrichtungen, Diensten, Funktionen und Geräten des EVG tun darf.

6.B.27 Die Erstellung einer Sicherheitspolitik oder einer Produktbeschreibung für die Verwendung im Rahmen von Sicherheitsvorgaben kann schwierig sein. Eine Sicherheitspolitik oder Produktbeschreibung soll ohne Berücksichtigung des Entwurfs des EVG die zu schützenden Werte und die für den Umgang mit den Werten geltenden Regeln zum Ausdruck bringen.

Vorgesehene Betriebsumgebung

6.B.28 Eine Studie über den EVG und der Umgebung, in der er eingesetzt wird, einschließlich einer Risiko-analyse der Sicherheitsaspekte des EVG, definiert die Betriebseigenschaften des EVG. Diese Eigen-schaften bestimmen darüber, wie sich der EVG in seine Betriebsumgebung einpaßt, und sollen daher in den Sicherheitsvorgaben beschrieben werden.

6.B.29 In diesem Abschnitt der Sicherheitsvorgaben soll folgendes festgelegt werden:

a) der Zweck und die Abgrenzung des EVG;

b) die vom EVG zu verarbeitenden Informationen und wie sie zu verarbeiten sind;

c) das Personal, das den EVG verwendet (z.B. Anwender, Bediener, Systemverwalter usw.);

d) die erforderliche technische Ausstattung zur Unterstützung des Betriebs des EVG;

e) der Aufstellort und die Topologie des EVG, einschließlich materieller Sicherheitsmaßnahmen;

f) die Betriebsarten und -prozeduren;

g) die Organisation und deren Verfahren.

Das SWAN-System: Vorgesehene Betriebsumgebung

6.B.30 Das Site-Wide Area Network (SWAN) ist ein Kommunikationsnetz, das mehreren Anwendergruppen den Zugriff auf verschiedene DV-Anwendungen ermöglicht.

6.B.31 Das Beispielsystem befindet sich auf einem großen Gelände, das einer Unternehmensorganisation gehört. Das Betriebsgelände ist vollständig von einem Schutzzaun umgeben, der gut bewacht ist. Alle Mitarbeiter sind von Unternehmensseite einer Sicherheitsprüfung unterzogen worden und gelten als vertrauenswürdig. Besucher dürfen das Betriebsgelände nur in Begleitung betreten.

6.B.32 Innerhalb des Betriebsgeländes gibt es verschiedene Bereiche, die zusätzlichen Schutz in Form einer Zugangskontrolle und anderer organisatorischer Sicherheitsmechanismen bieten. Es liegt eine geringe TEMPEST-Belastung und kryptographische Bedrohung vor. Die Terminals befinden sich in gesicherten Räumen, und Mitarbeiter werden durch die autorisierten Anwender daran gehindert, ein unbeaufsichtigtes Terminal in einem von ihnen betretenen Raum zu benutzen.

6.B.33 Auf dem Betriebsgelände befindet sich eine Vielzahl unterschiedlicher IT-Systeme, die zu unterschiedlichen Zeiten von unterschiedlichen Herstellern bezogen wurden und für eine Vielzahl von Zwecken, wie etwa für die Transaktionsverarbeitung, die Abrechnung und die Unternehmensverwaltung, eingesetzt werden.

6.B.34 Die Anwenderterminals und die Host-Rechner, die in verschiedenen Gebäuden untergebracht sein können, waren früher über festgeschaltete Lichtwellenleiterkabel verbunden. Inzwischen sind sie durch das SWAN-Netz ersetzt worden. Das SWAN ist ein TCP/IP Token Ring-Netz, das aus einem 'dual counter rotating backbone'-Netz und verschiedenen Teilnetzen besteht. Die Endsystemeinrichtungen sind an das SWAN über Zugangspunkte am Host-Rechner oder an den Terminals angeschlossen.

6.B.35 Host-Rechner werden entweder im 'dedicated mode' oder im 'system-high mode' betrieben, z.B. firmenvertraulich, managementvertraulich oder firmenleitungsvertraulich.

6.B.36 Für jeden Anwender sind Zugriffsrechte festgelegt. Alle auf dem Gelände befindlichen Mitarbeiter sind entweder autorisiert, zumindest auf firmenvertrauliche Informationen zuzugreifen, oder sie werden von autorisierten Mitarbeitern begleitet.

6.B.37 Die Betriebsprozeduren sind von einer früheren Konfiguration abgeleitet, bei der jeder Server der Hub eines speziellen Netzes war. Infolgedessen wird der Zugriff auf von jedem Host-Rechner unterstützte Anwendungen lokal auf anwenderbestimmbarer Basis durch einen Anwendungsmanager verwaltet.

6.B.38 Während jedes Terminal und jeder Host-Rechner auf verschiedenen Sicherheitsstufen arbeiten kann, hat der Systemverantwortliche bei der neuen SWAN-Version ein regelbasiertes Zugriffskontroll-verfahren für die Anbindung von Terminals an Server festgelegt.

Sicherheitsziele

6.B.39 Der erste Schritt bei der Konzipierung einer Sicherheitspolitik besteht darin, die Sicherheitsziele festzulegen. Die Sicherheitsziele kommen in folgendem zum Ausdruck:

a) in den Werten der Organisation, die geschützt werden müssen, sei es durch den EVG, irgendein anderes System oder eventuell mit manuellen/physischen Mitteln; zu den Werten gehören die Informationen, die der EVG zu verarbeiten hat, die vom EVG zu automatisierenden Prozesse und die Verantwortlichkeiten und/oder Rollen der Anwender.

b) in den Ressourcen des EVG nach der Definition in der externen Spezifikation; die Ressourcen können die materiellen Ressourcen wie etwa Anlagen oder Geräte oder abstrakte Ressourcen wie etwa die EVG-Konfiguration, Prozesse, Algorithmen oder ein Code sein.

6.B.40 Die Risikoanalyse befaßt sich mit der von den Sicherheitszielen vorgegebenen Sicherheitsstufe (zum Beispiel im Falle der Datenvertraulichkeit, welche Geheimhaltungsstufe geschützt werden kann). Die Evaluation geht darauf nicht ein, sondern konzentriert sich auf die Vertrauenswürdigkeit, die durch Implementierung der sicherheitsspezifischen Funktionen erworben werden kann. Daher soll in den Sicherheitsvorgaben auf diesen Schutzgrad nicht Bezug genommen werden.

6.B.41 Bei der Betrachtung von Sicherheitszielen sind zwei Vorgehensweisen möglich:

a) alle Daten und Ressourcen werden nacheinander analysiert, wobei sämtliche relevanten Sicherheitsziele berücksichtigt werden;

b) zu dem gleichen Sicherheitsziel gehörende Ressourcen und Daten werden für Analysezwecke gruppenweise zusammengestellt.

6.B.42 Verfügbarkeitsziele werden im Hinblick auf Status, Capabilities (Fähigkeiten), Betriebsdauer, Antwortzeiten, Prioritäten und Degradierungstoleranz beschrieben.

6.B.43 Integritätsziele werden wie folgt beschrieben:

a) als Übereinstimmung mit Normen, Spezifikationen und Verweisungen;

b) als Übereinstimmung mit einem Ausgangszustand oder einer Ausgangsbedingung;

c) als aus Gründen der Konsistenz und Kohärenz zu beachtende Regeln.

6.B.44 Vertraulichkeitsziele erklären die zu erwartende Verwendung jeder Ressource, anstatt sich mit den zu behebenden Schwachstellen zu befassen (z.B. Offenlegung, Veränderung des Zusammenhangs, Zielmanipulation).

6.B.45 Der Verfasser der Sicherheitsvorgaben soll sich um größtmögliche Vollständigkeit dieses Abschnitts bemühen, da die Sicherheitsziele letztendlich die Grundlage für die Evaluation bilden. Jedes Merkmal des EVG, das nicht zu einem Sicherheitsziel zurückverfolgt werden kann, kann auch nicht als sicherheitsspezifisch betrachtet werden.

Das SWAN-System: Sicherheitsziele

6.B.46 Die zu schützenden Werte der Organisation sind Anwendungsdienste, die jeder Anwendergruppe zur Verfügung stehen. Es gibt kein Sicherheitsziel für die Systemressourcen.

6.B.47 Zu diesen Diensten (Informationen und Verarbeitung) sollen Personen außerhalb der Anwendergruppe keinen Zugang haben.

6.B.48 Es gibt kein Verfügbarkeitsziel.

6.B.49 Es gibt kein Integritätsziel, was bedeutet, daß ein Angriff auf die Integrität der für jede Anwendergruppe erworbenen Dienste nicht erwartet wird oder daß ein solcher Angriff tolerierbar ist, solange die Vertraulichkeit der Dienste nicht gefährdet ist.

6.B.50 Eine nicht ordnungsgemäße Nutzung von Anwendungsdiensten durch autorisierte Anwender ist ohne Belang.

Die Bedrohungen

6.B.51 Der nächste Schritt bei der Festlegung einer Sicherheitspolitik besteht darin, die wahrgenommenen Bedrohungen der Werte zu bestimmen, d.h. Aktionen, die zu einer Verletzung der Sicherheitsziele führen können.

6.B.52 Wie die Sicherheitsziele sind Bedrohungen ein während der Spezifikation des EVG zu berücksichtigender Aspekt. Wie vorstehend angedeutet, beziehen sie sich auf die externe Beschreibung des EVG. Allerdings ist eine Bewertung der Bedrohungen schwieriger als die Bestimmung der Sicherheitsziele, da es unmöglich ist, auf alle potentiellen Angriffsarten einzugehen.

6.B.53 Die Methoden der Risikoanalyse können bei der Bewertung einer Bedrohung durchaus nützlich sein, nicht so sehr wegen des dafür verwendeten systematischen Prozesses, sondern wegen des dabei erworbenen Wissens. Mit den vorhandenen Techniken kann eine Liste generischer Bedrohungen erstellt werden, die sogleich auf den betreffenden EVG angewandt werden kann. Daraus können sich brauchbare Hinweise für eine Bedrohungsabschätzung ergeben, die den Anforderungen des Analytikers entsprechend ereignis- oder zielorientiert sein kann.

6.B.54 Verfasser von Sicherheitsvorgaben sollen bedenken, daß sie für die Unverfälschtheit und Vollständigkeit der Sicherheitsziele und der Bedrohungen verantwortlich sind. Evaluatoren können die Vollständigkeit dieser Informationen nicht nachprüfen, sie überprüfen aber die Unverfälschtheit und die Konsistenz.

Das SWAN-System: Die Bedrohungen

6.B.55 Während der Risikoanalyse sind der Reihe nach verschiedene Arten von Bedrohungen betrachtet worden:

a) physische Angriffe auf das System und seine Betriebsumgebung;

b) Auffangen von Strahlung;

c) direkte Angriffe auf Anwendungen.

6.B.56 Physische Angriffe kommen zwar für Host-Rechner oder Terminals, die permanent bewacht oder überwacht werden, nicht in Frage, sie kommen jedoch für Netzkabel in Frage, über die unzulässige Verbindungen hergestellt werden können.

6.B.57 Dank der TEMPEST-Abschirmung der Gebäude und der Verwendung von Lichtwellenleiterkabeln stellte die Abstrahlung keine Bedrohung dar.

6.B.58 Daher kann ein Angriff nur lokal über das Netz erfolgen:

a) Ein Anwender kann versuchen, sich Zugang zu einem Dienst zu verschaffen, zu dessen Nutzung er nicht berechtigt ist;

b) ein Anwender kann sich als ein anderer Anwender ausgeben.

6.B.59 Autorisierte Anwender gelten als vertrauenswürdig, so daß keine Gefahr eines Mißbrauchs des Systems oder einer geheimen Absprache mit einem Angreifer besteht.

System-Sicherheitspolitik

6.B.60 Für eine Systemevaluation ist die tatsächliche Betriebsumgebung bekannt, und die Bedrohungen für das System können abgeschätzt werden. Vorhandene Gegenmaßnahmen (die aus einer Kombination von elektronischen, materiellen, organisatorischen und personellen Gegenmaßnahmen bestehen können) können mit berücksichtigt werden, und die Sicherheitsziele des Systems können vom Antragsteller abgeleitet werden. Diese Informationen werden von einer System-Sicherheitspolitik zur Verfügung gestellt.

6.B.61 Im Normalfall verfügt eine Organisation über mehr als eine Sicherheitspolitik. Für gewöhnlich wird auf jeder Ebene der Organisation eine eigene Sicherheitspolitik entsprechend den der Ebene zugeordneten Werten verfolgt. Zum Beispiel gibt es normalerweise für das IT-System einer Organisation eine Sicherheitspolitik, in der geeignete Regeln zum Schutz der von dem System und den Systemkomponenten bearbeiteten Informationen festgelegt sind (z.B. Daten, Geräte, Prozesse usw.).

6.B.62 Die Sicherheitspolitik soll den Detaillierungsgrad auf jeder Organisationsebene verfeinern. So braucht beispielsweise der Schutz sensitiver Informationen in der ursprünglichen organisationsinternen Sicherheitspolitik nicht spezifiziert zu werden, er sollte jedoch Schritt für Schritt und iterativ in der Sicherheitspolitik der unteren Ebenen und bei der Festlegung ihrer sicherheitsspezifischen Funktionen berücksichtigt werden (siehe Abbildung 6.B.2).

6.B.63 Die System-Sicherheitspolitik legt die Gesetze, Regeln und Vorgehensweisen fest, die bestimmen, wie sensitive Informationen und andere Ressourcen innerhalb des Systems verwaltet werden. Im Gegensatz zur technischen Sicherheitspolitik umfaßt sie auch materielle, personelle und organisatorische Maßnahmen.

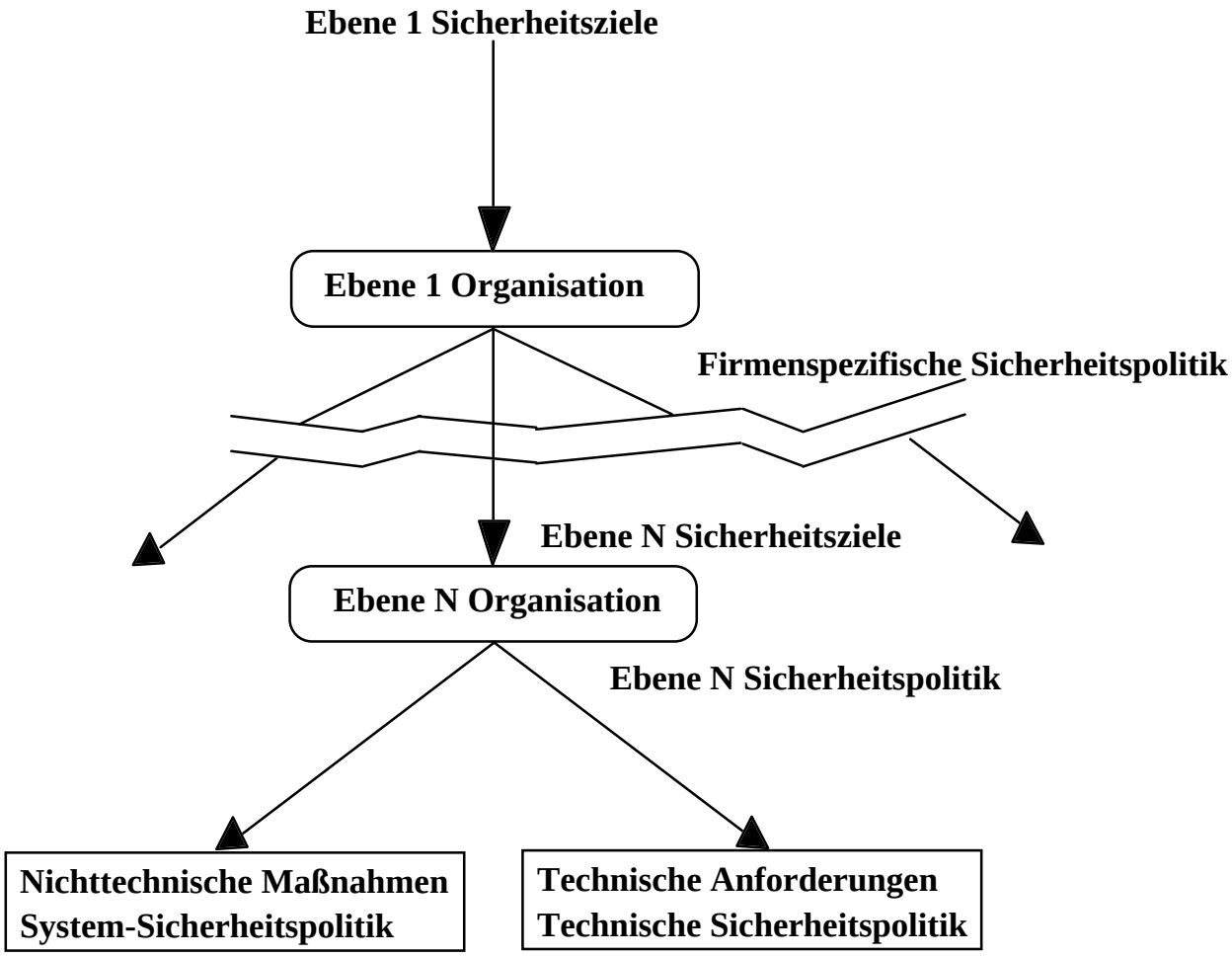


Abbildung 6.B.2 Ableitung einer Sicherheitspolitik

6.B.64 In der technischen Sicherheitspolitik sind Regeln für die Verarbeitung sensitiver Informationen und den Einsatz von Ressourcen innerhalb des Systems selbst festgelegt.

6.B.65 Die eigentliche Sicherheitspolitik stellt eine Verbindung zwischen den in den Schritten 'Bedrohungen' und 'Ziele' festgelegten Sicherheitsanforderungen und den später in den Sicherheitsvorgaben definierten sicherheitsspezifischen Funktionen her. Aus der Sicht der Organisation reichen die bereits in der Sicherheitspolitik enthaltenen Informationen aus, um eine Implementierungsspezifikation zu erstellen. Allerdings bedürfen die Informationen einer weiteren Verfeinerung, bevor sie als Spezifika-tion der Anforderungen für einen EVG dienen können. Diese Verfeinerung ist das Ziel des letzten Schrittes bei der Festlegung einer Sicherheitspolitik.

6.B.66 Anhand der Sicherheitsziele und der wahrgenommenen Bedrohungen können Regeln zur Kontrolle der verschiedenen Anwender des EVG aufgestellt werden.

6.B.67 In den Regeln wird festgelegt,

a) welche Operationen für den einzelnen Wert obligatorisch, erlaubt oder verboten sind;

b) welche Rollen diese Operationen übernehmen können oder müssen oder nicht übernehmen dürfen.

6.B.68 Die Regeln sind die Reaktion der Organisation auf den Sicherheitsbedarf und resultieren aus

a) den allgemeinen Vorgehensweisen im Sicherheitsbereich;

b) den innerhalb der Organisation vertretenen Lehrmeinungen;

c) gezielt auf die Bewältigung des betreffenden Problems ausgerichteten Plänen.

6.B.69 Außerdem müssen folgende allgemeine Sicherheitsgrundsätze eingehalten werden:

a) Trennung von Rollen/Anwendern, deren Ziel die Begrenzung der Möglichkeit eines Angriffs aufgrund der Weitergabe von Privilegien von einem Anwender an einen anderen ist; dies bezieht sich insbesondere auf die Entfernung von Rollen/Anwendern aus einem System;

b) Benutzerfreundlichkeit, deren Ziel die Vermeidung von Fehlern beim Betrieb des EVG ist, die zu Schwachstellen führen können;

c) Schutz durch Voreinstellung, deren Ziel die Vermeidung aktiver Maßnahmen zur Aufrechterhaltung der Sicherheit ist;

d) Eliminierung von Ausnahmen, deren Ziel die bessere Verständlichkeit und Befolgung des Sicherheitsmodells ist;

e) Minimalprivileg, dessen Ziel die Minimierung des Risikos eines Mißbrauchs durch Zuweisung einer Berechtigungsstufe (für einen Anwender, eine Rolle, einen Prozeß usw.) ist, die zur Durchführung der zugewiesenen Aufgaben gerade ausreicht.

6.B.70 Die fertige Sicherheitspolitik muß in sich konsistent sein und sämtliche Sicherheitsziele und Bedrohungen berücksichtigen.

6.B.71 Nach den ITSEC sollen die Regeln für die Sicherheitspolitik in zwei Gruppen eingeteilt werden:

a) nichttechnische Maßnahmen, die aus materiellen, personellen oder organisatorischen Maßnahmen zur Kontrolle der Betriebsumgebung des EVG bestehen (z.B. die System-Sicherheitspolitik);

b) technische Maßnahmen, welche die Sicherheitsanforderungen begründen, aus denen sicherheitsspezifische Funktionen entwickelt werden können (z.B. die technische Sicherheitspolitik).

Das SWAN-System: System-Sicherheitspolitik

6.B.72 Eine erste, auf hohem Abstraktionsniveau erfolgende Beschreibung der System-Sicherheitspolitik könnte in den folgenden Regeln zusammengefaßt werden:

a) ein Anwender darf Zugang zu autorisierten Diensten haben;

b) eine Person darf keinen Zugang zu nicht autorisierten Diensten haben.

6.B.73 Es ist zu bedenken, daß

a) diese Aussage aufgrund des "Autorisierungs"-Konzepts einen Systemverwalter für die Zuwei-sung und Verifizierung der Autorisierung voraussetzt;

b) eine Autorisierung ihrerseits eine zusätzliche Menge an Ressourcen einbringt, die integritäts-sensitiv sind;

c) die Beschreibung nicht exakt genug ist, da sie dem Anwender keine Aufgabe zuweist.

6.B.74 Regel (a) betrifft nur Anwender und berücksichtigt nicht das System, das nach der ursprünglichen Hypothese (keine Verfügbarkeitsziele) kein bestimmtes Dienstgüteniveau bereitstellen muß. Somit ist Regel (a) offensichtlich eine nichttechnische Maßnahme.

6.B.75 Regel (b) dagegen bezieht sich auf das System, das dieses Verbot in Kraft setzen soll. Daher ist dies eine technische Maßnahme, die wie folgt umformuliert werden sollte:

a) das System muß den Zugang zu nicht autorisierten Diensten verwehren.

6.B.76 Diese Beschreibung der Sicherheitspolitik ist auf einem zu hohen Niveau angesiedelt, da sie die externen Anforderungen des Systems unberücksichtigt läßt. Diese Anforderungen weisen unter anderem darauf hin, daß dieses System ein Netz ist, das Verbindungen zwischen Terminals und Host-Rechnern in dem von einer verbindlichen Strategie erlaubten Rahmen öffnet, und daß jeder Anwendungsdienst lokal auf anwenderbestimmbarer Basis von einem Systemverwalter verwaltet wird. All dies sind sensitive Ressourcen und Aufgaben, die in einer detaillierteren Beschreibung der Sicherheitspolitik explizit angegeben werden müssen. Regel (b) kann wie folgt umformuliert werden:

a) (1) das System muß den Zugang zu nicht autorisierten Verbindungen verwehren;

b) (2) das System muß den Zugang zu nicht autorisierten Host-Rechnern verwehren.

6.B.77 Durch explizite Angabe der Bedrohungen läßt sich Regel (1) wie folgt unterteilen:

a) (1.1) das System muß das Eindringen in Verbindungen verhindern;

b) (1.2) das System muß den Zugang zu nicht autorisierten Verbindungen aufgrund einer regelbasierten Zugangskontrollpolitik verwehren.

6.B.78 Zu (1) und (2) gibt es keine entsprechenden Regeln für Terminals, die sowohl unintelligent als auch überwacht sind und nicht als bedroht gelten.

6.B.79 Regeln zur Festlegung der Pflichten des Systemverwalters können nunmehr in zwei weiteren Regeln explizit formuliert werden:

a) (3) ein (Anwendungs-) Systemverwalter kann Autorisierungen für Dienste ändern;

b) (4) das System muß die Änderung von Autorisierungen durch Dritte verwehren.

6.B.80 Die Pflichten des Netzverwalters (einschließlich der Verantwortung für die den Host-Rechnern zugewiesenen Sicherheitsstufen) könnten in derselben Weise explizit angegeben werden.

Formales Sicherheitsmodell

6.B.81 Die Sicherheitspolitik muß von den Evaluatoren aus unabhängiger Sicht auf Konsistenz geprüft werden. Zur Erleichterung der Nachprüfung können die Regeln in eine mathematische Form gebracht werden. Dies führt zu dem Konzept eines formalen Sicherheitsmodells, wie es für eine Evaluation ab E4 verlangt wird.

Produktbeschreibung

6.B.82 Da ein Produkt in einer beliebigen Zahl unterschiedlicher Systeme und Betriebsumgebungen eingesetzt werden kann, ist seine konkrete Betriebsumgebung nicht bekannt. Die Sicherheitsvorgaben können nur eine vorgesehene Art der Nutzung definieren und Annahmen über die Betriebsumgebung treffen, in der das Produkt eingesetzt werden soll, sowie über die Bedrohungen, denen seine sicherheitsspezifischen Funktionen begegnen sollen.

6.B.83 Im Falle eines Produkts enthalten die Sicherheitsvorgaben eine Liste von Aussagen des Antragstellers (in der Regel des Herstellers des Produkts) über den EVG, die dem potentiellen Käufer ausreichende Informationen für die von ihm zu treffende Entscheidung liefern sollen, ob ein Produkt zur Erreichung eines Teils oder der Gesamtheit seiner System-Sicherheitsziele geeignet ist. Diese Informationen werden in Form einer Produktbeschreibung vorgelegt.

6.B.84 Ein Produkt kann auf den Betrieb in verschiedenen Konfigurationen ausgelegt sein. Zum Beispiel kann ein Datenbankpaket auf einem Einplatzsystem oder als verteiltes Datenbanksystem in einer Netzumgebung betrieben werden. Bei solchen Produkten ist es unter Umständen nicht wünschenswert oder durchführbar, sämtliche Konfigurationen zu evaluieren, weshalb die Evaluatoren und der Antragsteller die zu evaluierende(n) Konfiguration(en) miteinander absprechen müssen. Dies muß in den Sicherheitsvorgaben dokumentiert werden.

6.B.85 Der Hersteller des Produkts muß nach Durchführung einer Reihe von Marktprüfungen geltend machen können, daß sein Produkt in der Lage ist, einen spezifischen Wert (oder eine Menge von Werten) zu schützen, der sich in einer vorgesehenen Betriebsumgebung befindet. Darüber hinaus muß der Hersteller in der Lage sein, einige (für die vorgesehene Betriebsumgebung relevanten) Bedro-hungen zu nennen, denen das Produkt entgegenwirken kann.

Sicherheitsspezifische Funktionen

6.B.86 Sicherheitsspezifische Funktionen (SEFs) sind auf höchstem Abstraktionsniveau eine Beschreibung der erforderlichen Funktionalität zur Erreichung der Sicherheitsziele. Die SEFs müssen ein nicht veränderbares und nicht umgehbares Ganzes bilden, das die in der Sicherheitspolitik formulierten Anforderungen voll erfüllt.

6.B.87 Der erste Schritt bei der Spezifikation der SEFs besteht darin, für jede einzelne Regel der Sicherheits-politik eine SEF zu formulieren und dabei eine eineindeutige Beziehung zwischen den SEFs und den Regeln herzustellen. Solche SEFs werden als *operationelle SEF* bezeichnet, da sie die Sicherheits-politik direkt implementieren. Es können weitere SEFs formuliert werden, die Funktionen zur Unterstützung der operationellen SEFs zur Verfügung stellen. Diese SEFs werden als *Support-SEF* bezeichnet.

6.B.88 Operationelle SEFs können einer der vier nachstehenden Funktionsarten zugeordnet werden:

a) Ausschließungsfunktionen, deren Ziel die Verhinderung potentieller Angriffe durch Minimie-rung von Werten ist; zum Beispiel kann ein System zwischen Anwendersitzungen von sensitiven Daten bereinigt werden.

b) Aufdeckungsfunktionen, deren Ziel die Aufdeckung und Zurückverfolgung von Angriffen ist;

c) Abgrenzungsfunktionen, deren Ziel die Kontrolle des Zugangs zu sensitive Ressourcen ist; mit diesen Funktionen kann eine Trennung erreicht, können Schutzmasken erzwungen oder kann der Zugriff auf transiente Daten verhindert werden. Kryptographische Mechanismen sind häufig Beschränkungsfunktionen;

d) Wiederherstellungsfunktionen, die Unterstützung bei der sicheren Wiederherstellung des EVG nach einem Fehler oder einem Angriff leisten.

6.B.89 Sobald alle operationellen SEFs formuliert worden sind, könnte der Verfasser der Sicherheitsvorgaben etwaige erforderliche Support-SEFs bestimmen. Diese SEFs müssen sicherstellen, daß die operationellen SEFs stets korrekt arbeiten und nicht ausgeschaltet werden können. Unterstützende SEFs sind wichtig, da sie Schutz für eine Teilmenge sensitiver Ressourcen bieten, d.h. die SEFs selbst. Die Bestimmung von Support-SEFs ist ein iterativer Prozeß, der endet, sobald alle SEFs (einschließlich der Support-SEFs selbst) geschützt sind.

6.B.90 Dieser iterative Prozeß eignet sich für die Entwicklung der Sicherheitsvorgaben. In den ITSEC wird allerdings kein Unterschied zwischen operationellen und Support-SEFs gemacht, sondern stattdessen wird vorgeschlagen, daß alle SEFs nach den folgenden generischen Oberbegriffen klassifiziert werden:

a) Identifikation und Authentisierung;

b) Zugriffskontrolle;

c) Beweissicherung;

d) Protokollauswertung;

e) Wiederaufbereitung;

f) Unverfälschtheit;

g) Zuverlässigkeit der Dienstleistung;

h) Datenübertragung (Übertragungssicherheit).

6.B.91 Diese Klassifizierung sicherheitsspezifischer Funktionen (SEFs) soll den Vergleich unterschiedlicher EVG erleichtern.

6.B.92 Die vordefinierten Funktionalitätsklassen sind Bestandteil der ITSEC, was dazu geführt hat, daß den generischen Oberbegriffen der ITSEC der Vorzug gegenüber anderen gegeben wird.

6.B.93 Häufig ist eine sicherheitsspezifische Funktion für mehr als einen Oberbegriff relevant. In diesem Fall erfolgt ein Querverweis auf andere Oberbegriffe. Ist ein bestimmter generischer Oberbegriff für die Funktionalitätsklasse nicht relevant, wird er weggelassen.

6.B.94 In diesem Stadium müssen die SEFs mit ausreichendem Detaillierungsgrad beschrieben werden, damit ihre Übereinstimmung mit der ihnen zugrundeliegenden Sicherheitspolitik nachgewiesen werden kann.

Das SWAN-System: Sicherheitsspezifische Funktionen

6.B.95 Um der angegebenen technischen Sicherheitspolitik entsprechen zu können, haben die SWAN-Entwickler folgende Funktionen vorgeschlagen:

a) Die Verbindungen zwischen Terminals und Host-Rechnern werden mit Hilfe von 'anerkannten', vor den Netzzugangspunkten befindlichen Geräten verschlüsselt. Den Endsystemen sind spezielle kryptographische Schlüssel zugewiesen. Die gewählte Lösung soll den Aussagen zufolge ein Eindringen in das Netz wirkungsvoll verhindern und ist eine Lösung für Regel (1.1).

b) Im Netz ist eine Funktion zur Kontrolle des Zugangs zu den Host-Rechnern installiert. Diese Funktion implementiert eine regelbasierte Zugangskontrollpolitik, deren Wirkung darin besteht, die Öffnung virtueller Verbindungen zwischen einem Terminal und einem Host-Rechner, die nicht derselben Sicherheitsstufe angehören, zu verhindern. Diese Alternative ist eine Lösung für Regel (1.2).

c) Anwenderbestimmbare Zugangskontrollfunktionen, wie sie bei der alten dedizierten Lösung für jeden Server festgelegt waren, werden beibehalten. Diese durch externe Anforderungen erzwungene Entscheidung ist repräsentativ für die Beschränkungen, die typisch für das System und die Betriebsumgebung sind; sie ist eine Lösung für Regel (2).

6.B.96 Der Entwickler schlägt eine vierte Sicherheitsfunktion (vgl. SWAN-Beispiel in Teil 5 des ITSEM) zur Authentisierung von Anwendern vor, die Zugang zum Netz verlangen. Ist in Anbetracht der Tatsache, daß die Sicherheitspolitik bereits durch drei Funktionen abgedeckt zu sein scheint, diese Funktion überflüssig? Es liegt auf der Hand, daß die Netzzugangskontrolle (Funktion 2) eine Authentisierung der Terminals impliziert. Eine Zugangskontrolle ist ohne eine damit verbundene Authentisierung nicht realisierbar. Muß in einem solchen Fall die Zugangskontrolle explizit sein?

6.B.97 Wenn allgemein die Antwort *nein* lautet, kann die explizite Aussage bis zur Verfeinerung der Zugangskontrolle hinausgeschoben werden. Im vorliegenden Fall hat sich der Entwickler für die Verwendung der gleichwertigen Anwenderauthentisierung anstelle der Terminalauthentisierung entschieden.

6.B.98 Eine vollständige Darstellung der SWAN-SEF würde die Prüfung der erforderlichen Support-Funktionen zur Gewährleistung des korrekten Betriebs der vier beschriebenen Betriebsfunktionen erfordern. Eine solche Darstellung würde auch die Maßnahmen einschließen, die zur Verifizierung dieser Funktionen, zur Beibehaltung der geheimen Elemente oder zur Vermeidung der Umgehung der Netzkontrollen ergriffen werden. Diese Maßnahmen werden durch den Schutz der neu in die Systemdefinition eingebrachten sensitiven Ressourcen gerechtfertigt. Alle diese Probleme werden in Teil 5 des ITSEM als Implementierungsprobleme dargestellt, sie sollten jedoch auch in den Sicherheitsvorgaben berücksichtigt werden.

Geforderte Sicherheitsmechanismen

6.B.99 Sicherheitsvorgaben können nach Wahl die Verwendung bestimmter Sicherheitsmechanismen vorschreiben oder verlangen, d.h. die Geräte, Algorithmen oder Prozeduren, die zur Implementierung bestimmter sicherheitsspezifischer Funktionen (SEF) verwendet werden sollen. Zu diesen Mechanis-men gehören wahrscheinlich

a) Algorithmen wie etwa Datenverschlüsselungsalgorithmen, Prüfsummenalgorithmen, Fehler-korrekturcodes, und Paßwort-Generierungsalgorithmen;

b) Identifikations- und Authentisierungsmechanismen wie etwa die Biometrik (Spracherkennung, Fingerabdrücke) und PID-Geräte.

6.B.100 Solche Mechanismen können für Analysen, die während der Spezifikation der Sicherheitsanforderungen durchgeführt werden, verbindlich vorgeschrieben werden.

6.B.101 Der Verfasser der Sicherheitsvorgaben soll eine Überspezifikation von Sicherheitsmechanismen, in denen sowohl die Sicherheitsziele als auch die zu ihrer Erreichung ergriffenen Maßnahmen verbindlich vorgeschrieben würden, im allgemeinen vermeiden.

6.B.102 Bisher sind in den Sicherheitsvorgaben die SEF in abstrakter Form ohne Verweisung auf die Implementierungsmechanismen spezifiziert worden. In der Praxis wird jede SEF durch einen oder mehrere Mechanismen realisiert, von denen jeder mehrere SEF betreffen kann.

6.B.103 Bei der Spezifikation der geforderten Mechanismen muß der Verfasser abwägen, ob sie sicherheitsrelevant sind und ob sie somit in den Sicherheitsvorgaben erscheinen sollen.

6.B.104 Grundsätzlich soll die Spezifikation von Sicherheitsmechanismen auf die Abdeckung von Sicherheitsanforderungen beschränkt sein. Diese Anforderungen können die Verwendung einer bestimmten Art von Technik, Algorithmus, Komponente oder Entwicklungsmethode empfehlen. Sie können sogar die Verwendung eines bestimmten Produkts oder Entwicklers vorschreiben.

6.B.105 Attribute, die nicht in den Sicherheitsvorgaben spezifiziert sind, werden implizit als Bestandteil des Implementierungsprozesses betrachtet und dem Entwickler überlassen. Solche Wahlmöglichkeiten müssen in den zur Unterstützung der Evaluation erstellten Evaluationsbeiträgen begründet werden.

Das SWAN-System: Geforderte Sicherheitsmechanismen

6.B.106 In dem SWAN-Beispiel bleiben die geforderten Sicherheitsmechanismen für die Systeminstallation unerwähnt. Trotzdem kann man sich vorstellen, daß der Entwickler die in den Server eingebauten Paßwort-Authentisierungsmechanismen wiederverwenden möchte.

Postulierte Mindeststärke der Mechanismen

6.B.107 Ein Mechanismus ist die Logik oder der Algorithmus, die/der eine bestimmte sicherheitsspezifische oder sicherheitsrelevante Funktion implementiert.

6.B.108 Manchen Mechanismen liegt insoweit eine Schwäche zugrunde, als sie durch Nutzung von Ressourcen, einer speziellen Ausstattung oder einer Gelegenheit von einem Angreifer überwunden werden können. Ein Beispiel dafür ist ein Authentisierungssystem, das durch sukzessives Abfragen aller möglichen Paßwörter außer Kraft gesetzt werden kann.

6.B.109 Diese Mechanismen können je nach Stärke des Angriffs, dem sie standhalten können, als niedrig, mittel oder hoch eingestuft (weitere Angaben siehe Anhang 6.C) werden.

6.B.110 In den Sicherheitsvorgaben soll eine Bewertung nach dem schwächsten kritischen Mechanismus des EVG postuliert werden.

Das SWAN-System: Postulierte Mindeststärke der Mechanismen

6.B.111 Die geforderte Mindeststärke der Mechanismen des SWAN-Systems als Ganzes ist *mittel*.

6.B.112 Um diese Anforderung an das System erfüllen zu können, hat der Entwickler folgende einzelnen Stärken der Mechanismen postuliert:

a) für den Mechanismus zur Implementierung der Gegenmaßnahme 1 (CM1), der beim Netz sich anmeldende Anwender authentisiert, lautet die postulierte Stärke des Mechanismus *niedrig*;

b) für den Mechanismus zur Implementierung der Gegenmaßnahme 2 (CM2), der für die Zugangskontrolle sorgt, lautet die postulierte Stärke des Mechanismus *hoch*;

c) für den Mechanismus zur Implementierung von Gegenmaßnahme 3 (CM3), der über die Verbindungen zwischen Terminals und Host-Rechner laufende Daten verschlüsselt, wird ein von der nationalen Behörde genehmigter Mechanismus *mittlerer* Stärke verwendet;

d) für den Mechanismus zur Implementierung von Gegenmaßnahme 4 (CM4), der beim Host-Rechner sich anmeldende Anwender authentisiert, lautet die angestrebte Stärke ebenfalls *niedrig*.

6.B.113 Zur Begründung dieser Wahl gibt der Entwickler in den Sicherheitsvorgaben an, daß nur der Verschlüsselungsmechanismus kritisch ist. Diese Begründung ist korrekt, da selbst bei einem Versagen der Zugriffskontrollmechanismen der Angreifer nur Zugriff auf verschlüsselte Daten erlangt und keine Möglichkeit hat, die Sicherheitsziele zu verletzen.

6.B.114 Es wurde eine Analyse (nicht in Teil 5 des ITSEM dargelegt) durchgeführt, die folgende Ergebnisse erbrachte:

a) der Verschlüsselungsmechanismus wurde von der nationalen Sicherheitsbehörde bewertet und von der Stärke her als *mittel* eingestuft;

b) die automatisch generierten Paßwörter bestehen aus 8 Zeichen und sind bis zu 60 Tage gültig, wobei keine Vorkehrungen zur Beschränkung ungültiger Paßwortversuche getroffen worden sind; die Authentisierung des Netzes und der Anwendungsdienste wurde mit *niedrig* bewertet;

c) auf das Netzmanagement oder auf geheime Absprachen mit dem Netzverwalter wird an dieser Stelle nicht eingegangen; ohne unterstützende Authentisierung wurde die strenge Netzzu-gangskontrolle mangels Bedrohungen mit Ausnahme der Netzüberwachung mit *hoch* bewertet.

Die Evaluationsstufe

Auswahl einer Evaluationsstufe

6.B.115 In den Sicherheitsvorgaben muß die angestrebte Evaluationsstufe für die Evaluation des EVG spezifiziert werden. Diese muß einer der Bewertungen E1, E2, E3, E4, E5 oder E6 entsprechen.

6.B.116 Die gewählte Evaluationsstufe ist ein Kompromiß zwischen dem, was wünschenswert (d.h. maximale Vertrauenswürdigkeit) ist, und dem, was unter Berücksichtigung des Kostenaufwands möglich ist. Nicht nur die Kosten für die eigentliche Evaluation müssen sorgfältig geprüft werden, sondern auch andere Kosten wie etwa für die Erstellung und Weitergabe der geforderten Evaluationsbeiträge.

6.B.117 Abbildung 6.B.7 und 6.B.8 enthalten eine Zusammenfassung der Wirkung der Evaluationsstufe auf den Inhalt von Sicherheitsvorgaben.

Benötigte Informationen

6.B.118 Evaluationsstufen unterscheiden sich durch den unterschiedlichen Detaillierungsgrad der für die Evaluation benötigten Entwurfsinformationen. Dies ist aus der nachfolgenden Tabelle zu ersehen:

Abbildung 6.B.3 Stufe und Informationen

Evaluationsstufe	Benötigte Informationen
E1	Architekturentwurf
E2	Architekturentwurf und Feinentwurf
ab E3	Architekturentwurf, Feinentwurf, Quellcode und Hardware-Konstruktionszeichnungen

Spezifikationsform

6.B.119 Wie aus der nachfolgenden Tabelle zu ersehen ist, erfordern die verschiedenen Evaluationsstufen unterschiedliche Spezifikationsstufen:

Abbildung 6.B.4 Stufe und Form

Evaluationsstufe	Spezifikationsform
E1, E2, E3	Informelle Dokumentation
E4, E5	Zugrundeliegendes formales Modell einer Sicherheitspolitik, semiformale Spezifikation der sicherheitsspezifischen Funktionen und semiformale Beschreibungen der Architektur und des Feinentwurfs
E6	Zugrundeliegendes formales Modell einer Sicherheitspolitik, formale Spezifikation der sicherheitsspezifischen Funktionen, formale Beschreibungen der Architektur und semiformale Beschreibung des Feinentwurfs

Genauigkeit der Spezifikation

6.B.120 Die Genauigkeit der Einhaltung von Inhalt, Form und Nachweis hängt ebenfalls von der angestrebten Evaluationsstufe ausgehend von den Übergängen zwischen *darlegen/angeben*, *beschreiben*, *erklären* ab. Die Anforderungen für die einzelnen Evaluationsstufen sind in Abbildung 6.B.5 zusammengefaßt.

Abbildung 6.B.5 Genauigkeit der Spezifikation

Anforderungen an Nachweise	Angestrebte Evaluationsstufe					
	E1	E2	E3	E4	E5	E6
	darlegen/ angeben		*beschreiben*		*erklären*	
Vorgelegte relevante Fakten	✓	✓	✓	✓	✓	✓
Aufgelistete Eigenschaften			✓	✓	✓	✓
Gegebene Begründungen					✓	✓

6.B.121 Zum Beispiel könnte auf E1 und E2 in den Sicherheitsvorgaben ein Anmeldeprozeß wie folgt beschrieben werden:

> Der <EVG> muß autorisierte Anwender durch Überprüfen der Gültigkeit einer PID, einer Anwen-der-ID und eines Paßworts identifizieren und authentisieren. Die Übereinstimmung von PID, An-wender-ID und Paßwort wird überprüft. Anwendern werden maximal drei Versuche zur erfolgrei-chen Durchführung des Anmeldeprozesses zugestanden. Wenn die Anzahl der Versuche drei über-schreitet, muß der Mißerfolg protokolliert und der Anwender aus dem System ausgesperrt werden.

6.B.122 Auf E3 und E4 soll der Prozeß ausführlicher beschrieben werden, indem die Eigenschaften des Anmeldeprozesses aufgelistet werden. Die Sicherheitsvorgaben könnten Angaben wie die folgenden enthalten:

> Der <EVG> muß autorisierte Anwender durch Prüfen der Gültigkeit einer PID, einer Anwender-ID und eines Paßworts identifizieren und authentisieren. Das System muß überprüfen,
>
> a) ob die mit der Tastatur eingegebene Anwender-ID mit der in maschinenlesbarer Form vorliegenden Anwender-ID im PID übereinstimmt;
>
> b) ob die Anwender-ID in der Anwenderauthorisierungsdatei eingetragen ist;
>
> c) ob das Paßwort für die Anwender-ID gültig ist.
>
> Wenn die Anzahl der Versuche über drei hinausgeht, muß das System
>
> a) eine Protokollnachricht schreiben, in der die Art (d.h. erfolglose Anmeldung), das Datum und die Uhrzeit des Vorfalls, die Terminal-Kennung und der Anwendername genannt werden;

b) den Anwender aus dem System aussperren, indem es ihm den Zutritt zur Anwender-authorisierungsdatei verwehrt.

6.B.123 Auf E5 und E6 sind Erklärungen erforderlich, die eine Begründung für die spezifizierte Funktionalität liefern. Die Sicherheitsvorgaben könnten Angaben wie die folgenden enthalten:

a) Protokollauswertung mißlungener Anmeldeversuche warnt den Sicherheitsbeauf-tragten, daß ein bestimmtes Terminal, ein spezifisches Anwenderkonto oder das System als Ganzes angegriffen wird;

b) Zugriff auf die Anwenderauthorisierungsdatei wird dem Anwender verwehrt, um den Zugang zum System zu verhindern, bis die Autorisierung des Sicherheits-beauftragten vorliegt.

Einsatz von Werkzeugen

6.B.124 Wie aus der nachfolgenden Tabelle zu ersehen ist, werden für die verschiedenen Evaluationsstufen unterschiedliche Werkzeuge benötigt:

Abbildung 6.B.6 Stufe und Werkzeuge

Evaluationsstufe	Benötigte Werkzeuge
E1	Keine
ab E2	Testwerkzeuge
ab E3	Klar definierte Programmiersprachen
ab E4	Entwicklerwerkzeuge, Werkzeuggestütztes Konfigurationskontrollsystem
ab E6	Objektcode-Analysewerkzeuge

Das SWAN-System: Evaluationsstufe

6.B.125 Es wurde eine Vertrauenswürdigkeitsstufe von E3 beschlossen. Diese gewährleistete ein ausreichen-des Maß an Vertrauenswürdigkeit und war im Rahmen der beschränkten finanziellen und zeitlichen Möglichkeiten realisierbar.

Abbildung 6.B.7 Sicherheitsvorgaben für eine Produktevaluation

			E1	E2	E3	E4	E5	E6
1.	Einleitung							
	1.1	Postulierte Mindeststärke der Mechanismen {2.25}	○	○	○	○	○	○
	1.2	Angestrebte Evaluationsstufe {2.26}	○	○	○	○	○	○
2.	Produktbeschreibung {2.16-2.17}							
	2.1	Sicherheitsziele	○	○	○	○	○	○
	2.2	Vorgesehene Art der Nutzung {2.17}	○	○	○	○	○	○
	2.3	Vorgesehene Betriebsumgebung {2.17}	○	○	○	○	○	○
	2.4	Angenommene Bedrohungen {2.17}	○	○	○	○	○	○
3.	Modell einer Sicherheitspolitik {2.81-2.83}					◎	◎	◎
4.	Spezifikation sicherheitsspezifischer Funktionen {2.18-2.24}		○	○	○	⊙	⊙	◎
		[Def. sicherheitsspezifischer Funktionen]	○	○	○	⊙	⊙	◎
		[Def. der geforderten Sicherheitsmechanismen (optional)]	○	○	○	⊙	⊙	◎
	4.1	Identifikation und Authentisierung {2.34-2.36}	○	○	○	⊙	⊙	◎
	4.2	Zugriffskontrolle {2.37-2.39}	○	○	○	⊙	⊙	◎
	4.3	Beweissicherung {2.40-2.42}	○	○	○	⊙	⊙	◎
	4.4	Protokollauswertung {2.43-2.45}	○	○	○	⊙	⊙	◎
	4.5	Wiederaufbereitung {2.46-2.48)	○	○	○	⊙	⊙	◎
	4.6	Unverfälschtheit {2.49-2.51}	○	○	○	⊙	⊙	◎
	4.7	Zuverlässigkeit der Dienstleistung {2.52-2.54}	○	○	○	⊙	⊙	◎
	4.8	Datenübertragung {2.55-2.58}	○	○	○	⊙	⊙	◎

usw.

Erläuterung zur Spezifikationsform: ○ informell; ⊙ semiformal & informell; ◎ formal & informell

Abbildung 6.B.8 Sicherheitsvorgaben für eine Systemevaluation

		E1	E2	E3	E4	E5	E6
1.	Einleitung						
1.1	Postulierte Mindeststärke der Mechanismen {2.25}	○	○	○	○	○	○
1.2	Angestrebte Evaluationsstufe {2.26}	○	○	○	○	○	○
2.	System-Sicherheitspolitik {2.9-2.15}						
2.1	Sicherheitsziele {2.9}	○	○	○	○	○	○
2.2	Beschreibung der Betriebsumgebung {2.9}	○	○	○	○	○	○
2.3	Tatsächliche Bedrohungen {2.9}	○	○	○	○	○	○
3.	Modell einer Sicherheitspolitik {2.81-2.83}				◎	◎	◎
4.	Spezifikation sicherheitsspezifischer Funktionen {2.18-2.24}	○	○	○	⊙	⊙	◎
	[Def. sicherheitsspezifischer Funktionen]	○	○	○	⊙	⊙	◎
	[Def. der geforderten Sicherheitsmechanismen (optional)]	○	○	○	⊙	⊙	◎
4.1	Identifikation und Authentisierung {2.34-2.36}	○	○	○	⊙	⊙	◎
4.2	Zugriffskontrolle {2.37-2.39}	○	○	○	⊙	⊙	◎
4.3	Beweissicherung {2.40-2.42}	○	○	○	⊙	⊙	◎
4.4	Protokollauswertung {2.43-2.45}	○	○	○	⊙	⊙	◎
4.5	Wiederaufbereitung {2.46-2.48)	○	○	○	⊙	⊙	◎
4.6	Unverfälschtheit {2.49-2.51}	○	○	○	⊙	⊙	◎
4.7	Zuverlässigkeit der Dienstleistung{2.52-2.54}	○	○	○	⊙	⊙	◎
4.8	Datenübertragung {2.55-2.58}	○	○	○	⊙	⊙	◎
usw.							

Erläuterung zur Spezifikationsform: ○ informell; ⊙ semiformal & informell; ◎ formal & informell

Anhang 6.C Wirksamkeit

Einleitung

6.C.1 In diesem Anhang wird die Anwendung der ITSEC im Bereich der Wirksamkeit beschrieben.

Mechanismen

Klassifizierung der Mechanismen

6.C.2 In diesem Abschnitt werden die unterschiedlichen Typen von Mechanismen beschrieben, die innerhalb eines EVG angewendet werden können.

6.C.3 In den ITSEC, Absatz 6.59 wird ein Sicherheitsmechanismus als die Logik oder der Algorithmus definiert, die/der eine bestimmte sicherheitsspezifische oder sicherheitsrelevante Funktion in Hardware und Software implementiert. Ein kritischer Mechanismus wird in den ITSEC, Absatz 6.22 als Mechanismus innerhalb eines Evaluationsgegenstandes definiert, dessen Ausfall eine Sicherheitslücke schaffen würde.

6.C.4 Ein *Mechanismus vom Typ A* ist ein Sicherheitsmechanismus mit einer potentiellen Schwachstelle in seinem Algorithmus, seinen Prinzipien oder seinen Eigenschaften, aufgrund derer er durch Einsatz ausreichender Ressourcen, Fachkenntnisse und entsprechender Gelegenheiten mit einem direkten Angriff überwunden werden kann. Ein Beispiel für einen Mechanismus vom Typ A ist ein Authentisierungsprogramm, bei dem ein Paßwort verwendet wird; wenn das Paßwort erraten werden kann, indem nacheinander alle möglichen Paßwörter ausprobiert werden, handelt es sich um einen Authentisierungsmechanismus vom Typ A. Mechanismen vom Typ A bedienen sich häufig eines "Geheimnisses" wie etwa eines Paßworts oder eines kryptographischen Schlüssels.

6.C.5 Alle Mechanismen vom Typ A eines EVG haben eine Stärke, die dem Aufwand an Ressourcen, Fachkenntnissen und Gelegenheiten, zur Gefährdung der Sicherheit durch einen direkten Angriff auf den Mechanismus entspricht.

6.C.6 Bei der Bewertung der Stärke eines Mechanismus soll der Kontext, in dem der Mechanismus eingesetzt wird, mit berücksichtigt werden. Siehe den Unterabschnitt *Beispiele* weiter unten.

6.C.7 Ein *Mechanismus vom Typ B* ist ein Sicherheitsmechanismus, der bei perfekter Konzipierung und Implementierung keine Schwächen aufweist. Ein Mechanismus vom Typ B kann als nicht durch einen direkten Angriff überwindbar betrachtet werden, gleichgültig, wie groß der Aufwand an Ressourcen, Fachkenntnissen und entsprechenden Gelegenheiten ist. Ein mögliches Beispiel für einen Mechanismus vom Typ B wäre die Zugangskontrolle auf der Basis von Zugangskontrollisten: Bei perfekter Konzipierung und Implementierung kann dieser Mechanismus vom Typ B nicht durch einen direkten Angriff überwunden werden. Mechanismen vom Typ B können jedoch durch indirekte Angriffe überwunden werden, mit denen sich andere Wirksamkeitsanalysen befassen.

6.C.8 Die Sicherheitsvorgaben eines EVG sollen die Mindeststärke der Mechanismen vorgeben, d.h. die Stärke des schwächsten Mechanismus vom Typ A im EVG. Die Analyse der Stärke der Mechanismen durch den Entwickler kann

a) die kritischen Mechanismen aufzeigen und erklären, warum die übrigen Mechanismen nicht kritisch sind;

b) die Stärke jedes einzelnen kritischen Mechanismus vom Typ A darlegen und bestätigen;

c) bestätigen, daß kritische Mechanismen vom Typ B keine Schwächen aufweisen (ggf. durch Verweis auf andere Wirksamkeitsanalysen).

Beispiel

6.C.9 Ein Sicherheitsmechanismus ist die Logik oder der Algorithmus, die/der eine bestimmte sicherheitsspezifische oder sicherheitsrelevante Funktion in Hardware und Software implementiert. Beispielsweise könnte ein komplexer Paßwortalgorithmus *A* von einem einfachen Paßwortalgorithmus *B* abgeleitet und durch das Prinzip *C* verstärkt sein, mit welchem die Anzahl der erneuten Eingabeversuche bei einer fehlgeschlagenen Authentisierung begrenzt wird: Während ein Entwickler diesen Algorithmus *A* unter Umständen als durch einen einzelnen Sicherheitsmechanismus M_A implementiert ansieht, betrachtet ein anderer Entwickler denselben Algorithmus *A* statt dessen als durch die beiden Mechanismen M_B und M_C implementiert, wovon M_B den Algorithmus *B* und M_C das Prinzip *C* implementiert. Wenn daher im vorhandenen Entwurf nur der Algorithmus *B* angewendet wird und beide Entwickler ihn durch Anwendung von Algorithmus *A* verstärken, gilt folgendes:

a) der erste Entwickler betrachtet dieses Vorgehen als Stärkung des Mechanismus;

b) der zweite Entwickler betrachtet dasselbe Vorgehen als Anwendung eines zusätzlichen Mechanismus.

6.C.10 Da beide Vorgehensweisen in der Praxis identisch sind, sind die Fälle in den obigen Absätzen a) und b) gleichwertig. Die beiden Situationen sind in Abbildung 6.C.1 dargestellt.

6.C.11 In der Abbildung gehören sowohl Mechanismus A als auch Mechanismus B zum Typ A, da sie durch direkten Angriff (z.B. wiederholtes Ausprobieren von Paßwörtern) überwunden werden können. Mechanismus A einerseits und Mechanismus B im Kontext von Mechanismus C andererseits haben die gleiche Stärke. Ein Teil der Stärke des Mechanismus A beruht darauf, daß er die Anzahl der Wiederholungen begrenzt. Mechanismus B weist zwar keine solche Begrenzung auf, jedoch muß er unter Berücksichtigung seines Kontextes bewertet werden. Daher stärkt die Tatsache, daß Mechanis-mus C die Wiederholungen begrenzt, die Kombination aus Mechanismus B und C.

Die Wirksamkeitskriterien

Wirksamkeit und Korrektheit

6.C.12 Im allgemeinen hängt die Arbeitsteilung zwischen Korrektheit und Wirksamkeit von den Sicherheitsvorgaben ab. Der Grund ist, daß die Korrektheit die Funktionalität betrifft und an den Spezifikationen in den Sicherheitsvorgaben gemessen wird, während die Wirksamkeit sich mit dem Mangel an ausnutzbaren Schwachstellen befaßt. Je mehr Einzelangaben in den Sicherheitsvorgaben enthalten sind, desto größer ist der anteilige Evaluationsaufwand für die Bewertung der Korrektheit.

6.C.13 Sicherheitsvorgaben könnten beispielsweise verlangen, daß die Funktionalität der Identifikation und der Authentisierung mit einer hohen Stärke des Mechanismus implementiert wird, ohne daß der Mechanismus selbst vorgegeben wird. Eine Implementierung, die den Anwendern die Eingabe von aus zwei Zeichen bestehenden Paßwörtern erlaubt, würde in diesem Fall als unwirksam zurückgewiesen. Wenn die Sicherheitsvorgaben keine Paßwörter mit zwei Zeichen zulassen, würde dieselbe Implementierung aus Gründen der Korrektheit abgelehnt.

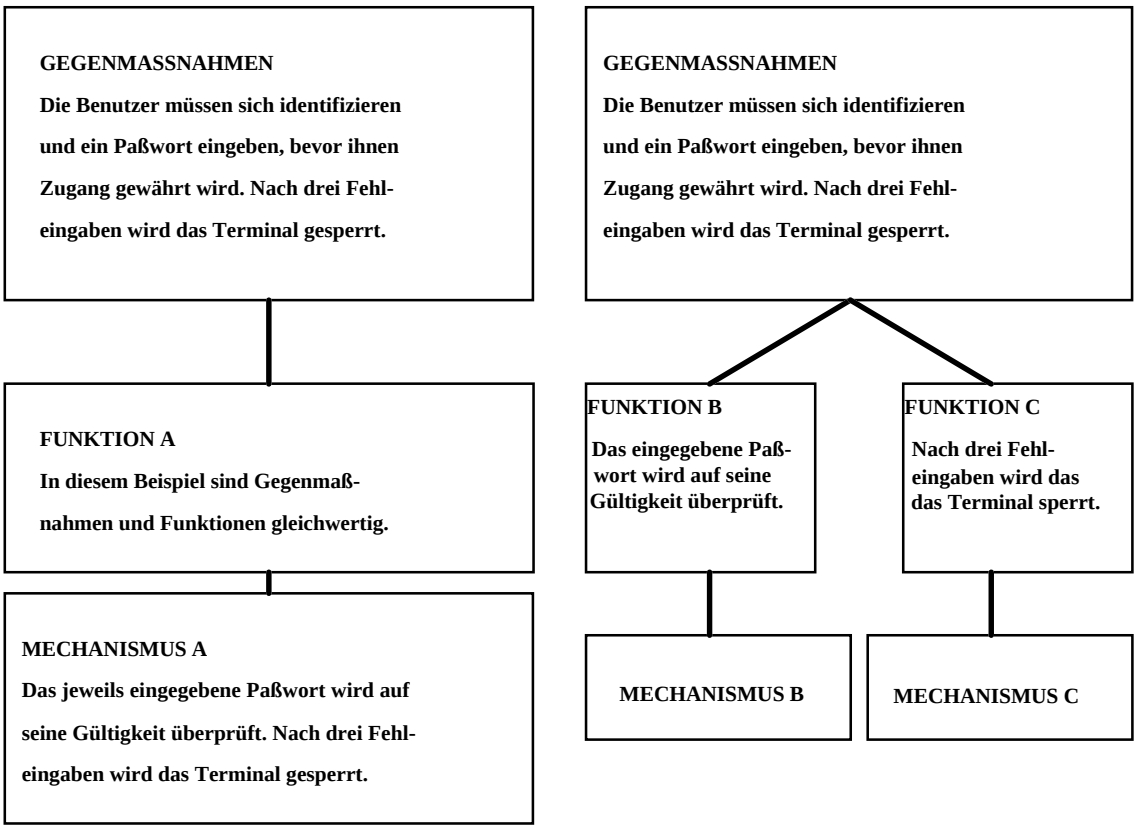


Abbildung 6.C.1 Zwei Arten der Behandlung von Mechanismen

Wirksamkeitsaspekte

6.C.14 Dieser Unterabschnitt befaßt sich mit den Beziehungen zwischen den Wirksamkeitskriterien.

6.C.15 Es ist hilfreich, die Wirksamkeitskriterien aus der Sicht des Entwicklers zu betrachten. Der Entwickler soll eine Risikoabschätzung vornehmen, um die erforderlichen sicherheitsspezifischen Funktionen zu bestimmen, und dabei folgendes zugrunde legen:

a) eine allgemeine Definition der erforderlichen (nicht sicherheitsrelevanten) Funktionalität des EVG;

b) die Bedrohungen des EVG und/oder der Sicherheitsziele des EVG;

c) die durch den EVG zu schützenden Werte (Werte können Informationen oder Software sein, deren Vertraulichkeit, Integrität und Verfügbarkeit zu schützen sind).

6.C.16 Bei der Auswahl der sicherheitsspezifischen Funktionen soll der Entwickler entscheiden, ob diese

a) geeignet sind, d.h., ob sie der/den Bedrohung(en) entgegenwirken;

b) in der Lage sind zusammenzuarbeiten (d.h. zusammenwirken), falls mehr als eine sicherheitsspezifische Funktion ausgewählt wurde, und zwar so, daß sich die Funktionen gegenseitig verstärken und ein integriertes und wirksames Ganzes bilden.

6.C.17 Eine einfache schematische Darstellung dieses Verfahrens ist in Abbildung 6.C.2 wiedergegeben. In dieser Abbildung (sowie in den Abbildungen 6.C.3 und 6.C.4) werden die einzelnen Elemente wie folgt dargestellt:

a) die Werte durch "ECU";

b) die Bedrohungen durch "Nägel", deren Länge "proportional" zur Menge der Fachkenntnisse, Gelegenheiten und Ressourcen ist, über die der Angreifer verfügt;

c) die Gegenmaßnahmen (z.B. sicherheitsspezifische Funktionen) durch einen "Wall", dessen Breite "proportional" zur Stärke der Mechanismen vom Typ A ist, durch die sie implementiert werden (d.h. die Fähigkeit der Gegenmaßnahmen zur Abwehr eines direkten Angriffs).

6.C.18 Je länger der "Nagel", desto schwerwiegender die Bedrohung; je breiter der Wall, desto größer die Fähigkeit der Gegenmaßnahmen, diese Bedrohung der Werte abzuwehren. Der EVG kann als gesichert angesehen werden, wenn die Werte vollständig von einem Wall umgeben sind, dessen Mindestdurchmesser gleich groß wie oder größer als die Länge aller Nägel ist.

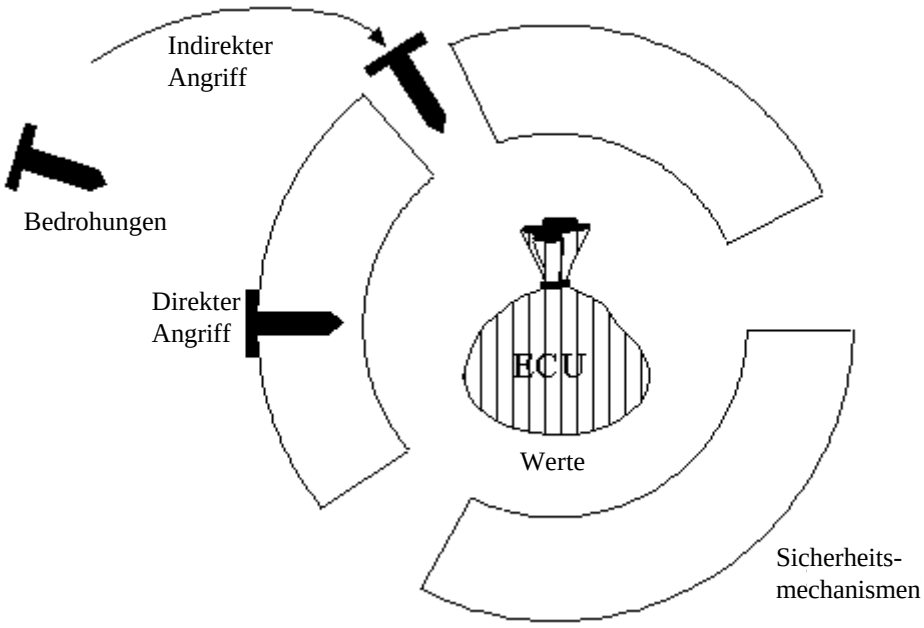


Abbildung 6.C.2 Das Fehlschlagen von Eignung und Zusammenwirken

6.C.19 In Abbildung 6.C.2 ist der Fall dargestellt, daß die gewählten sicherheitsspezifischen Funktionen zur Abwehr der Bedrohung nicht ausreichen, obwohl ihre Mechanismen ausreichende Stärke aufweisen. Die Abbildung gibt den Entwurf eines sicheren Betriebssystems wieder (z.B. F-B2), bei dem der Entwickler versäumt hat, die notwendigen Mechanismen bereitzustellen, mit denen die traditionellen sicherheitsspezifischen Funktionen (z.B. Identifikation und Authentisierung, Zugangskontrolle usw.) vor externen Eingriffen und Verfälschungen geschützt werden. In dieser Phase der Schwach-stellenbewertung könnte der Entwickler geltend machen, daß seine Lösung bislang

a) ungeeignet ist, da sie der Bedrohung nicht entgegenwirkt;

b) nicht zusammenwirkt, da sie kein integriertes Ganzes bildet.

6.C.20 Diese Mängel sind in Abbildung 6.C.3 behoben, in der die Einführung einer zweiten Reihe von Gegenmaßnahmen dargestellt ist, die die erste Reihe von Gegenmaßnahmen vor externen Eingriffen oder Verfälschungen schützen soll.

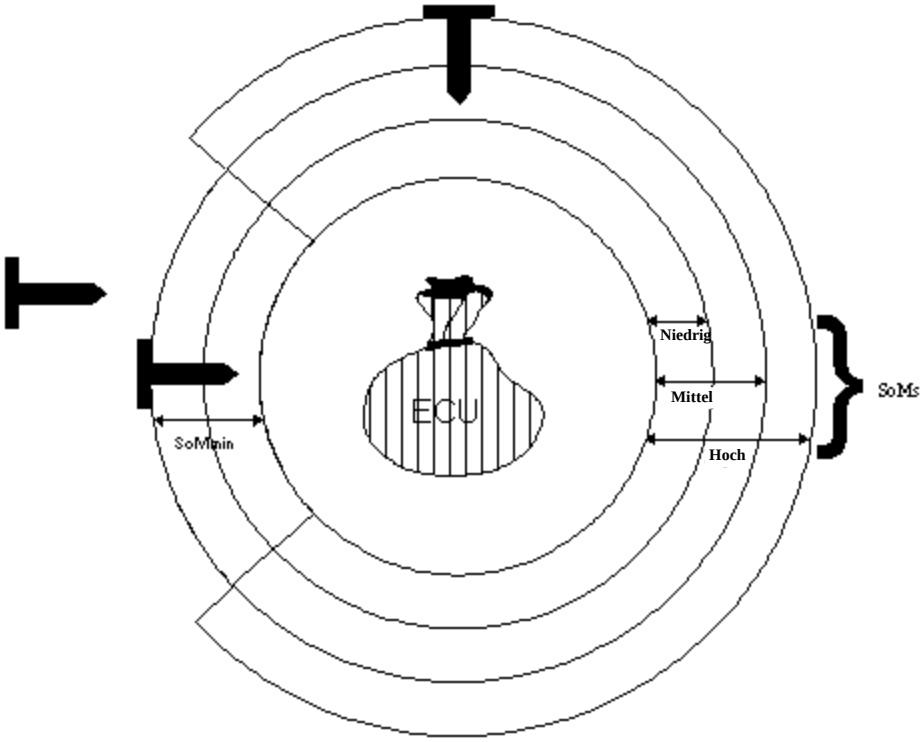


Abbildung 6.C.3 Ein sicherer EVG

6.C.21 Aus dieser Abbildung geht auch die Breite des 'Walls' von Gegenmaßnahmen hervor, die zur Erfüllung der ITSEC-Definitionen für die Stärke der Mechanismen (SoM) erforderlich ist: *niedrig*, *mittel* und *hoch*. Die Schutzmechanismen sind mit *hoch* dargestellt, die ursprünglichen Gegenmaßnahmen mit *mittel*. Ist die Mindeststärke der Mechanismen (SoM_{min}) *mittel*, dann geht aus dieser Abbildung hervor, daß der EVG die Kriterien für Eignung, Zusammenwirken und Stärke der Mechanismen erfüllen dürfte:

a) die Mindestbreite des 'Walls' ist mittel, was bedeutet, daß er die Anforderungen hinsichtlich der Stärke der Mechanismen erfüllt;

b) der 'Wall' umgibt die Werte vollständig und lückenlos, so daß die Gegenmaßnahmen der Bedrohung entgegenwirken und die Kriterien für Eignung und Zusammenwirken erfüllt sind.

6.C.22 Der Entwickler soll seine Schwachstellenbewertung in jeder Entwicklungsstufe wiederholen. Vom Standpunkt der Evaluation gesehen soll er dies so lange tun, bis alle in Abb 4 der ITSEC aufgeführten Informationen für die betreffende Evaluationsstufe berücksichtigt worden sind.

6.C.23 In Abbildung 6.C.4(a) wird eine Schwachstelle als 'Abnahme der Breite des durch die Gegenmaßnahmen gebildeten Walls' dargestellt, d.h., der Wall weist nicht die von SoM_{min} geforderte Breite auf. In diesem Fall entspricht die Bewertung der Stärke des Mechanismus des EVG der niedrigsten Bewertung jedes kritischen Mechanismus.

6.C.24 Nach den ITSEC sind vier Möglichkeiten gegeben, wie der Entwickler seinen Entwurf modifizieren kann, um dieser Schwachstelle entgegenzuwirken:

a) Dem Entwickler steht es frei, die Schwachstelle als Nichterfüllung der Anforderungen an die Mindeststärke des Mechanismus durch die den betreffenden Mechanismen zugrundeliegenden Algorithmen, Prinzipien und Eigenschaften anzusehen. In diesem Fall hat der Entwickler die Möglichkeit, die vorhandenen Algorithmen, Prinzipien und Eigenschaften so zu ändern (oder neue Algorithmen, Prinzipien und Eigenschaften anzuwenden), daß die geforderte SoM_{min} erfüllt wird. Wenn der Entwickler diese Vorgehensweise wählt, sieht das Ergebnis wie in Abbildung 6.C.4(b) dargestellt aus.

b) Als Alternative dazu kann der Entwickler gemäß den ITSEC, Absatz 3.27 (erster Punkt), der das Kriterium der Bewertung der **Konstruktionsschwachstellen** betrifft, einen oder mehrere zusätzliche EVG-interne Sicherheitsmechanismen einführen. Wenn der Entwickler diese Vorgehensweise wählt, sieht das Ergebnis wiederum wie in Abbildung 6.C.4(b) dargestellt aus. Diese Vorgehensweise ist gleichbedeutend mit der ersten.

c) Laut dem zweiten Punkt der ITSEC, Absatz 3.27 zum Kriterium für die Bewertung der Konstruktionsschwachstellen (oder zum Kriterium für **operationelle Schwachstellen**) kann der Entwickler die Einführung einer externen Gegenmaßnahme fordern. Bei dieser Vorgehensweise sieht das Ergebnis wie in Abbildung 6.C.4(c) dargestellt aus. Wenn diese Vorgehensweise gewählt wird, soll die Gegenmaßnahme in den Sicherheitsvorgaben dokumentiert werden.

d) Und schließlich kann der Entwickler gemäß dem Kriterium für die Benutzerfreundlichkeit eine Kombination von internen und externen Maßnahmen einführen, die die Schwachstelle zwar nicht direkt beheben (d.h. den Wall verbreitern), die aber den Effekt haben, daß jeder Versuch, die Schwachstelle auszuwerten, einem Endanwender oder Systemverwalter zur Kenntnis gebracht wird. Diese Vorgehensweise ist in Abbildung 6.C.4(d) dargestellt. Dieser Fall wäre z.B. gegeben, wenn die Benutzung von verdeckten Kanälen, die nicht beseitigt werden können, durch ein sicheres Betriebssystem überwacht wird.

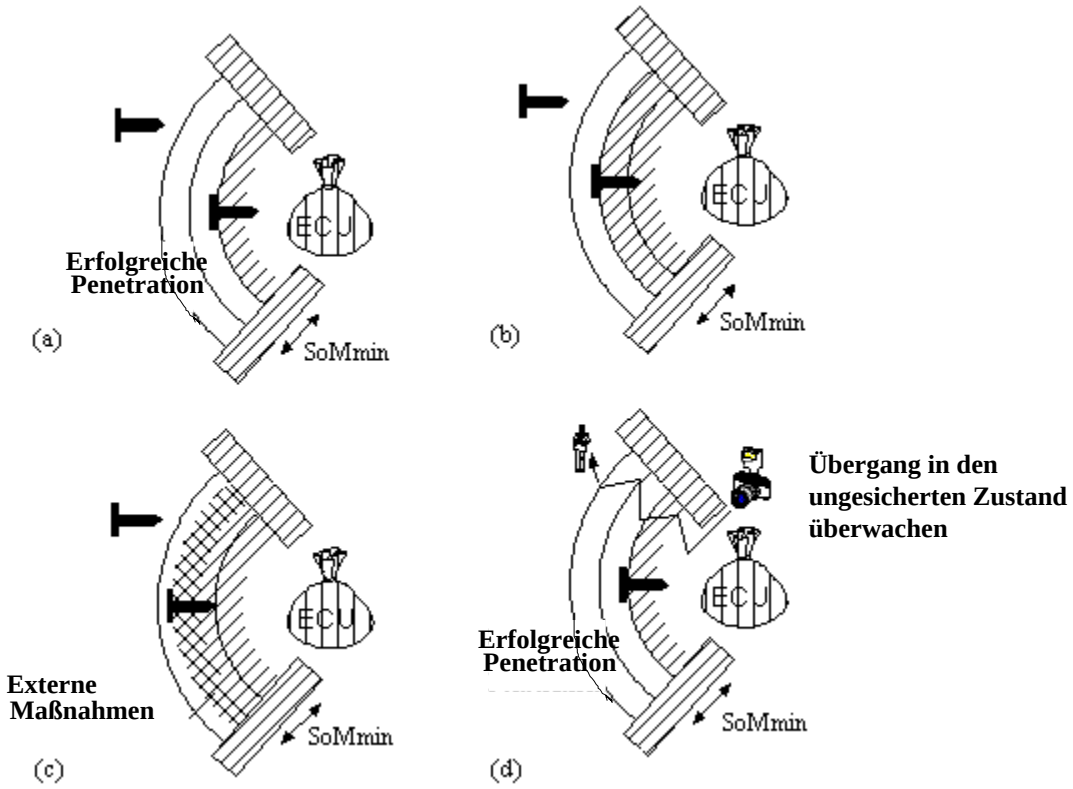


Abbildung 6.C.4 Beseitigung von Sicherheitsschwachstellen

6.C.25 Sobald der Entwickler sich entschieden hat, wie er den zuvor ermittelten Schwachstellen entgegenwirken will, wird durch Anwendung des Kriteriums 'Zusammenwirken der Funktionalität' überprüft, ob die gewählte Lösung das Schwachstellenproblem tatsächlich beseitigt (das in dieser Entwurfsstufe ermittelt wurde) und keine weiteren Schwachstellen einführt. Sollte eine weitere Schwachstelle entdeckt werden, müßte der Entwickler seine Schritte zurückverfolgen und andere Lösungen mit internen und externen Gegenmaßnahmen wählen, bis das Kriterium des Zusammenwirkens der Funktionalität schließlich erfüllt ist.

6.C.26 Es ist darauf hinzuweisen, daß, wenn eine Schwachstelle entdeckt wird, diese häufig auf mehr als eine Art charakterisiert werden kann; so kann es mitunter schwierig sein zu entscheiden, ob es an der Eignung oder dem Zusammenwirken liegt. In der Praxis ist dies kein Problem. Es ist wichtiger, darauf vertrauen zu können, daß alle Schwachstellen entdeckt worden sind, als die verschiedenen Typen von Schwachstellen ohne allzu große Schwierigkeiten unterscheiden zu können.

6.C.27 Zusammenfassend sind zwei Arten von Wirksamkeitsfehlern zu unterscheiden:

a) Fehler hinsichtlich Inhalt, Form und Nachweis eines bestimmten Evaluationsbeitrags zur Wirksamkeit. Diese Art von Fehler entspricht einem bestimmten Wirksamkeitsaspekt;

b) Schwachstellen, die beim Penetrationstest entdeckt werden. Dieser Art von Schwachstellen einen Wirksamkeitsaspekt zuzuordnen, kann möglicherweise größere Schwierigkeiten bereiten.

Abschätzen der Stärke der Mechanismen

6.C.28 Nach den ITSEC (Absätze 3.6-3.8) haben Bewertungen der Stärke der Mechanismen folgende Bedeutung:

a) Damit die Mindeststärke eines kritischen Mechanismus als *niedrig* eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen zufälliges unbeabsichtigtes Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.

b) Damit die Mindeststärke eines kritischen Mechanismus als *mittel* eingestuft werden kann, muß erkennbar sein, daß er Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln bietet.

c) Damit die Mindeststärke eines kritischen Mechanismus als *hoch* eingestuft werden kann, muß erkennbar sein, daß er nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.

6.C.29 Diese Begriffsbestimmungen sind informell und sollen als Anleitung für Anwender eines EVG dienen. Dieser Unterabschnitt enthält Hinweise zu objektiveren Mitteln der Bemessung.

6.C.30 Da die Stärke der Mechanismen Fachkenntnisse, Gelegenheiten und Betriebsmittel (Ressourcen) betreffen, muß die Bedeutung dieser Begriffe näher erläutert werden:

a) *Fachkenntnisse* betreffen das Wissen, über das Personen verfügen müssen, um einen EVG angreifen zu können. Ein *Laie* ist jemand ohne besondere Fachkenntnisse; eine *kenntnisreiche* Person ist jemand, der mit der internen Arbeitsweise des EVG vertraut ist, und ein *Experte* ist jemand, der mit den zugrundeliegenden Prinzipien und Algorithmen des EVG vertraut ist.

b) *Ressourcen* betreffen die Mittel, die ein Angreifer für einen erfolgreichen Angriff auf den EVG aufwenden muß. Evaluatoren haben es in der Regel mit zwei Arten von Ressourcen zu tun: *Zeit* und *Ausstattung*. Unter Zeit ist die Zeit zu verstehen, die ein Angreifer für die Durchführung des Angriffs ohne die vorherige Denkarbeit benötigt. Zur Ausstattung gehören Rechner, elektronische Geräte, Hardware-Werkzeuge und Computer-Software. In diesem Zusammenhang

- bedeutet *innerhalb von Minuten*, daß ein Angriff in weniger als zehn Minuten erfolgreich durchgeführt werden kann; *innerhalb von Tagen* bedeutet, daß ein Angriff in weniger als einem Monat erfolgreich durchgeführt werden kann, und *innerhalb von Monaten* bedeutet, daß für einen erfolgreichen Angriff mindestens ein Monat benötigt wird.

- bedeutet *ohne Hilfsmittel*, daß zur Durchführung eines Angriffs keine besondere Ausstattung erforderlich ist; *vorhandene Ausstattung* bedeutet Ausstattung, die ohne weiteres in der Betriebsumgebung des EVG verfügbar oder Teil des eigentlichen EVG ist oder von jedermann käuflich erworben werden kann; *Sonderausstattung* ist eine besondere Ausstattung zur Durchführung eines Angriffs.

c) *Gelegenheiten* beziehen sich auf Faktoren, die im allgemeinen außerhalb der Kontrolle des Angreifers liegen würden, z.B. ob Hilfestellung durch eine andere Person benötigt wird (geheime Absprache), die Wahrscheinlichkeit eines Zusammentreffens bestimmter Umstände (Zufall) und die Wahrscheinlichkeit und die Konsequenzen einer Ermittlung des Angreifers (Entdeckung). Diese Faktoren sind im allgemeinen schwer zu bewerten. Auf den Fall der geheimen Absprache wird hier eingegangen, jedoch müssen ggf. auch andere Faktoren berücksichtigt werden. Die folgenden Abstufungen einer *geheimen Absprache* werden erörtert: *allein*, wenn keine Absprache erforderlich ist; *mit einem Anwender*, wenn der Angreifer, um einen erfolgreichen Angriff starten zu können, sich heimlich mit einem nicht vertrauenswürdigen Anwender des EVG absprechen muß; und *mit einem Systemverwalter*, wenn eine Absprache mit einem besonders vertrauenswürdigen Anwender des EVG getroffen werden muß. Bei dieser Definition der geheimen Absprache wird davon ausgegangen, daß der Angreifer kein authorisierter Anwender des EVG ist.

6.C.31 Die oben erörterten Faktoren gelten nicht als abschließend oder vollständig behandelt, sie sind lediglich als Orientierungshilfe gedacht. Sobald die Faktoren für einen bestimmten Mechanismus evaluiert worden sind, können zur Berechnung der Stärke des Mechanismus folgende Regeln angewandt werden:

a) Kann der Mechanismus innerhalb von Minuten von einem Laien allein überwunden werden, dann kann er nicht einmal als *niedrig* eingestuft werden.

b) Kann der Mechanismus nur von einem Experten mit Sonderausstattung überwunden werden, der dafür Monate braucht und eine geheime Absprache mit einem Systemverwalter treffen muß, dann ist er als *hoch* einzustufen.

c) Kann der Mechanismus nur in geheimer Absprache mit einem Anwender überwunden werden, dann ist er mindestens als *mittel* einzustufen.

d) Kann der Mechanismus nur in geheimer Absprache mit einem Systemverwalter überwunden werden, dann ist er als *hoch* einzustufen.

e) Sind für einen erfolgreichen Angriff Monate erforderlich, ist der Mechanismus mindestens als *mittel* einzustufen.

f) Erfordert ein erfolgreicher Angriff monatelange Bemühungen eines Experten und Sonderausstattung, dann ist der Mechanismus als *hoch* einzustufen, egal ob eine geheime Absprache notwendig ist oder nicht.

g) Sind für einen erfolgreichen Angriff tagelange Bemühungen erforderlich, ist der Mechanismus mindestens als *niedrig* einzustufen.

h) Kann ein erfolgreicher Angriff von jedem bis auf einen Laien innerhalb von Minuten durchgeführt werden, dann ist der Mechanismus als *niedrig* einzustufen.

i) Wenn für einen erfolgreichen Angriff ein Experte benötigt wird, der mit der vorhandenen Ausstattung Tage braucht, dann ist der Mechanismus als *mittel* einzustufen.

6.C.32 Anstatt diese Prädikate zu errechnen, können die Evaluatoren die Orientierungshilfen in den Abbildungen 6.C.5 und 6.C.6 anwenden. Dazu ist die in Abbildung 6.C.5 ermittelte Zahl für ZEIT und GEHEIME ABSPRACHE mit der in Abbildung 6.C.6 ermittelten Zahl für FACHKENNTNISSE und AUSSTATTUNG zu addieren:

a) Ist das Ergebnis 1, dann erreicht die Stärke nicht einmal die Stufe *niedrig*.

b) Ist das Ergebnis größer als 1, aber nicht größer als 12, dann erreicht die Stärke die Stufe *niedrig*.

c) Ist das Ergebnis größer als 12, aber nicht größer als 24, erreicht die Stärke die Stufe *mittel*.

d) Ist das Ergebnis größer als 24, erreicht die Stärke die Stufe *hoch*.

6.C.33 Die Werte in den Abbildungen 6.C.5 und 6.C.6 dienen nur zur Evaluation des Prädikats. Sie haben keine andere Bedeutung. Beispielsweise ist ein Angriff eines Laien ohne Hilfsmittel innerhalb von Minuten und in geheimer Absprache mit einem Anwender (Wert 13) im Ergebnis weder besser noch schlechter als der eines Experten ohne Hilfsmittel, der dafür Monate/Jahre braucht (Wert 22) - beide Fälle werden mit *mittel* bewertet.

Abbildung 6.C.5 Vergleichstabelle Zeit/geheime Absprache

ZEIT \ GEHEIME ABSPRACHE	allein	mit einem Anwender	mit einem Systemverwalter
innerhalb von Minuten	0	12	24
innerhalb von Tagen	5	12	24
Monate/Jahre	16	16	24

Abbildung 6.C.6 Vergleichstabelle Fachkenntnisse/Ausstattung

FACHKENNTNISSE \ AUSSTATTUNG	ohne Hilfsmittel	mit vorhandener Ausstattung	mit Sonderausstattung
Laie	1	entfällt	entfällt
kenntnisreiche Person	4	4	entfällt
Experte	6	8	12

6.C.34 Diese Tabellen sollen nur als Orientierungshilfe verwendet werden, da sie nicht unbedingt für alle Mechanismen und Betriebsumgebungen verwendbar sind. Sie sind nicht zur Bewertung kryptograph-ischer Mechanismen gedacht.(siehe ITSEC, Absatz 3.23).

Anhang 6.D Auswirkungsanalyse für die Reevaluation

Einleitung

6.D.1 Es ist unrealistisch anzunehmen, daß es im Laufe der Zeit nicht zu Veränderungen beim EVG selbst, seiner Betriebsumgebung oder seiner Entwicklungsumgebung kommt. Es ist wahrscheinlicher, daß die im Rahmen der IT-Sicherheit zu durchlaufenden Prozesse kontinuierlich weitergehen, wie dies in Teil 1 des ITSEM, Abbildung 1.1.1, dargestellt ist.

6.D.2 Ein Evaluationsergebnis gilt nur für ein bestimmtes Release oder eine bestimmte Version eines IT-Systems oder eines IT-Produkts. Daher könnte eine Änderung des EVG oder seiner Evaluationsbeiträge eine Reevaluation erforderlich machen. Bei jeder eintretenden Änderung eine vollständige Evaluation durchzuführen, ist unnötig, und es besteht durchaus die Möglichkeit, frühere Evaluationsergebnisse heranzuziehen. Da die Auswirkungen von Änderungen nicht immer sicherheitsrelevant sind, müssen die Konsequenzen einer Änderung in den obengenannten Bereichen - d.h., ob aufgrund einer Änderung eine Reevaluation erforderlich ist - im Rahmen eines als Auswirkungsanalyse bezeichneten Prozesses aufgezeigt werden.

6.D.3 Dieser Anhang enthält grundlegende Hinweise für Antragsteller, Entwickler und Systemakkreditierer und beschreibt den Prozeß der Auswirkungsanalyse, der folgende Punkte umfaßt:

a) wie die Notwendigkeit einer Reevaluation ermittelt wird;

b) wie die betroffenen Teile des EVG ermittelt werden;

c) welche Evaluatoraufgaben erneut durchgeführt werden müssen.

6.D.4 Teil 3 (in dem *Grundsätze, Konzepte und Prinzipien* beschrieben werden) und Teil 4 (in dem der *Evaluationsprozeß* beschrieben wird) des ITSEM bilden die Grundlage für Evaluationen. Teil 4, Kapitel 4.6, in dem die *Wiederverwendung* behandelt wird, steht in engem Zusammenhang mit diesem Anhang.

Auswirkungsanalyse

Überblick

6.D.5 Ein Evaluationsergebnis gilt nur für das Release und die Version eines EVG, das/die evaluiert wurde. Wenn sich bei einem EVG, seiner Betriebsumgebung oder seiner Entwicklungsumgebung spätere Änderungen ergeben, ist es Sache des Antragstellers, die Art der Änderung und die Konsequenzen für das Zertifikat/den Zertifizierungsreport zu bestimmen.

6.D.6 Je nach Art der Änderung kann es erforderlich sein, daß der Antragsteller/Entwickler die Zertifizierungsstelle von der Änderung in Kenntnis setzt. Wenn eine Reevaluation erforderlich wird, muß der Antragsteller/Entwickler einer ITSEF die entsprechenden Evaluationsbeiträge liefern.

6.D.7 Wichtigste Regel für dieses Verfahren ist, daß alle Entscheidungen anhand der Evaluationsstufe zu treffen sind, die für den EVG vergeben wurde. Da die vergebene Evaluationsstufe ein Maß für das in den EVG gesetzte Vertrauen auf Erfüllung der Sicherheitsvorgaben ist, muß eine Änderung mit derselben Strenge geprüft werden wie bei der ursprünglichen Evaluation. Andernfalls kann der Grad des Vertrauens nicht aufrechterhalten werden.

6.D.8 Ein Sonderfall liegt bei Änderungen der Entwicklungsumgebung oder der Hardware-Plattform vor. Im Verlauf einer Evaluation werden Werkzeuge ermittelt, die sicherheitsrelevant sind, z.B. der Compiler zur Generierung des Objektcodes.

6.D.9 Da es erhebliche Unterschiede im Hinblick auf die verwendeten Entwicklungswerkzeuge und deren Einfluß auf das Vertrauen in den EVG gibt, können keine allgemeingültigen Regeln für deren Behandlung aufgestellt werden. Änderungen in der Entwicklungsumgebung oder der Hardware-Plattform müssen daher fallspezifisch behandelt werden. Aufgabe der Evaluation ist es, diejenigen Werkzeuge zu ermitteln, die für die angestrebte Evaluationsstufe sicherheitsrelevant sind. Auf Verlangen können diese in Kapitel 7 des ETR zusammen mit anderen für die Auswirkungsanalyse nützlichen Informationen aufgeführt werden.

Voraussetzungen

6.D.10 Für den Prozeß der Auswirkungsanalyse sind Informationen über die Komponenten des EVG und seiner Entwicklungsumgebung erforderlich. Wenn ein Antragsteller die Reevaluation eines EVG für erforderlich erachtet, soll er die ITSEF ersuchen, solche Informationen in Kapitel 7 des ETR aufzunehmen.

6.D.11 Ein EVG und seine Entwicklungsumgebung bestehen aus einer Auswahl von Komponenten, die zusammenarbeiten und jeweils eine der folgenden Eigenschaften aufweisen. Die verschiedenen Arten von Komponenten sind wie folgt definiert (siehe Teil 3 des ITSEM):

a) SE (Security Enforcing): sicherheitsspezifisch;

b) SR (Security Relevant): sicherheitsrelevant;

c) SI (Security Irrelevant): nicht sicherheitsrelevant.

6.D.12 Die folgenden Beispiele gelten nur für die Anforderungen an die Vertraulichkeit. Die Identifikations- und Authentisierungskomponente eines Betriebssystems implementiert eine sicherheitsspezifische Funktion und gehört daher zum Typ SE. Das Steuermodul eines Betriebssystems stellt sicherheitsrelevante Software dar und zählt daher zum Typ SR. Die in Firmware und Hardware implementierte Speicherverwaltungseinheit einschließlich der von ihr bearbeiteten Daten ist sicherheitsspezifisch und gehört daher zum Typ SE. Der Prozessor eines Rechners, wiederum eine Kombination aus Firmware und Hardware, ist sicherheitsrelevant und zählt somit zum Typ SR. Nicht privilegierte Anwenderprogramme gehören zum Typ SI.

Der Prozeß

6.D.13 Das Grundkonzept für den Auswirkungsanalyseprozeß ist in Abbildung 6.D.1 dargestellt. Er umfaßt zwei Schritte: im ersten wird die Art der Änderung bestimmt, der zweite führt zu der Entscheidung über die Notwendigkeit einer Reevaluation und zu den je nach Art der Änderung erforderlichen Aufgaben.

Schritt 1 (Art der Änderung ermitteln)

6.D.14 Die Art der am EVG vorgenommenen Änderung muß anhand von Abbildung 6.D.2 bestimmt werden. Eine detaillierte Beschreibung des Prozesses und der zugrundeliegenden Überlegungen wird im folgenden gegeben.

6.D.15 Eine Änderung kann sich auf die Sicherheitsvorgaben, die Wirksamkeitskriterien oder die Korrektheitskriterien beziehen. Diese Änderung kann Konsequenzen für das in den EVG gesetzte Vertrauen haben.

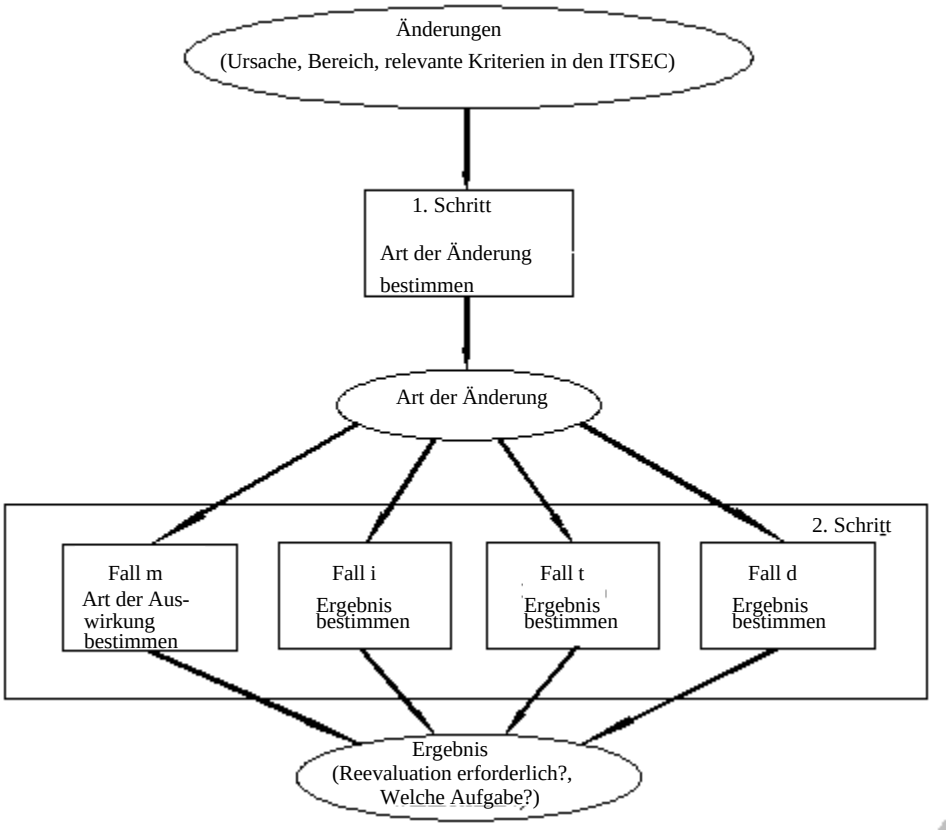


Abbildung 6.D.1 Überblick über den Prozeß der Auswirkungsanalyse

6.D.16 Die folgende Abbildung zeigt mögliche Ursachen und Auswirkungen einer Änderung eines EVG. Die Abbildung ist in vier Spalten unterteilt: die Ursache der Änderung, der Bereich, auf den sich die Änderung bezieht, die relevanten Kriterien in den ITSEC, auf die sich die Änderung bezieht, und die resultierende *Art der Änderung.*

6.D.17 Die Art der Änderung ist einem von vier möglichen Werten zuzuordnen:

m: eine Änderung, die letztendlich zu einer *Modifikation* des EVG führt;

i: eine Änderung, die sich nur *indirekt* auf den EVG auswirkt;

d: eine Änderung der *Dokumentation*, die Konsequenzen für den Betrieb des EVG mit sich bringen kann;

t: eine Änderung eines bei der Entwicklung verwendeten *Werkzeugs.*

Ursache	Bereich	Relevante Kriterien in den ITSEC		Art der Änderung
Neue Bedrohung hinzugekommen Neue sicherheitsspezifische Funktion hinzugekommen Geänderte Bewertung der Stärke der Mechanismen	Sicherheits-vorgaben	Phase 1 - Anforderungen Phase 2 - Architekturentwurf Phase 3 - Feinentwurf Phase 4 - Implementierung	und/oder und/oder und/oder	m m m m
Ausnutzbare Schwachstelle gefunden	Wirksamkeit	Phase 1 - Anforderungen Phase 2 - Architekturentwurf Phase 3 - Feinentwurf Phase 4 - Implementierung	und/oder und/oder und/oder	m m m m
Änderung des Entwicklungsprozesses	Korrektheit	Phase 1 - Anforderungen Phase 2 - Architekturentwurf Phase 3 - Feinentwurf Phase 4 - Implementierung	und/oder und/oder und/oder	m m m m
Änderung der Entwicklungsumgebung		Aspekt 1 - Konfigurationskontrolle Aspekt 2 - Prog.sprachen und Compiler Aspekt 3 - Sicherheit beim Entwickler		i t i
Änderung der Betriebsdokumentation		Aspekt 1 - Benutzerdokumentation Aspekt 2 - Systemverwalter-Dokum.		d d
Änderung der Betriebsumgebung		Aspekt 1 - Auslieferung und Konfiguration Aspekt 2 - Anlauf und Betrieb		d d

Abbildung 6.D.2 Arten von Änderungen bei einem EVG

Schritt 2 (Ergebnis ermitteln)

6.D.18 Mit diesem Schritt wird das Ergebnis ermittelt, d.h. festgestellt, ob eine Reevaluation erforderlich ist und welche Aufgaben durchzuführen sind. Es werden vier Fälle unterschieden, die je nach Art der Änderung Anwendung finden.

6.D.19 In diesem Abschnitt wird angenommen, daß die Komponententypen unverändert sind. Dies trifft nicht immer zu. So können bei einer bestimmten Reevaluation beispielsweise aus einigen Komponenten, die zuvor *sicherheitsrelevant* waren, *sicherheitsspezifische* Komponenten werden und umgekehrt. Wenn eine Änderung in der Architektur vorliegt, kann sich darüber hinaus die Trennung in sicherheits-spezifische, sicherheitsrelevante und nicht sicherheitsrelevante Komponenten ändern.

Fall m (Ergebnis für Änderung vom Typ "m" ermitteln)

6.D.20 Die Änderungsart m wird in vier weitere *Arten der Änderung auf unterer Ebene* unterteilt, die wie folgt definiert sind:

m0: Es kommt zu einer Änderung der Sicherheitsvorgaben.

m1: Es kommt zu einer Änderung auf der Ebene des Architekturentwurfs, die keinen Einfluß auf die Sicherheitsvorgaben hat.

m2: Es kommt zu einer isolierten Änderung auf Feinentwurfsebene. Diese Änderung ist auf der Ebene des Architekturentwurfs nicht sichtbar, so daß keine Aktualisierung der Dokumentation auf dieser Ebene erforderlich ist.

m3: Es kommt zu einer isolierten Änderung auf der Implementierungsebene. Diese Änderung ist auf Feinentwurfsebene nicht sichtbar, so daß keine Aktualisierung der Dokumentation auf dieser Ebene erforderlich ist.

6.D.21 Die folgenden zusätzlichen Beschränkungen bringen Konsequenzen für die Arten der Änderung auf unterer Ebene mit sich. Wenn für m2 oder m3 eine Änderung nicht als 'isoliert' identifiziert werden kann, weil sie sich z.B. über mehrere Basiskomponenten erstreckt, gilt die nächsthöhere Art der Änderung. Eine Änderung auf der Implementierungsebene (m3), die nicht die Eigenschaft 'isoliert' aufweist, entspricht daher einer Änderung vom Typ m2. Dieselbe Regel gilt für Änderungen vom Typ m2, die im entsprechenden Fall Änderungen vom Typ m1 werden. Der Nachweis, daß eine Änderung zum Typ m0, m1, m2 oder m3 gehört, ist vom Antragsteller/Entwickler zu erbringen.

6.D.22 Die Auswirkungsart der Änderungen wird anhand der entsprechenden Tabelle für die angestrebte Evaluationsstufe in Abbildung 6.D.3 bestimmt. Jede der fünf definierten Auswirkungsarten führt zu einem anderen Ergebnis.

6.D.23 Für diesen Fall müssen die folgenden Punkte als Eingangsdaten bekannt sein:

a) die vom EVG erreichte Evaluationsstufe;

b) die Art der Änderung auf unterer Ebene (m0 bis m3);

c) der Komponententyp (SE, SR oder SI, siehe 6.D.11) der geänderten Komponente(n).

6.D.24 Das anhand der Tabelle ermittelte Ergebnis ergibt die Art der Auswirkung der jeweiligen Änderung. Die Auswirkungsart gibt Aufschluß über die vom Antragsteller/Entwickler und von der ITSEF durchzuführenden Aufgaben.

Arten der Auswirkung

6.D.25 Bei den Tabellenangaben in Abbildung 6.D.3 wird zwischen fünf möglichen Werten (den Auswirkungsarten I1 - I5) unterschieden, aus denen die Konsequenzen einer Änderung des evaluierten EVG zu ersehen sind. Es ist zu beachten, daß sich nach genauerer Analyse eine abweichende Auswirkungsart ergeben kann. Die Auswirkungsarten sind in der Abbildung 6.D.4 zusammengefaßt.

Evaluationsstufe	Art der Änderung auf unterer Ebene
Komponententyp	Auswirkungsart

E1	m0	m1	m2	m3
SE	I5	I4	I2	I2
SR	I5	I3	I2	I2
SI	X	I1	I1	I1

E2	m0	m1	m2	m3
SE	I5	I4	I3	I2
SR	I5	I3	I3	I2
SI	X	I1	I1	I1

E3	m0	m1	m2	m3
SE	I5	I4	I4	I3
SR	I5	I4	I3	I3
SI	X	I1	I1	I1

E4	m0	m1	m2	m3
SE	I5	I5	I5	I4
SR	I5	I4	I3	I3
SI	X	I1	I1	I1

E5	m0	m1	m2	m3
SE	I5	I5	I5	I4
SR	I5	I5	I4	I3
SI	X	I1	I1	I1

E6	m0	m1	m2	m3
SE	I5	I5	I5	I5
SR	I5	I5	I5	I4
SI	X	I1	I1	I1

"X" kennzeichnet eine nicht mögliche Kombination

Abbildung 6.D.3 Auswirkungsarten für E1 bis E6

Abbildung 6.D.4 Zusammenfassung der Auswirkungsarten	
Auswirkungsart	Durchzuführende Aufgaben
I1	Zertifizierungsstelle informieren
I2	I1 + der Zertifizierungsstelle Testdokumentation zur Verfügung stellen
I3	Evaluationsbeiträge für die ITSEFs bereitstellen, ITSEF prüft Evaluationsbeiträge auf Inhalt, Form und Nachweis
I4	I3 + ITSEF führt alle ITSEC-Evaluatoraufgaben durch
I5	Komplette Reevaluation

Auswirkungsart I1

6.D.26 Änderungen, die zu Auswirkungen vom Typ I1 führen, sind nicht sicherheitsrelevant und erfordern keine Maßnahmen, es sei denn, eine derartige Änderung hat Konsequenzen für die Abfassung des Evaluationsergebnisses und des Zertifikats/Zertifizierungsreports. Dessenungeachtet soll der Antrag-steller/Entwickler im Zweifelsfall die Zertifizierungsstelle informieren.

Auswirkungsart I2

6.D.27 Die Zertifizierungsstelle wird über die Änderung informiert, da sich Auswirkungen auf die Durchsetzung der Sicherheitspolitik ergeben können. Der Zertifizierungsstelle werden Prüfdokumente zusammen mit einer der jeweiligen Evaluationsstufe entsprechenden Änderungsanzeige zugeschickt.

Auswirkungsart I3

6.D.28 Die Zertifizierungsstelle wird über die Änderung informiert, da Änderungen dieser Art auch Auswirkungen auf die Durchsetzung der Sicherheitspolitik haben können. Die der Änderungsanzeige beigefügten Informationen müssen den Anforderungen bezüglich Inhalt, Form und Nachweis der jeweiligen Evaluationsstufe und den relevanten Phasen oder Aspekten entsprechen. Von der ITSEF wird überprüft, ob die bereitgestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis sowohl für die Wirksamkeit als auch für die Korrektheit erfüllen. Der Nachweis der Wirksamkeit ist für Änderungen vom Typ m2 in der Tabelle für E2 sowie für Änderungen vom Typ m3 in der Tabelle für E3 nicht erforderlich (da sie für die ursprüngliche Evaluation nicht gefordert werden).

Auswirkungsart I4

6.D.29 Änderungen mit Auswirkungen vom Typ I4 betreffen mit großer Wahrscheinlichkeit die Durchsetzung der Sicherheitspolitik. Es gelten dieselben Regeln wie für I3, jedoch reichen die gemäß I3 bereitgestellten Informationen nicht aus, um nachzuweisen, daß die Evaluationsstufe nach den durchgeführten Überprüfungen weiterhin Gültigkeit hat. Die in den Evaluatoraufgaben der ITSEC im Hinblick auf die entsprechende Evaluationsstufe und Phase festgelegten Aktivitäten müssen von der ITSEF sowohl für die Korrektheit als auch für die Wirksamkeit durchgeführt werden. Sollte bei dieser Aktivität ein Korrektheitsfehler oder eine ausnutzbare Schwachstelle ermittelt werden, ändert sich die Auswirkungsart in I5.

Auswirkungsart I5

6.D.30 Änderungen mit Auswirkungen vom Typ I5 sind stets sicherheitsrelevant. Die Zertifizierungsstelle wird von der Änderung in Kenntnis gesetzt. Die der Änderungsanzeige beigefügten Informationen müssen für eine zwischen Zertifizierungsstelle, ITSEF und Antragsteller anzuberaumende Besprechung ausreichen. Bei dieser Besprechung wird der erforderliche Umfang der Reevaluation erörtert. Ein Problem, das zu der vorgeschlagenen Änderung geführt hat, ist der Zertifizierungsstelle mitzuteilen. Die Mitteilung soll eine aktualisierte Liste der Schwachstellen enthalten.

Änderungsanzeigen

6.D.31 Die zusammen mit den Änderungsanzeigen zu liefernden Informationen sind von Fall zu Fall verschieden; für die Auswirkungsarten I1 bis I4 sind folgende Informationen erforderlich:

a) Nachweis, daß die Art der Änderung den Angaben entspricht;

b) Nachweis, daß der Komponententyp den Angaben entspricht;

c) Nachweis für die angestrebte neue Evaluationsstufe.

6.D.32 Beispielsweise besteht der Nachweis für Punkt c) aus den relevanten Evaluationsbeiträgen mit den ausgewiesenen Änderungen sowie einer Erklärung, warum die Kriterien 'isoliert' und 'auf der nächsten Entwurfsstufe nicht sichtbar' erfüllt sind.

Fall i (Ergebnis für Änderung vom Typ "i" ermitteln)

6.D.33 Bei dieser Art der Änderung ist mit Blick auf die angestrebte Evaluationsstufe zu überprüfen, ob die Anforderungen nach der Änderung weiterhin Gültigkeit haben.

Fall d (Ergebnis für Änderung vom Typ "d" ermitteln)

6.D.34 Es ist zu überprüfen, ob die Änderungen in der Dokumentation Einfluß auf die Kriterien für *Korrektheit - Betrieb, Benutzerfreundlichkeit* oder *operationelle Schwachstellen* haben könnten. Sind diese nicht betroffen, sind auch keine weiteren Maßnahmen erforderlich. Wenn diese Kriterien betroffen sind, müssen sie erneut angewandt werden.

Fall t (Ergebnis für Änderung vom Typ "t" ermitteln)

6.D.35 Bei dieser Art der Änderung bleibt das Evaluationsergebnis für eine angestrebte Evaluationsstufe bis E2 gültig. Bei einer angestrebten Evaluationsstufe ab E3 muß hinsichtlich der Kriterien *Program-miersprachen und Compiler* überprüft werden, ob die Änderung an sich den Grad des in den EVG gesetzten Vertrauens ungültig machen kann.

Der Reevaluationsprozeß

6.D.36 Nachdem die Entscheidung über die Notwendigkeit einer Reevaluation und die geforderten Aufgaben getroffen worden ist, wird die eigentliche Reevaluation durchgeführt.

6.D.37 Da die Evaluationsstufe ein Maß für das in einen EVG zu setzende Vertrauen auf Erfüllung seiner Sicherheitsziele ist, muß eine Reevaluation mit derselben Strenge durchgeführt werden wie die ursprüngliche Evaluation oder sogar mit einem höheren Maß an Strenge, wenn die angestrebte Evaluationsstufe der Reevaluation höher liegt. Andernfalls kann der Grad des Vertrauens nicht aufrechterhalten werden.

6.D.38 Man beachte, daß sich seit der Erstevaluation (beispielsweise aufgrund von Mängelberichten) Verbesserungen ergeben haben können. Diese Änderungen könnten Auswirkungen auf den Arbeitsumfang haben, den die Evaluatoren für diese oder künftige Reevaluationen für notwendig erachten.

Anhang 6.E Hinweise für Werkzeuganbieter: Erstellen einer Evaluations-Arbeitsoberfläche

Einleitung

6.E.1 In diesem Anhang werden verschiedene Konzepte für die Spezifikation und Konstruktion einer Evaluations-Arbeitsoberfläche beschrieben. Werkzeuganbieter oder -Hersteller sollten diese Konzepte bei der Erstellung eigener Evaluationswerkzeuge berücksichtigen.

6.E.2 Die Grundideen stammen aus dem Bereich der Software-Entwicklung. Mit der rechnergestützten Software-Entwicklung (Computer Aided Software Engineering, CASE) stehen den Entwicklern eine ganze Reihe von Werkzeugen zur Implementierung von Methoden zur Verfügung, die für die Spezifikation, den Entwurf, die Programmierung, das Testen und die Validierung von Software eingesetzt werden. Eine integrierte Projektunterstützungsumgebung (Integrated Project Support Environment – IPSE) ist eine Software-Plattform, auf der ein Entwickler alle Werkzeuge ablegen kann, die er zur Abdeckung des kompletten Entwicklungszyklus benötigt. Durch Einfügen dieser Werkzeuge wird aus der IPSE eine bestückte IPSE (Populated IPSE, PIPSE). Eine auf einer PIPSE aufbauende Arbeitsoberfläche kann Entwicklungsmethodik (z. B. Organisation) und ein ganzes Spektrum an Verwaltungswerkzeuge für die Erzeugung von Qualitätssoftware umfassen.

6.E.3 In diesem Anhang sollen diese Prinzipien auf die Erstellung einer Evaluations-Arbeitsoberfläche angewandt werden, die den Evaluatoren Werkzeuge zur effizienten Durchführung ihrer Arbeit und zur gesicherten Einhaltung der in Teil 3 des ITSEM beschriebenen Evaluationsprinzipien zur Verfügung stellt. Die größte Herausforderung bleibt die Vielfalt der im Rahmen der ITSEC durchführbaren Evaluationen und die Schwierigkeit, gemeinsame Lösungen zur Abdeckung des gesamten IT-Bereichs zu finden. Dies müßte durch die immer weiter zunehmende Tendenz zur Standardisierung und Offenheit in diesem Bereich zu lösen sein.

6.E.4 Dieser Anhang ist deshalb darauf ausgerichtet,

a) die Grundkonzepte für den Aufbau einer Evaluations-PIPSE vorzustellen, um zu zeigen, daß eine enge Verbindung zwischen Techniken und Werkzeugen (Beschreibung in Teil 4, Kapitel 4.5) für die Durchführung von Evaluationen Vorteile mit sich bringt;

b) die typischen Merkmale aufzuführen, die von den auf der Arbeitsoberfläche des Evaluators befindlichen Werkzeugen zu erwarten sind; es wird hier nicht versucht, auf die spezifischen Werkzeuge und Techniken einzugehen, die bei der Entwicklung von Systemen eingesetzt werden. Es steht eindeutig fest, daß die Evaluations-Arbeitsoberfläche um so kostengünstiger ist, je mehr Gemeinsamkeiten es zwischen Entwicklungswerkzeugen und Evaluationswerk-zeugen gibt;

c) zusätzliche Informationen zu Werkzeugkategorien zu liefern, bei denen die vom Evaluator zu treffende Wahl schwierig ist; der Inhalt des betreffenden Abschnitts wird sich wohl gemein-sam mit der Informationstechnik fortentwickeln.

Eine PIPSE für die Evaluations-Arbeitsoberfläche

Konzept

6.E.5 Es ist von Vorteil, wenn die in Teil 4, Kapitel 4.5 beschriebenen Techniken und Werkzeuge bei der Unterstützung des gesamten Evaluationsprozesses zusammenarbeiten. Um dies zu erreichen, können sie innerhalb einer IPSE organisiert werden. Die IPSE bietet eine Infrastruktur (definierte Formate für den Datenaustausch, eine gemeinsam genutzte Evaluationsdatenbank, gemeinsame Dienstleistungen für Textverarbeitung, Bearbeitung und Anzeige von Ergebnissen usw.), innerhalb derer die einzelnen Werkzeuge integriert werden können.

6.E.6 Die PIPSE befaßt sich mit den zentralen Problemen der Produktivität, Dauer und Qualität einer Evaluation.

6.E.7 Im Einklang mit internationalen und europäischen Standards und Verfahren wie etwa [ECMA] ist es außerdem wichtig, ein offenes Systemkonzept (Open Systems) anzustreben und bei der Evaluation von einer Open IPSE oder Open PIPSE zu sprechen. Und schließlich ist es auch hilfreich, Hardware-CAD oder andere EVG-spezifische Werkzeuge einzubeziehen.

Nutzvorteile

6.E.8 Die Vorteile einer PIPSE bestehen darin, daß sie die folgenden Aufgaben vereinfacht:

a) Projektmanagement bei einer Evaluation: die Abschätzung des Kosten- und Zeitrahmens, die Projektplanung für die Evaluation, die Zeitplanung für die Evaluationsaktivitäten usw.;

b) Konfigurationsmanagement für die Evaluation: die Evaluationsaktivitäten sollen im Rahmen eines Konfigurationsmanagements durchgeführt werden (besonders wichtig bei der Behebung der während der Evaluation festgestellten Fehler sowie bei einer Reevaluation nach Änderung des EVG);

c) Erstellung und Verwaltung der Evaluationsdokumentation;

d) Werkzeuge für die Kommunikation zwischen PIPSE: es kann durchaus sinnvoll sein, Evaluatoren, die denselben EVG bearbeiten, zu vernetzen, wobei es sich, falls dies aus Sicherheitsgründen möglich ist, auch um zwei oder mehr ITSEFs handeln kann;

e) die Erstellung einer Evaluationsdatenbank: beim Erfassen und Speichern der firmeneigenen Informationen von Herstellern ist Sorgfalt geboten;

f) andere zugehörige Dienstleistungen: z. B. Online-Hilfe.

6.E.9 Vorteilhaft für die PIPSE ist auch die Einbindung neuer Werkzeuge, die eine Automatisierung des Evaluationsvorgangs ermöglichen.

Architektur

6.E.10 Abbildung 6.E.1 zeigt eine mögliche allgemeine Schichtenarchitektur, die für die Entwicklung der Evaluations-PIPSE verwendet werden kann. Die Architektur umfaßt

a) ein Betriebssystem, das einige grundlegende Sicherheitsmechanismen zum Schutz der evaluierten firmeneigenen Informationen (z. B. Quellcode) und der während des Evaluations-prozesses erzeugten Informationen anbietet;

b) eine Schicht mit gemeinsamen Dienstleistungen, die Unterstützung für eine integrierte Software-Entwicklungsumgebung bieten (unter Umständen gemeinsam mit der Entwicklungsumgebung für den EVG) und als Grundlage für die Integration von Werkzeugen dienen wie etwa [PCTE];

c) ein Software-Grundgerüst, das die Homogenität der Methoden und Werkzeuge sowie gegebenenfalls der Evaluationsregeln gewährleistet;

d) eine horizontale Umgebung, die grundlegende Managementdienstleistungen bereitstellt wie etwa dokumentationsspezifische Editier- und Managementfunktionen, ein Konfigurationsmanagementtool, Projektmanagement, elektronische Post; diese horizontale Umgebung kann auch die für die Evaluation erforderlichen Entwicklerwerkzeuge aufnehmen (Compiler, Bibliotheken);

e) eine vertikale Umgebung, in die die verschiedenen Evaluationswerkzeuge (wie in Teil 4, Kapitel 4.5 beschrieben) eingefügt werden;

f) eine anwenderfreundliche Mensch-Maschine-Schnittstelle.

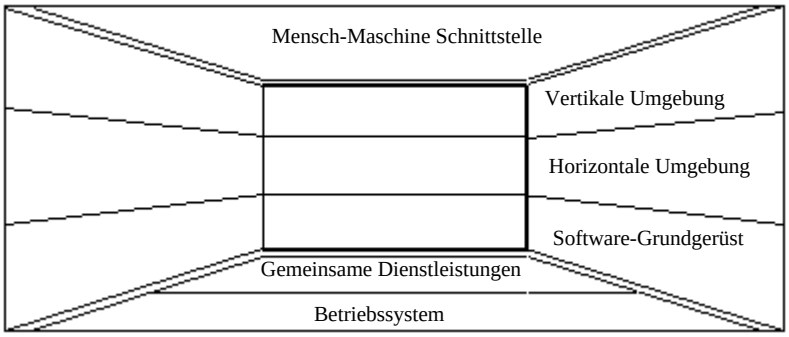


Abbildung 6.E.1 Mögliche PIPSE-Architektur

Checklisten

6.E.11 Es muß gewährleistet werden, daß die ITSEFs während der Anwendung der einzelnen Kriterien in den ITSEC sämtliche relevanten Fakten berücksichtigen. Die ITSEC bieten keine Allzweck-Checkliste an, da die spezifischen Evaluatoraufgaben von der Art des EVG und den Sicherheitsanforderungen bestimmt werden, die in seinen Sicherheitsvorgaben definiert sind.

6.E.12 Die Arbeitsoberfläche kann bei der Generierung und Validierung konsistenter Checklisten innerhalb verschiedener Evaluationen mithelfen, so daß bei einer Evaluation desselben EVG durch zwei ITSEFs anhand derselben Sicherheitsvorgaben die gleichen Checklisten erzeugt würden.

Bestückung einer Evaluations-Arbeitsoberfläche

Allgemeines

6.E.13 Dieser Abschnitt beschreibt die erwünschten Leistungsmerkmale von Evaluationswerkzeugen. Er befaßt sich hauptsächlich mit den Eigenschaften der Werkzeuge, die zur Verwirklichung der Prinzipien ***Wiederholbarkeit***, ***Reproduzierbarkeit*** und ***Objektivität*** beitragen.

Technische Eignung der Werkzeuge

6.E.14 Die technische Eignung eines Werkzeugs kommt in seiner Anwendungsbreite und dem Grad der erzielten Unverfälschtheit zum Ausdruck.

6.E.15 *Anwendungsbreite*: Für die Generierung von Werkzeugen für die Evaluationsaktivitäten gibt es zwei mögliche Methoden. Bei der ersten wird versucht, möglichst universelle Werkzeuge zu erzeugen; bei der zweiten wird versucht, einen Satz spezialisierter Werkzeuge zu erzeugen.

6.E.16 Diese spezialisierten Werkzeuge haben den Nachteil, daß sie nur eingeschränkt anwendbar und nicht flexibel genug sind. Daher kann es sich als schwierig erweisen, sie wirksam einzusetzen. Mit zunehmender Standardisierung der Informationstechnik und zunehmend besserer Definition der Aufgaben des Evaluators wird sich der Anwendungsbereich solcher Spezialwerkzeuge immer weiter ausdehnen.

6.E.17 Die Möglichkeit einer Kombination von Werkzeugen ist insbesondere für die Evaluation in den Bereichen wichtig, in denen kein geeignetes Einzelwerkzeug zur Verfügung steht. Die Organisation der PIPSE gestattet eine effiziente, flexible Kombination.

6.E.18 *Grad der Formalisierung*: Auf den höheren Evaluationsstufen müssen die Werkzeuge in der Lage sein, die von den ITSEC geforderten semiformalen und formalen Methoden zu unterstützen. Die Eigenschaften der Werkzeuge können wie folgt charakterisiert werden:

a) die Eingabesprachen weisen eine genau definierte Syntax und Semantik auf;

b) es existiert eine mathematische Theorie oder ein formales Modell, das die Gültigkeit der erzeugten Ergebnisse gewährleistet.

Einfaches Erlernen und Anwenden der Werkzeuge

6.E.19 Die zugrundeliegende Technik, auf der das Werkzeug aufbaut, soll einfach zu erlernen und anzuwenden sein, damit Mißverständnisse und falsche Schlußfolgerungen ausgeschlossen werden können. Dies bedeutet nicht, daß die Technik selbst einfach sein muß. Selbst dann, wenn die Techniken komplex sind oder ihnen eine komplexe Theorie zugrundeliegt, sollen die Evaluatoren in der Lage sein, das Werkzeug wirksam einzusetzen. Hier ist Schulung ein wichtiger Aspekt.

6.E.20 *Einfaches Erlernen* ist eine Grundanforderung. Selbst wenn die zu automatisierende Aufgabe komplex ist, soll ein Werkzeug die Erzielung brauchbarer Resultate ermöglichen. Folgende Faktoren beeinflussen ein einfaches Erlernen:

a) die Qualität und Relevanz der Dokumentation (einschließlich Fehlermeldungen und Online-Hilfe);

b) die Qualität der Schulungen;

c) die Gestaltung der Mensch-Maschine-Schnittstelle;

d) die Einhaltung von Standards.

6.E.21 Die Dokumentation soll vollständig sein und Hinweise und Beispiele enthalten, die für die Evaluation von Nutzen sind.

6.E.22 *Einfache Vorbereitung der Eingabe* ist wünschenswert, damit das Werkzeug auf Änderungen im Format von Eingaben möglichst flexibel reagieren kann.

6.E.23 *Einfache Interaktion* verbessert die Leistungsfähigkeit der Evaluatoren. Durch Berücksichtigung folgender Punkte kann die Interaktion unterstützt und somit die Eignung des Werkzeugs verbessert werden:

a) Bildschirmanzeige;

b) Befehlsstruktur (d. h. Menüs, Eingabeaufforderungen) und möglichst sinnvolle Benennung.

Anforderungen an die Ausgaben für Werkzeuge

6.E.24 *Eignung der Ausgabe*: Die Eignung eines Werkzeugs wird durch die Relevanz und Klarheit seiner Ausgabe verbessert. Die Einfachheit der Interpretation einer Werkzeugausgabe wird von den gleichen Faktoren beeinflußt, die die Einfachheit der Eingabevorbereitung und der Interaktion beeinflussen. Die Klarheit der Ausgabe kann erhebliche Auswirkungen auf den Gebrauchswert des Werkzeugs haben.

6.E.25 Unabhängig von der Art der Ausgaben sollen diese gut dargestellt sein. Die Gesamtergebnisse sollen in einer überschaubaren Form geliefert werden und präzise Schlußfolgerungen darstellen.

6.E.26 Die Anforderungen an die Ausgabe werden unter den folgenden Überschriften behandelt: *Aufzeichnung der Evaluatoraktivitäten, positive Ergebnisse* und *Gültigkeit der Ergebnisse.*

6.E.27 *Aufzeichnung der Evaluatoraktivitäten*: Die Forderung nach Aufzeichnung der Evaluatoraktivitäten ist besonders wichtig, wenn interaktive Werkzeuge verwendet werden. Es muß eine Möglichkeit zur wiederholten Verwendung des Werkzeugs gegeben sein, damit ein Ergebnis anderen Evaluatoren oder Dritten vorgeführt werden kann. Eine Möglichkeit, dies zu erreichen, ist die Aufzeichnung aller eingegebenen Befehlssequenzen, so daß diese entweder von Hand erneut eingegeben oder aber vorzugsweise automatisch abgerufen werden können (hierbei kann es sich um einen standardisierten Mechanismus der Arbeitsoberfläche selbst handeln). Eine ausführliche Aufzeichnung der Evaluator-aktivitäten ist einer der Hauptvorteile der Automatisierung des Evaluationsprozesses.

6.E.28 *Positive Ergebnisse*: Wenn die Ausgabe des Werkzeugs eine Aussage darüber enthält, ob das betreffende Ergebnis richtig ist, bedeutet dies einen deutlichen Vorteil gegenüber einem Werkzeug, das lediglich keinen negativen Hinweis ausgibt.

6.E.29 *Fehlen negativer Ergebnisse*: Es ist wichtig, daß bei einem für die Suche nach bestimmten unerwünschten Eigenschaften ausgelegten Werkzeug deren Fehlen leicht festzustellen ist. Das Fehlen negativer Ergebnisse liefert einen Nachweis für den Evaluationsprozeß, auch wenn es nicht das Nichtvorhandensein von Schwachstellen garantiert, jedoch ist dies bei unklarer Ausgabe nicht leicht zu erkennen.

6.E.30 *Gültigkeit der Ergebnisse*: Die Werkzeugausgabe soll vertrauenswürdig sein; wenn der Nachweis von einem formalen Werkzeug stammt, kann diese Vertrauenswürdigkeit im Sinne von Zuverlässigkeit angegeben werden. Das heißt, wenn das Werkzeug nur 'wahre' Ergebnisse nachweisen kann, ist ihm größeres Vertrauen entgegenzubringen, als wenn es auch 'falsche' nachweisen kann.

Kommerzielle Verwendbarkeit von Werkzeugen

6.E.31 Schließlich ist anzustreben, daß nur Werkzeuge verwendet werden, die aus kommerzieller Sicht günstige Eigenschaften aufweisen; dazu gehören Portabilität, Wartung und Weiterentwicklung.

6.E.32 *Portabilität*: Die Portabilität eines Werkzeugs bezieht sich darauf, ob das Werkzeug für verschiedene Betriebssysteme und Hardwaretypen verfügbar ist. Bei der Evaluation ist Portabilität aufgrund der Vielzahl der bearbeiteten Betriebssysteme ein wesentlicher Vorteil. Allerdings muß die Frage "Wird ein Port ein identisches Werkzeug erzeugen?" sorgfältig geprüft werden.

6.E.33 *Wartungsfreundlichkeit*: Es ist wichtig, daß das Werkzeug einsatzbereit bleibt, wenn das Betriebssystem, unter dem es läuft, aufgerüstet wird. Dies ist eigentlich eine Forderung an den Werkzeuganbieter, die Wartung des Werkzeugs fortzusetzen.

6.E.34 *Weiterentwicklung*: Werkzeuge entwickeln sich mit den Techniken, die sie implementieren. Es können zwar erweiterte Funktionen hinzukommen, jedoch darf aus Gründen der Wiederholbarkeit die Änderung eines Werkzeugs nicht die Anwendbarkeit der zuvor mit diesem Werkzeug erzielten Resultate verändern.

Anhang 6.F Modell einer Zusammenfügung und Anwendungsbeispiel

Zweck

6.F.1 Dieser Anhang richtet sich an Antragsteller, Systemintegrierer und Systemakkreditierer, die mit der Zusammensetzung früher evaluierter EVG befaßt sind.

6.F.2 Der Zweck dieses Anhangs besteht darin,

a) ein Modell für das Zusammenfügen früher evaluierter EVG zu beschreiben;

b) die Anwendung des Modells anhand von Beispielen zu beschreiben.

6.F.3 Aufgrund der Komplexität des allgemeinen Sachverhalts kann nur ein vereinfachtes Modell beschrieben werden. Weitere Hinweise zu dieser Frage sind bei den Zertifizierungsstellen zu erfragen.

Zusammenfassung

6.F.4 Dieser Anhang beginnt mit der Beschreibung eines einfachen Modells einer Komponente und zeigt anschließend, wie sich das Modell zur Beschreibung des Zusammenfügens von zwei zuvor evaluierten Komponenten verwenden läßt.

6.F.5 Da eine ganze Reihe von Möglichkeiten für das Zusammenfügen gegeben sind, werden zwei Fälle dargelegt, aus denen die relevanten Eigenschaften der Zusammenfügung hervorgehen.

6.F.6 Die praktischen Erfahrungen mit dem Zusammenfügen evaluierter Produkte sind gering.

Das Modell für das Zusammenfügen

6.F.7 Im Zusammenhang mit dem Zusammenfügen dient der Begriff *Komponente* in diesem Anhang zur Bezeichnung einer bereits früher evaluierten Komponente, die bei der Konstruktion eines EVG verwendet wurde. Die Verwendung dieses Begriffs entspricht der Definition in den ITSEC (d.h., eine Komponente ist ein identifizierbarer und in sich geschlossener Teil eines EVG), da das Ergebnis des Zusammenfügens wiederum ein EVG ist.

6.F.8 Eine Komponente wird als "white box" bezeichnet (hierdurch wird angedeutet, daß ihr Inneres bis zu einem gewissen Grad - je nach Evaluationsstufe - bekannt ist), im Gegensatz zu einer "black box", deren Inneres nicht bekannt ist.

6.F.9 Eine Komponente wird im Modell beschrieben durch:

a) eine Prädikatenmenge P, die sie unterstützt;

b) eine Schnittstelle, die Dienstleistungen an die Betriebsumgebung liefert, in der sich die Komponente befindet, sowie eine Schnittstelle zur Bereitstellung von Dienstleistungen für die Komponente;

c) Annahmen über die Betriebsumgebung, in der sich die Komponente befindet;

d) ihre internen Details.

6.F.10 Die Prädikatenmenge steht in direktem Zusammenhang mit der Funktionalität der Komponente. Diese Funktionalität kann entweder sicherheitsspezifisch sein (sie bezieht sich auf die Sicherheitsvorgaben) oder sicherheitsrelevant (d. h., sie dient zur Unterstützung einer sicherheitsspezifischen Funktion). Die Prädikatenmenge kann sich zwischen einer kompletten Sicherheitspolitik und einem Einzelprädikat bewegen, das eine notwendige Eigenschaft einer Komponente beschreibt.

6.F.11 Die von der Schnittstelle bereitgestellten Dienstleistungen sollen entweder von einer anderen Komponente genutzt oder einem Anwender zur Verfügung gestellt werden. Diese Schnittstelle kann als Schnittstelle des Herstellers bezeichnet werden. Der Detaillierungsgrad der Schnittstellenbeschreibungen und der Beschreibungen der von ihr bereitgestellten Dienstleistungen hängt von der Evaluationsstufe ab.

6.F.12 Es gibt zwei mögliche Arten von Annahmen über die Umgebung:

a) Die eine Teilmenge könnte notwendige externe Nicht-IT-Dienstleistungen beschreiben, von denen der sichere Betrieb der Komponente abhängt (korrekter Betrieb beinhaltet Korrektheit und Wirksamkeit im Sinne der ITSEC).

b) Die andere Teilmenge könnte notwendige externe IT-Dienstleistungen beschreiben, von denen der sichere Betrieb der Komponente abhängt. Für diese IT-Dienstleistungen muß eine Schnittstellenbeschreibung sowie eine Beschreibung der zu erwartenden Dienstleistungen vorhanden sein. Diese Schnittstelle kann als Schnittstelle des Anwenders der Komponente bezeichnet werden.

6.F.13 Beliebige willkürliche Kombinationen von Annahmen sind möglich. Zum Beispiel kann ein Datenbank-Managementsystem ausschließlich IT-bezogene Annahmen hinsichtlich der Bereitstellung von Dienstleistungen durch ein zugrundeliegendes Betriebssystem treffen. Das zugrundeliegende Betriebssystem hingegen kann Nicht-IT-Annahmen hinsichtlich der physischen Sicherheitsumgebung treffen, in der es arbeitet.

6.F.14 Die internen Details werden mit einer von der Evaluationsstufe abhängigen Genauigkeit beschrieben. Die internen Details bilden eine Quelle für Schwachstellen.

6.F.15 Abbildung 6.F.1 enthält die bildliche Darstellung einer Komponente.

6.F.16 Anhand der obigen Definition des Modells einer Komponente kann eine Kombination von Komponenten beschrieben werden. Zur Vereinfachung wird in der folgenden Darstellung davon ausgegangen, daß die Menge der Annahmen über Nicht-IT-Dienstleistungen leer ist.

Kombination von Komponenten – Fall 1

6.F.17 Komponente C1 nutzt Dienstleistungen, die von Komponente C2 erzeugt werden. Von Komponente C1 wird eine von außen sichtbare Schnittstelle bereitgestellt. C2 verfügt über eine Herstellerschnittstelle zu Komponente C1, doch diese Schnittstelle ist für einen Anwender nicht sichtbar.

6.F.18 Beispiel für Fall 1:

a) Komponente C1 – Kunde;

b) Komponente C2 – Server.

6.F.19 In Abbildung 6.F.2 ist Fall 1 bildlich dargestellt. Der auf Komponente C2 weisende Pfeil zwischen den beiden Komponenten soll andeuten, daß C2 von C1 genutzt wird.

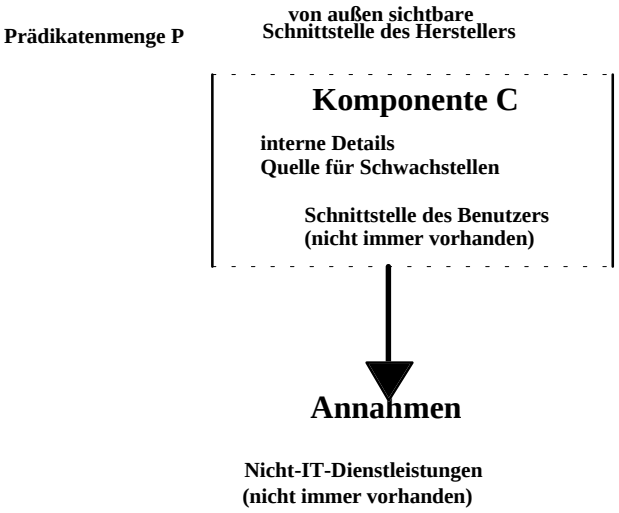


Abbildung 6.F.1 Eine EVG-Komponente

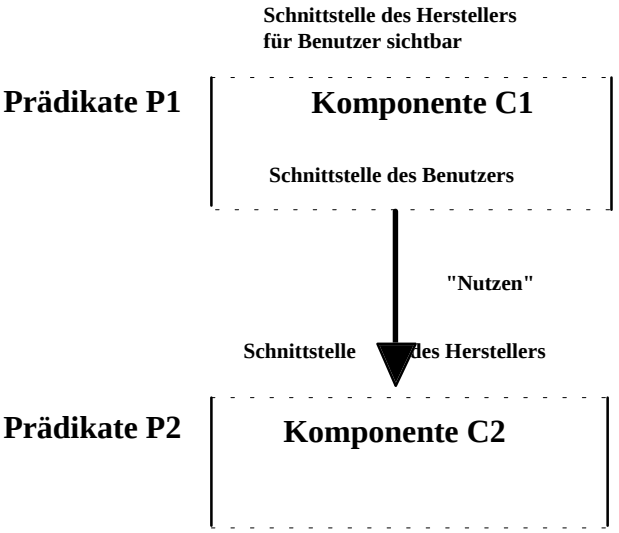


Abbildung 6.F.2 Kombination von Komponenten; Fall 1

Kombination von Komponenten – Fall 2

6.F.20 Komponente C1 nutzt Dienstleistungen, die von Komponente C2 erzeugt werden. Eine von außen sichtbare Schnittstelle wird von Komponente C1 und C2 bereitgestellt.

6.F.21 Beispiel für Fall 2:

a) Komponente C1 – Monitor für virtuelle Maschine (Virtual Machine Monitor, VMM);

b) Komponente C2 – Hardware-Plattform.

6.F.22 Die sichtbare Schnittstelle wird von der VMM-Schnittstelle und den Maschinenbefehlen der Hardware-Plattform bereitgestellt.

6.F.23 In Abbildung 6.F.3 ist Fall 2 bildlich dargestellt.

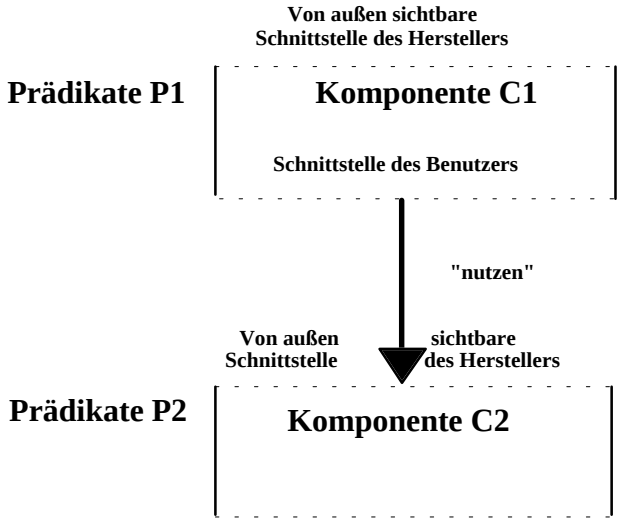


Abbildung 6.F.3 Kombination von Komponenten; Fall 2

Kombination von Komponenten – Fall 3

6.F.24 Komponente C1 nutzt von Komponente C2 erzeugte Dienstleistungen und Komponente C2 von C1 erzeugte Dienstleistungen. Eine von außen sichtbare Schnittstelle wird von Komponente C1 und Komponente C2 bereitgestellt.

6.F.25 In Abbildung 6.F.4 ist Fall 3 bildlich dargestellt.

Durch Anwendung des Modells entstehende Zusammenfügungen

6.F.26 Bei allen Kombinationen wird die entstehende Komponente als C3 bezeichnet. Sie besitzt ihre eigene Prädikatenmenge P3 und alle sonstigen Merkmale einer Komponente wie Schnittstelle des Herstellers, interne Details, usw. .

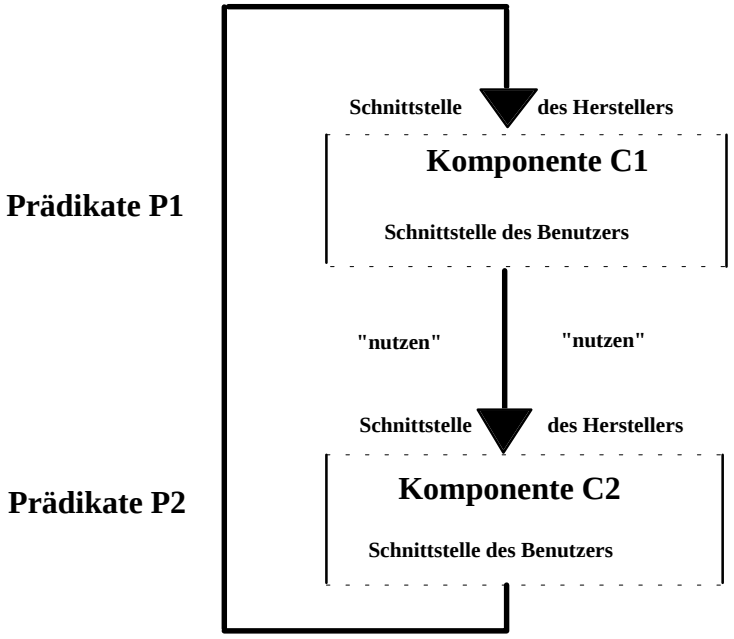


Abbildung 6.F.4 Kombination von Komponenten; Fall 3

6.F.27 Wenn die Kombination beispielsweise Fall 1 entspricht, müssen die folgenden Bedingungen wahr sein, damit Komponente C3 ihre Prädikate P3 beibehält:

Bedingung 1: C1 muß korrekt implementiert sein.

Bedingung 2: C2 muß korrekt implementiert sein.

Bedingung 3: Die Anwenderschnittstelle von C1 muß mit der Herstellerschnittstelle von C2 genau übereinstimmen.

Bedingung 4: Die Kombination der Prädikate P1 und P2 ergibt die Prädikate P3. Dies bedeutet, daß P3 aus P1 und P2 abgeleitet ist.

Bedingung 5: Die Prädikate P2 müssen trotz etwaiger Schwachstellen in C2 erhalten bleiben. Das heißt, es muß nachgewiesen werden, daß die Schwachstellen in C2 hinsichtlich der Prädikate P2 nicht ausnutzbar sind.

Bedingung 6: Die Prädikate P1 müssen trotz etwaiger Schwachstellen in C1 erhalten bleiben. Das heißt, es muß nachgewiesen werden, daß die Schwachstellen in C1 hinsichtlich der Prädikate P1 nicht ausnutzbar sind.

Bedingung 7: Es muß nachgewiesen werden, daß Schwachstellen in C2 hinsichtlich der Prädikate P1 nicht ausnutzbar sind.

Bedingung 8: Die Nutzungsbeziehung besteht tatsächlich nur von Komponente C1 zu Komponente C2 (einseitig gerichtet).

6.F.28 Nachfolgend werden mögliche Probleme in diesem Szenarium aufgeführt:

a) Das Vertrauen in die Wahrheit von Bedingung 1 unterscheidet sich von dem Vertrauen in die Wahrheit von Bedingung 2. Dies ist dann der Fall, wenn Komponente C1 auf einer anderen Evaluationsstufe bewertet wird als Komponente C2.

b) Bedingung 3 ist nicht wahr. Mögliche Ursachen sind:

– Die Anwenderschnittstelle von C1 ist eine Teilmenge der Herstellerschnittstelle von C2;

– die Anwenderschnittstelle von C1 ist eine Obermenge der Herstellerschnittstelle von C2;

– der Detaillierungsgrad der Schnittstellenbeschreibungen für die Anwenderschnittstelle (C1) und die Herstellerschnittstelle (C2) ist unterschiedlich.

c) Wie kann nachgewiesen werden, daß die Prädikate P1 und P2 zusammen P3 bilden, wenn P1 und P2 eine beliebige Prädikatenmenge sein können?

d) Das Vertrauen in die Richtigkeit von Bedingung 5 unterscheidet sich von dem Vertrauen in die Richtigkeit von Bedingung 6. Dies ist auch der Fall, wenn die Komponenten C1 und C2 auf verschiedenen Stufen evaluiert werden.

e) Es muß auf der spezifizierten Evaluationsstufe nachgewiesen werden, daß die Nutzungsbeziehung wie vorgesehen einseitig ist.

6.F.29 Sind die Darstellungen von Einheiten unterschiedlich detailliert, was in der Regel der Fall ist, wenn sie auf unterschiedlichen Abstraktionsstufen angesiedelt sind, läßt sich eine Transformation finden, so daß die Prädikate von Komponente C1 und Komponente C2 zumindest auf dieselben Einheiten verweisen. Die hierbei erzeugten Prädikate P1’ können nun dahingehend untersucht werden, ob sie gemeinsam mit P2 die Prädikate P3 der Kombination bilden. Widersprüche zwischen den beiden Prädikatenmengen müssen unbedingt offengelegt werden.

6.F.30 Da die Prädikate P1 und P2 willkürlich gewählt sind, gibt es keine allgemeingültigen Regeln, ob und wie die Prädikate P1 und P2 die Prädikate P3 bilden.

Leerseite

Index

Begriffe aus dem ITSEC-Glossar sind mit ○ gekennzeichnet:

Leerseite

Europäische Gemeinschaften - Kommission

Handbuch für die Bewertung der Sicherheit von Systemen

der Informationstechnik (ITSEM)

Luxemburg: Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften

1994 — VIII, 262 S. — 21,0 x 29,7 cm

ISBN 92-826-7087-2