erschienen in *Computer und Recht* 9. Jg., Heft 3 (März 1993), S. 170 – 179

Staatliche Initiativen und Dokumente zur IT-Sicherheit – eine kritische Würdigung

Andreas Pfitzmann, Kai Rannenberg
Universität Hildesheim, TU Berlin
Tel.+49-5121-883-735, +49-30-314-73499

Die Vielfalt der in ihrer Qualität und praktischen Brauchbarkeit durchweg umstrittenen staatlichen Initiativen und Dokumente zur IT-Sicherheit verwirrt inzwischen auch einen aufmerksamen Beobachter.

Der vorliegende Basisbeitrag wendet sich bewußt an den Nichtfachmann, also den Leser, der keine vertieften Kenntnisse der IT-Sicherheit besitzt. Die Abhandlung stellt alle wesentlichen Dokumente und Initiativen vor, charakterisiert Inhalte und Ziele und benennt die wesentlichen Schwachstellen. Sie gelangt zu dem Schluß, daß die Wirtschaftskraft und sogar die Demokratie gefährdet werden, wenn Evaluation, Zertifizierung und Akkreditierung weiterhin so unvollkommen stattfinden wie bisher. (Red.)

I. Grundlagenwerke zur IT-Sicherheit

Entsprechend den Vorgaben des IT-Sicherheitsrahmenkonzeptes[1] sind in den letzen Jahren in Deutschland drei sogenannte „Grundlagenwerke der IT-Sicherheit“[2] entstanden, denen teilweise auch international erschienene Dokumente entsprechen und die zur Steigerung der IT-Sicherheit in der Bundesrepublik Deutschland beitragen sollen[3]:

(1) Ein IT-Sicherheitshandbuch soll die sichere Anwendung der Informationstechnik unterstützen.

(2) IT-Sicherheitsevaluationskriterien sollen als Grundlage für die Bewertung (Evaluation) der Sicherheit von Systemen der Informationstechnik dienen.

(3) Evaluationshandbücher sollen Ziele und Prozeß der Evaluation sowie die Anforderungen der Evaluationskriterien für Hersteller, Prüfer und Anwender verdeutlichen.

In diesem Beitrag werden die Dokumente und ihre Bezüge zueinander sowie die daran geäußerte, teilweise heftige Kritik und die Beziehungen zu den im Zusammenhang wichtigsten internationalen Entwicklungen vorgestellt und bewertet. Begonnen wird mit dem IT-Sicherheitshandbuch (II). Eine Betrachtung der Sicherheitsevaluierung bei der Informationstechnik schließt sich an (III), bestehend aus einer Darstellung der gesetzlichen Grundlagen und organisatorischen Zusammenhänge (III.2), einer teilweise vergleichenden Vorstellung von Evaluationskriterien (III.3) und Evaluationshandbüchern (III.4) sowie einer Präsentation und Bewertung von

Dr. Andreas Pfitzmann, Diplom-Informatiker, ist wiss. Mitarbeiter und Lehrbeauftragter am Institut für Informatik der Universität Hildesheim. Er forscht und lehrt über technischen Datenschutz sowie damit verträgliche Verfahren zur Fehlertoleranz und Betrugssicherheit in digitalen Kommunikationssystemen.
Kai Rannenberg, Diplom-Informatiker, ist wiss. Mitarbeiter und Lehrbeauftragter am Institut für Angewandte Informatik der Technischen Universität Berlin. Er forscht und lehrt u.a. zum Thema Datenschutz und Datensicherheit, besonders bei offenen und öffentlichen Kommunikationssystemen. Ab April 1993 arbeitet er in der Abteilung Telematik des Instituts für Informatik und Gesellschaft der Universität Freiburg.
Die Autoren danken Dr. Michael Waidner (Universität Karlsruhe) für Kritik an einer früheren Textversion.
17.04.1996

Evaluationserfahrungen (III.5). Abschließend werden einige Empfehlungen und Anregungen zur Gewährleistung einer verfassungsverträglichen IT-Sicherheit gegeben (IV)[4].

II. Das IT-Sicherheitshandbuch

1. Struktur und Inhalt

Bundesbehörden sind gemäß IT-Sicherheitsrahmenkonzept[5] verpflichtet, vor der Beschaffung von IT-Systemen ein Sicherheitskonzept zu erarbeiten. Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* hat die Aufgabe, Behörden auf Anforderung dabei zu unterstützen. Diese Arbeit soll das IT-Sicherheitshandbuch begleiten[6], das vor kurzem in einer ersten Fassung für den Behördenbereich erschienen ist[7]. Es ist in 6 Hauptteile gegliedert:

(1) Eine vierseitige Kurzinformation „IT-Sicherheit – Eine Aufgabe für Führungskräfte“ für die Leitung von Firmen, Behörden und Institutionen soll verdeutlichen, daß IT-Sicherheit eine Aufgabe für Führungskräfte ist.

(2) Eine allgemeine Einführung für interessierte Leser beschreibt den Adressatenkreis und die Aufgaben und Grenzen des Handbuches sowie die Bedrohungen, denen IT-Systeme ausgesetzt sind.

(3) Eine praktische Anleitung zur Untersuchung und Gewährleistung der IT-Sicherheit stellt ein 4stufiges Verfahren zur Bedrohungs- und Risikoanalyse sowie zur Erstellung eines Sicherheitskonzeptes vor. Zum Thema Auswahl von IT-Systemen wird auf die Bedeutung der IT-Sicherheitskriterien bzw. der ITSEC (vgl. III.3) hingewiesen und erläutert, wie sich Evaluationsergebnisse im Rahmen des Sicherheitskonzeptes nutzen lassen. Ein eigenes Kapitel ist der „Sicherheit beim Einsatz von Arbeitsplatzcomputern“ gewidmet. Kapitel über „Grenzen beim Einsatz von Sicherheitsmechanismen“ und „Standardfehler“, letzteres insbesondere zur Unterstützung der Risikoanalyse, schließen diesen Teil ab.

(4) Ein Grundschutz soll mit Hilfe von Leitlinien und Fragenkatalogen für die jeweils für IT-Sicherheit Verantwortlichen gewährleistet werden.

(5) Die Anhänge 1-13 bieten Hilfsmittel und Durchführungshinweise zum Verfahren, wie es in Teil 3 des Handbuches vorgestellt wird.

(6) Die Anhänge A-H enthalten Hintergrundinformationen und Hilfen vor allem zum Verständnis der allgemeinen Einführung.

2. Kritik am vierten Entwurf

Der vierte Entwurf des IT-Sicherheitshandbuchs[8] hat scharfe Kritik ausgelöst, die unter dem Titel „IT-Sicherheitshandbuch – ein Rückfall“ teilweise im Jahresbericht des *Berliner Datenschutzbeauftragten* für das Jahr 1991 veröffentlicht ist[9]. Einige Kritikpunkte lauten:

„Viele Abschnitte können weder inhaltlich noch nach der Ausdrucksweise und Darstellung den üblichen fachlichen Ansprüchen standhalten. Die Methode zur Analyse der Risiken und zur Entwicklung von IT-Sicherheitskonzepten krankt u.a. an folgenden Mängeln.

- Das Verfahren verzichtet auf eine ganzheitliche Betrachtung der Organisationen, die sich der Informationstechnik bedienen, um ihre Leistungen zu erbringen. Damit werden Ursachen wie Mängel übergeordneter Organisationsstrukturen, Interessengegensätze,

Führungsmängel und mangelhafte Planung der Informationsflüsse aus der Risikoanalyse ausgeblendet.

- Die Risikobewertung und -ermittlung erfolgt an einer pauschalisierenden numerischen Wertskala, die mit ihrer Pseudomathematik Objektivität und Unangreifbarkeit vortäuscht, jedoch nicht nachvollziehbar ist und bei Risiken, die mehr ideeller Natur sind (z.B die Wahrung des informationellen Selbstbestimmungsrechtes), ungeeignet ist.
- Die Wahrung der informationellen Selbstbestimmung und die Beachtung bestimmter besonderer gesetzlicher Rahmenbedingungen, die den Wert einer Anwendung beeinflussen, werden zwar pauschal erwähnt, bei dem Verfahren zur Ermittlung der Schutzbedürftigkeit jedoch nicht beachtet.
- Ein Konzept für die Aktualisierung und Fortschreibung der Ergebnisse der Risikoanalyse und des IT-Sicherheitskonzeptes wird nicht mitgeliefert. Die organisatorische Installation eines Sicherheitsmanagements wird nicht explizit unterstützt.
- Der zeitliche und personelle Aufwand für die Anwendung des Sicherheitshandbuches verletzt bei kleineren IT-Anwendungen die Grundsätze der Verhältnismäßigkeit und Wirtschaftlichkeit. Gerade angesichts der Änderungshäufigkeit bei Hard- und Softwarekomponenten ist zu erwarten, daß die Analysen von sicherheitsrelevanten Änderungen der Konfigurationen überholt werden.

Eine Befassung mit den Details des Entwurfs des IT-Sicherheitshandbuches, z.B. bei den Anforderungen an sichere Anwendungen im PC-Bereich oder bei Mehrplatzsystemen zeigt bald, daß die längst veröffentlichten und größtenteils auch akzeptierten Anforderungen der Datenschutzbeauftragten und auch anderer Fachleute bei weitem nicht erreicht werden.

Angesichts der uns bekannt gewordenen Absicht, trotz der warnenden Stellungnahmen das IT-Sicherheitshandbuch zumindest erprobungshalber für eine bestimmte Frist für die Bundesverwaltung verbindlich zu machen, warnen wir davor, daß sich die *Berliner Landesverwaltung* einer solchen Vorgehensweise bei der Erstellung von Sicherheitskonzepten anschließt, solange das Handbuch nicht wesentlich verbessert wird."

Weitere Kritik wird beispielsweise von *Reinhard Voßbein*, geäußert, der die Vorgehensweise des *BSI* mit den Worten kommentiert: „Dies ist der Sache wenig dienlich, wenn ein an sich begrüßenswertes Vorhaben sich selbst durch fragwürdige Qualität diskreditiert."[10]

Alle zitierten Kritikpunkte gelten auch für die inzwischen geltende Version 1.0 des Sicherheitshandbuchs.

III. Sicherheitsevaluation bei der Informationstechnik

1. Ziele

Die Komplexität informationstechnischer Systeme (kurz: IT-Systeme) macht bereits seit mehreren Jahrzehnten eine Beurteilung ihrer Sicherheit durch einfache „Draufschau" unmöglich. Gleichzeitig haben die für Beschaffung und Betrieb von IT-Systemen Verantwortlichen nur selten die Zeit und Kompetenz, die Aussagen von Herstellern bezüglich der Sicherheit der angebotenen Systeme und der Angemessenheit für die jeweilige Aufgabe und Einsatzumgebung zu beurteilen. Sicherheitsevaluation soll deshalb zunächst zweierlei erreichen:

(1) Bewertungen sollen durch eine herstellerunabhängige Instanz vorgenommen werden.

(2) Sicherheitseigenschaften von IT-Systemen und Sicherheitsanforderungen von Anwendungen sollen strukturiert und gegebenenfalls hierarchisiert werden. Eine Gegenüberstellung von Anforderungen und Eigenschaften soll die Auswahl eines IT-Systemes erleichtern. („Für diese Anwendung ist E2-Sicherheit nötig, also können wir unter allen Angeboten auswählen, die wenigstens E2 erreicht haben.“)

Die gesetzlichen Grundlagen für die Sicherheitsevaluation in Deutschland wurden im wesentlichen durch das BSI-Gesetz geschaffen und werden in III.2 vorgestellt. Fachliche Grundlage für die Evaluationen sind Kriterienkataloge, wie sie in III.3 beschrieben und verglichen werden. Evaluationshandbücher (vgl. III.4) sollen den an der Evaluation Beteiligten das Verständnis der Kriterien und des Evaluationsprozesses erleichtern. Über mittlerweile in Deutschland und Europa bekanntgewordene Evaluationserfahrungen wird in III.5 berichtet.

2. Evaluation, Zertifizierung, Akkreditierung und ihre gesetzlichen Grundlagen

a) Regelung gemäß ITSEC und ITSEM

Evaluation, Zertifizierung und Akkreditierung sollen die drei Schritte zum sicheren Einsatz von IT-Systemen sein. In den ITSEC (vgl. III.3.c) findet sich ihre Definition und gegenseitige Abgrenzung, die weitgehend auf die gesetzlichen Grundlagen der beteiligten EG-Mitgliedsstaaten abgestimmt ist. In Deutschland ist dies vor allem der § 4 des am 17.12.1990 beschlossenen Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz)[11], in dem ein „Sicherheitszertifikat“ beschrieben wird.

Evaluation wird im Glossar der ITSEC als „die Bewertung eines IT-Systems oder -Produkts anhand definierter Evaluationskriterien“ erklärt[12].

Zertifizierung ist „die Abgabe einer formalen Erklärung, die die Ergebnisse einer Evaluation und die ordnungsgemäße Anwendung der benutzten Evaluationskriterien bestätigt“.

Akkreditierung kann zweierlei sein: zum einen „das Verfahren, welches ein IT-System zum Betrieb in einer speziellen Umgebung freigibt“, zum anderen „das Verfahren, welches für ein Prüflabor gleichzeitig die technische Kompetenz und die Unabhängigkeit, die zugehörigen Aufgaben durchzuführen, anerkennt.“

Ein IT-System muß also entsprechend den Definitionen der ITSEC bis zum Einsatz wenigstens drei „Phasen“ bei eventuell, aber nicht notwendigerweise verschiedenen „Stationen“ (beide Oberbegriffe finden sich nicht in den ITSEC) durchlaufen:

(1) Die Evaluation soll durch ein anerkannt „technisch kompetentes und unabhängiges Prüflabor“ erfolgen. Im ITSEM (vgl. III.4) werden diese Labors „Information Technology Security Evaluation Facilities“ (ITSEF) genannt.

(2) Die Zertifizierung soll durch eine „unabhängige und neutrale nationale Stelle“ vorgenommen werden. Gemäß ITSEM ist dies ein „Certification Body“ (CB).

(3) Schließlich gibt der Anwender das System im Rahmen der Akkreditierung zum Betrieb frei.

Die zweite Bedeutung von **Akkreditierung** weist auf die Beziehungen zwischen zwei der Stationen hin. Die technische Kompetenz und Unabhängigkeit eines Prüflabors muß anerkannt sein und infolgedessen anerkannt werden, schon weil nach Intention der ITSEC auch Evaluationsergebnisse europa- und nach Abschluß der entsprechenden Normungsbemühungen weltweit

anerkannt werden sollen. Darüber, wer diese Akkreditierung vornimmt, gibt das Glossar der ITSEC keine Auskunft. Bezüglich des Verhältnisses zwischen den drei Stationen haben die ITSEC auch keine normative Wirkung. Hier lohnt der Blick auf den vergleichsweise weit fortgeschrittenen Aufbau der Evaluationsorganisationen in Deutschland und Großbritannien.

b) Bundesrepublik Deutschland

In Deutschland wird das Verhältnis zwischen Zertifizierungs-, Akkreditierungs- und Evaluationsstellen derzeit durch das BSI-Errichtungsgesetz geregelt. Zertifizierungsstelle ist demgemäß das BSI, das auch selbst evaluieren darf. Das BSI-Errichtungsgesetz ermächtigt in § 5 (1) den *Bundesminister des Innern (BMI)*, „nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesminister für Wirtschaft durch Rechtsverordnung das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten" zu bestimmen. Diese Verordnung ist inzwischen erlassen. Darüberhinaus hat der *BMI* in einem Erlaß die Akkreditierung der gemäß § 4 (2) BSI-Errichtungsgesetz „sachverständigen Stellen" (der ITSEF gemäß ITSEM) geregelt. Gegenwärtig sind die Technischen Überwachungsvereine (TÜVs) in Essen, Köln und München sowie die Industrieanlagenbetriebsgesellschaft (IABG, München) akkreditiert. Diese Form der Akkreditierung wird beim *BSI* vorgenommen, das damit neben seinen sonstigen Aufgaben (u.a. der Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik zur Erfüllung von Aufgaben des Bundes) für die Evaluation und Zertifizierung von Systemen sowie die Akkreditierung von Prüflabors bzw. -stellen zuständig ist bzw. sein kann.

Die übermächtige Stellung des *BSI* im deutschen Zertifizierungs- und Akkreditierungssystem ist – beispielsweise im für IT-Sicherheit zuständigen Arbeitsausschuß des *Deutschen Instituts für Normung (DIN)* – deutlich zu spüren. Sie wäre noch stärker geworden, wenn das BSI das Sekretariat des entsprechenden internationalen Normungsgremiums der ISO/IEC (ISO/IEC JTC1/SC27 – „Security Techniques") übernommen hätte. Dies war vom *BSI* angestrebt, vom *DIN* jedoch letztendlich nicht zugelassen worden, um internationale Proteste, die sich national bereits andeuteten, zu vermeiden.

c) Großbritannien

In Großbritannien sind die verschiedenen Stellen organisatorisch stärker als in Deutschland voneinander getrennt beziehungsweise weitere Organisationen einbezogen[13]. In einem „Scheme Management Board" sind alle zuständigen Regierungsstellen unter dem Vorsitz des Wirtschaftsministeriums (*Department of Trade and Industry – DTI*) und der „*Communications-Electronics Security Group*" (*CESG*) vertreten. Dieses „Management Board" leitet den von *DTI* und *CESG* gemeinsam betriebenen „Certification Body" – der eben diesen Namen hat – an. Der „Certification Body" vergibt Zertifikate und lizenziert die Evaluationsstellen (Commercial Licensed Evaluation Facilities – CLEFs), ist also für Zertifizierung von Systemen und die Akkreditierung von Evaluationsstellen zuständig. Bei der Akkreditierung stützt er sich auf Bewertungen des „National Measurement Accreditation Service" (NAMAS), einer Einrichtung des „*National Physical Laboratory*" (*NPL*), das seinerseits eine Forschungseinrichtung des *DTI* ist.

d) Aufsicht durch Europäisches Parlament

Aufgrund der starken Stellung der Zertifizierungsstellen ist in Fachkreisen bereits gefordert worden, die Zertifizierungsstellen nicht nur durch die ihnen jeweils vorgesetzten Behörden beaufsichtigen zu lassen, sondern beispielsweise eine parlamentarische Kontrolle durch das Europäische Parlament einzuführen[14].

3. Evaluationskriterien

a) USA als Vorreiter

Erste Initiativen zu einer Sicherheitsevaluierung von IT-Systemen wurden in den 70er Jahren vom *Verteidigungsministerium* der USA unternommen. 1983 wurden die „Trusted Computer System Evaluation Criteria" (TCSEC[15], vgl. III.3.b), zum ersten Mal veröffentlicht. Seitdem werden in den USA Evaluierungen vorgenommen und bei vielen Beschaffungen der öffentlichen Hand vorausgesetzt. Das Vorbild der USA einerseits und die eher protektionistisch ausgerichtete Evaluierungspolitik der zuständigen amerikanischen Stelle andererseits veranlaßten in Kanada und mehreren Staaten Europas die Entwicklung eigener Evaluationskriterien. In III.3.c werden als Beispiel die „IT-Sicherheitskriterien" der *Zentralstelle für Sicherheit in der Informationstechnik (ZSI)* vorgestellt. Die aktuell europaweit harmonisierten Kriterien (ITSEC[16], vgl. III.3.d) dienen als wesentliche Grundlage für die internationale Normung (III.3.e), die nicht nur zu einheitlichen Kriterien, sondern auch zur gegenseitigen Anerkennung von Evaluationsergebnissen führen soll. Nicht zuletzt die internationalen Normungsaktivitäten gaben den Anlaß für ein Projekt zur Neuentwicklung von Sicherheitskriterien in den USA (III.3.f). Einen in vielem neuen Ansatz präsentieren die kanadischen Evaluationskriterien (III.3.g).

b) „Orange Book" (TCSEC)

Als erste Evaluationskriterien für die Sicherheit von IT-Systemen gelten die 1983 erstmals und 1985 nahezu unverändert veröffentlichten „Trusted Computer Security Evaluation Criteria" (TCSEC) des „*Department of Defense*" der USA; oft ist der aus ihrer Einbandfarbe abgeleitete Name „Orange Book" bekannter. Die beste Eigenschaft der TCSEC ist die Einfachheit ihrer Struktur. Sicherheitsanforderungen und -eigenschaften werden in 7 hierarchische „Level" von D aufsteigend bis A1 eingeordnet. Dieser Einfachheit steht allerdings eine erhebliche Beschränkung der allgemeinen Anwendbarkeit der TCSEC gegenüber, wie sich aus folgenden Gesichtspunkten ergibt:

(1) Technisch orientieren sich die TCSEC am Stand der Informationstechnik der 70er Jahre, die wesentlich von organisatorisch zentral angesiedelten Großrechenanlagen geprägt war. Infolgedessen eignen die TCSEC sich nicht für die Evaluierung vernetzter und dezentral angesiedelter Systeme, und auch die 1987 erschienene „Trusted Network Interpretation – Red Book"[17] machte eine angemessene Evaluierung nicht möglich[18,19].

(2) Die den TCSEC zugrundegelegte Sicherheitspolitik orientiert sich überwiegend an militärischen Führungsstrukturen und Geheimhaltungsbedürfnissen: Informationen haben „von unten nach oben" zu fließen und vor allem vertraulich zu bleiben, selbst wenn dies den Betriebsablauf erheblich kompliziert. Die im kommerziellen Bereich wichtige Forderung nach der Integrität von Daten oder Systemen, etwa daß Daten in Vertragsformulierungen sicher unmanipuliert bleiben, spielt in den TCSEC eine gegenüber Geheimhaltungsbestrebungen untergeordnete Rolle.

(3) Sicherheit wird stets nur als die Sicherheit eines schützenswerten Systembetreibers vor Angriffen von außen verstanden. Daß ein Teilnehmer eines Kommunikationssystemes Schutz vor dem Betreiber benötigt, liegt außerhalb des Fokus der TCSEC. Damit sind Anforderungen in der Bundesrepublik Deutschland, etwa das in Artikel 10 GG festgeschriebene Fernmeldegeheimnis, das auch für die Umstände der Kommunikation gilt (vgl. die jüngste Rechtsprechung des *Bundesverfassungsgerichtes*[20]), durch die TCSEC nicht abgedeckt.

(4) Zwischen Sicherheitsfunktionen, etwa der Protokollierung sicherheitsrelevanter Vorfälle, einerseits und dem Aufwand, der zur Qualitätssicherung der jeweils eingesetzten Mechanismen, etwa durch formale Verifikation oder ausgiebiges Testen, andererseits betrieben wird, wird in den TCSEC strukturell nicht unterschieden. Die Anforderungen für die verschiedenen „Level" sind infolgedessen eine eher bunte Mischung aus Funktionalitäten und Qualitätssicherungsmaßnahmen.

c) „IT-Sicherheitskriterien" der ZSI

1989 erschien in Deutschland die erste – und vermutlich auch letzte – Fassung der „IT-Sicherheitskriterien – Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT)"[21] (ZSIEC) der damaligen *Zentralstelle für Sicherheit in der Informationstechnik (ZSI)*, der Vorgängerbehörde des *BSI*[22]. Diese Kriterien unterscheiden zwischen Funktionalitäten und Qualitätssicherungsmaßnahmen. Entsprechend sind die zu erreichenden Zertifikate zweidimensional gegliedert: Ein System wird für eine von 10 Funktionsklassen auf einer von 8 Qualitätsstufen evaluiert und zertifiziert, so daß insgesamt 80 verschiedene Zertifikate möglich sind. Da in den ZSIEC schon strukturell zwischen Funktionalitäten und Qualitätssicherungsmaßnahmen unterschieden wird, gilt Punkt 4 der Kritik an den TCSEC hier nicht.

Fünf der 10 Funktionsklassen der ZSIEC wurden aus den TCSEC abgeleitet, indem die funktionalen Anteile der TCSEC-Level C1 bis B3 zu Funktionsklassen gemacht wurden (Die Level D und A1 wurden nicht berücksichtigt: D wird nur für Systeme vergeben, die die Evaluierungen gemäß TCSEC nicht bestehen; A1 entspricht funktional B3). Die für den kommerziellen Bereich wichtigen – und von der Industrie wiederholt nachgefragten[23] – Aspekte der Integrität von Daten werden in weiteren Funktionalitätsklassen (F6, F8, F10) berücksichtigt. Die Funktionalitätsklasse F7 soll Anforderungsbereiche abdecken, in denen besonders die Verfügbarkeit eines Rechnersystemes wichtig ist, etwa zur Steuerung von Flugzeugen in Echtzeit. Die Funktionalitätsklasse F9 ist für Systeme gedacht, die hohe Anforderungen an die Geheimhaltung von Daten bei der Datenübertragung verlangen, wobei besonders an Geräte zur Verschlüsselung von Nutzinformationen gedacht ist.

Die Funktionalitätsklassen spiegeln das in der Einleitung der ZSIEC beschriebene Verständnis von Sicherheit als Schutz von Vertraulichkeit, Integrität und Verfügbarkeit wider. Dieses Verständnis war 1989 nicht neu; es findet sich beispielsweise in einem 1983 erschienenen und seitdem viel zitierten Text der Autoren Voydock und Kent[24], allerdings ohne motiviert zu werden[25]. Seit Veröffentlichung der Kriterien und besonders seit Veröffentlichung der ersten Entwürfe des BSI-Errichtungsgesetzes sind in Deutschland immer wieder Diskussionen um die Angemessenheit dieses Verständnisses von Sicherheit aufgeflammt[26,27]. Sie richten sich im Kern gegen

- den Denkansatz, Sicherheit nur als die Sicherheit des Systembetreibers gegenüber Angriffen von außen zu betrachten, wie er aus den TCSEC übernommen wurde (Kritikpunkt 3 in III.3.b) und
- die gefährliche Tendenz, in Evaluationskriterien lediglich kritiklos den kommerziell bereits erreichten Stand der Technik zu dokumentieren und diesen damit für die Zukunft festzuschreiben und gegen Verbesserungen „abzusichern".

Zweifelsohne verdienen die ZSIEC genauso wie die TCSEC Kritik für die Beschränkung von Sicherheit auf Betreibersicherheit. Allerdings läßt sich diese Kritik kaum auf der Ebene der drei „Sicherheitsgrundbestandteile" „Vertraulichkeit", „Integrität" und „Verfügbarkeit" diskutieren, da die Begriffe selbst kaum weniger abstrakt sind als der Begriff der Sicherheit selbst. Außerdem spielen die Begriffe lediglich in der Einleitung der ZSIEC eine Rolle. Es werden aus Ihnen

keinesfalls die für Sicherheit notwendigen Funktionalitäten oder gar die 10 Funktionalitätsklassen abgeleitet. Das Sicherheitsverständnis der ZSIEC kommt eigentlich in den 8 „Grundfunktionen sicherer IT-Systeme“ zum Ausdruck. Sie lauten (vgl. auch Bild 1):

(1) Identifikation und Authentisierung

(2) Rechteverwaltung

(3) Rechteprüfung

(4) Beweissicherung

(5) Wiederaufbereitung

(6) Fehlerüberbrückung

(7) Gewährleistung der Funktionalität

(8) Übertragungssicherung

Das den ersten vier Grundfunktionen zugrundeliegende Konzept läßt sich vereinfacht wie folgt beschreiben: Sicherheit ist gegeben, wenn jeder nur das tun kann, was er soll. Dieses ist festgeschrieben, indem Subjekten (beispielsweise Menschen, aber auch von Menschengruppen gemeinsam benutzten Programmen) Rechte zugewiesen werden. Damit ein Rechnersystem weiß, welche Rechte es einem Benutzer zuzugestehen hat, muß dieser sich ihm gegenüber identifizieren und authentisieren (Grundfunktion 1). Die Rechte müssen im System verwaltet (Grundfunktion 2) und bei Inanspruchnahme geprüft werden (Grundfunktion 3). Sollte jemand versuchen, ihm zugestandene Rechte zu mißbrauchen oder anderweitig dem System zu schaden, soll eine Protokollierung aller sicherheitsrelevanten Vorfälle im System (Grundfunktion 4) die Suche nach dem Schuldigen erleichtern[28]. Insgesamt modellieren die ersten vier Grundfunktionen also ein ideales Rechteverwaltungssystem, wie es auch ohne Rechner existieren könnte.

Die Grundfunktionen 5 - 7 sollen einigen als besonders gefährlich eingeschätzten spezifischen Eigenschaften realer Rechnersysteme entgegenwirken. Die physikalischen Eigenschaften der in Rechnern verwendeten elektrischen oder magnetischen Speichermedien führen dazu, daß gespeicherte Daten nicht ohne besonderen Anstoß gelöscht werden. Werden Schreib-Lese-Speicher nach Abschluß einer Aufgabe wiederverwendet, was bei Massenspeichern (bisher vor allem durch magnetische Medien realisiert) oft vorkommt und beim Arbeitsspeicher eines Rechners (bisher vor allem durch integrierte Schaltkreise realisiert) im Regelfall unumgänglich ist, können die dort noch gespeicherten Daten vom neuen Nutzer gelesen werden, ohne daß seine Berechtigung hierfür geprüft wird. Aus diesem Grund soll die Grundfunktion 5 dafür sorgen, daß Subsysteme ohne Sicherheitsrisiken wiederverwendet werden können, beispielsweise indem Speichermedien mehrfach mit Zufallszahlen beschrieben werden. Die (nicht unbedingt überschneidungsfreien) Grundfunktionen 6 und 7 sollen der oft komplizierten Fehlererkennung in technischen Systemen, der Behebung der Fehler und der Aufrechterhaltung des Betriebes dienen.

Die Grundfunktion 8 „Übertragungssicherung“ ist weiter untergliedert, denn hier sind alle Sicherheitsfunktionen zusammengefaßt, die in vernetzten Systemen benötigt werden. Diese Gliederung in 6 Unterfunktionen wurde an die Sicherheitsarchitektur des ISO-OSI-Referenzmodells für offene Kommunikationssysteme[29] angelehnt.

Für die Grundfunktionen der ZSIEC gilt der Kritikpunkt 1 an den TCSEC: Die speziellen Probleme vernetzter Systeme sind in beiden Kriterien strukturell nicht bewältigt. Schon die unausgewogene Struktur der 8 Grundfunktionen, von denen nur eine, nämlich „Datenaustausch“ Unterfunktionen hat, ist ein Beleg dafür. Hinzu kommt, daß fünf der Unterfunktionen sich inhaltlich mit den ersten sieben Grundfunktionen überschneiden.

Wichtigster Kritikpunkt an den Grundfunktionen ist, daß sie lediglich die Strategie unterstützen, ein System und seine Betreiber durch die Sammlung möglichst vieler Daten, etwa mittels Identifizierung und Protokollierung zu schützen. Schutzbedürfnisse von Benutzern oder Gespeicherten, etwa Telekommunikationsteilnehmern oder Bankkunden, die Kommunikations- oder Konsumentenprofile fürchten, sind mit den aufgezählten Grundfunktionen nicht zu erfüllen. Entsprechend ist es unmöglich, mit solchen Grundfunktionen technische Systeme, die Teilnehmer- oder Kundenschutz realisieren[30], angemessen zu beschreiben, zu evaluieren oder zu zertifizieren.

d) ITSEC

Seit Mai 1990 werden im Rahmen der INFOSEC-Initiative der *Kommission der Europäischen Gemeinschaften* neue Evaluationskriterien diskutiert: die „Information Technology Security Evaluation Criteria (ITSEC)"[31], deren aktuelle Version 1.2 vom 28. Juni 1991 offiziell vom *BSI* (Bundesamt für Sicherheit in der Informationstechnik) ins Deutsche übersetzt wurde und in deutscher Fassung „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC)" heißt[32]. Die ITSEC sind ihrem Untertitel gemäß harmonisierte Kriterien der EG-Nationen Deutschland, Frankreich, Großbritannien und Niederlande, wobei der Einfluß der britischen und der deutschen Kriterien am stärksten erscheint. Die Version 1.2 der ITSEC ist vorerst bis 1993 gültig und hat in Deutschland die ZSIEC als Grundlage für Evaluationen abgelöst. 1993 sollen die ITSEC – jedenfalls nach dem erklärten Willen ihrer Herausgeber – auf der Basis von Evaluationserfahrungen und des Diskussionsstandes in der internationalen Normung in Richtung auf eine „stabile" Version 2.0 überarbeitet werden.

Die ITSEC sehen wie die ZSIEC eine Evaluierung und Zertifizierung bezüglich Funktionalitätsumfang und Qualitätssicherungsmaßnahmen[33] vor. Wie in den ZSIEC wird auch in den ITSEC „Sicherheit" als „die Kombination aus Vertraulichkeit, Integrität und Verfügbarkeit"[34] betrachtet, ohne daß dies direkte Konsequenzen für die Ableitung von Sicherheitsfunktionalität hätte. Anders als in den ZSIEC wird in den ITSEC ausdrücklich zwischen Systemen und Produkten unterschieden: Systeme haben einen zum Zeitpunkt der Evaluierung bekannten Zweck und eine spezifische Betriebsumgebung; bei Produkten, etwa Sicherheitssoftware für Personalcomputer, ist die Einsatzumgebung zum Zeitpunkt der Evaluierung unbekannt. Infolgedessen mußte ein neuer gemeinsamer Oberbegriff (Evaluationsgegenstand – EVG, engl. Target of Evaluation – TOE) gefunden werden. Im übrigen haben die ITSEC zwar die gleiche Grundstruktur wie die ZSIEC, sind jedoch in zwei wesentlichen Punkten allgemeiner und weniger verbindlich gefaßt:

(1) Die zu evaluierende Sicherheitsfunktionalität muß sich nicht mehr verbindlich an einer von zehn Funktionalitätsklassen orientieren. Wer ein System evaluieren und zertifizieren lassen möchte, kann selbst bestimmen, auf welche Funktionalität sich eine Prüfung beziehen soll. Die 10 Funktionsklassen der ZSIEC sind infolgedessen nur noch als Beispiele im Anhang der ITSEC enthalten.

(2) Den 8 „Grundfunktionen sicherer IT-Systeme" gemäß ZSIEC entsprechen in den ITSEC 8 „generische Oberbegriffe", die als Ordnungshilfe zur Spezifikation der jeweiligen sicherheitsspezifischen Funktionen empfohlen werden.

Die acht generischen Oberbegriffe der ITSEC (und ihre offiziellen Übersetzungen ins Deutsche) lauten:

(1) Identification and Authentication (Identifizierung und Authentisierung)

(2) Access Control (Zugriffskontrolle)

(3) Accountability (Beweissicherung)

(4) Audit (Protokollauswertung)

(5) Object Reuse (Wiederaufbereitung)

(6) Accuracy (Unverfälschtheit)

(7) Reliability of Service (Zuverlässigkeit der Dienstleistung)

(8) Data Exchange (Übertragungssicherung)

„Access Control“ faßt die Grundfunktionen „Rechteverwaltung“ und „Rechteprüfung“ zusammen, „Accountability“ und „Audit“ erbringen zusammen den Funktionsumfang der Grundfunktion „Beweissicherung“ (vgl. Bild 1).

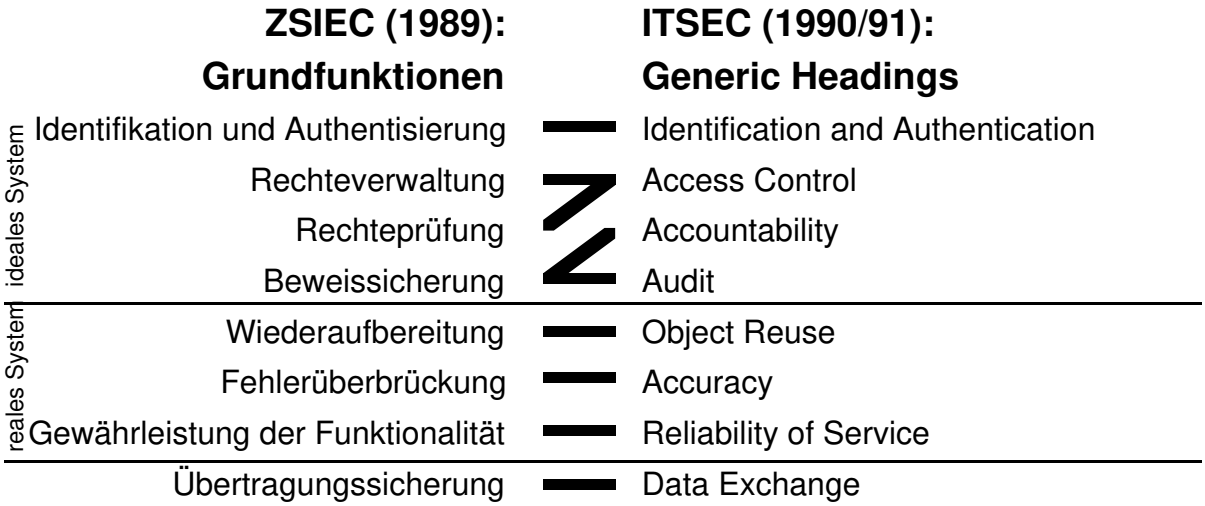

Bild 1: „Grundfunktionen sicherer IT-Systeme“ in den ZSIEC und ITSEC im Vergleich

Für die generischen Oberbegriffe der ITSEC gilt die gleiche Kritik wie für die Grundfunktionen der ZSIEC: Die ersten vier generischen Überschriften sind einseitig von der Idee geprägt, durch Sammlung von Daten den Systembetreiber vor Angriffen von außen zu schützen. Vorschläge, die Oberbegriffe neutraler zu formulieren, indem man den Begriffen Duale gegenüberstellte, so daß etwa der Begriff „Identifikation und Authentisierung“ durch die Duale „Anonymität und Pseudonymität“[35] ergänzt würde (Bild 2), wurden nicht aufgenommen. Auch der „Beweissicherung“ wurde nicht ihr Dual „Unbeobachtbarkeit“[36] gegenübergestellt, ebenso wie bei „Rechteverwaltung und -prüfung“ weiterhin keine „Pflichten“[37] erwähnt werden.

	Grundfunktionen	***Duale***
ideales System	Identifikation und Authentisierung	*Anonymität und Pseudonymität*
	Rechteverwaltung und -prüfung	*Pflichten*
	Beweissicherung	*Unbeobachtbarkeit*
reales System	Wiederaufbereitung	
	Fehlerüberbrückung	
	Gewährleistung der Funktionalität	
	Übertragungssicherung	

Bild 2: Grundfunktionen „sicherer" IT-Systeme und ihre Duale

Die bislang unbegründet gebliebene Starrheit der ITSEC-Autoren verblüfft, wenn man bedenkt, daß die generischen Oberbegriffe in den ITSEC eigentlich nur vorgeschlagen werden, und deutet darauf hin, daß den „generischen Oberbegriffen" mehr Bedeutung zugemessen wird, als die wortwörtliche Formulierung des entsprechenden Absatzes (2.31) nahelegt. Als Ansatz für einen Kompromiß wurde lediglich eine Passage in den (englischen) Text der Version 1.2 eingefügt, daß Sicherheitsziele auch durch Ausschluß (preclusion) der durch die Oberbegriffe repräsentierten Funktionalität erreicht werden könnten[38]. Diese Passage ist allerdings so unauffällig formuliert, daß sie bei der deutschen Übersetzung der Version 1.2 verloren ging. Diese Übersetzung lautet nämlich: „Es wird empfohlen, möglichst diese Oberbegriffe zu benutzen. Ihr Gebrauch wird den Vergleich mit anderen Sicherheitsvorgaben vereinfachen und die Feststellung erleichtern, ob sicherheitsspezifische Funktionen eines bestimmten Typs in speziellen Sicherheitsvorgaben enthalten sind."

Seitens des BSI, das die fehlerhafte Übersetzung zu verantworten hat, wurde zugesichert, durch eine Beilage auf den Fehler aufmerksam zu machen. Leider ist die Beilage nicht in jedem vom BSI versandten Exemplar der ITSEC enthalten, und inzwischen ist das BSI von seiner ursprünglichen Zusicherung abgerückt.

Daß die schweren Mängel der ITSEC Version 1.0 auch in der Version 1.2 im wesentlichen fortbestehen, ohne daß ihre Autoren während des Diskussionsprozesses eine wirkliche Begründung für ihre Entwurfsentscheidungen vorlegten, hat den Präsidiums-Arbeitskreis „Datenschutz und Datensicherung" der Gesellschaft für Informatik zu einer ausführlichen Stellungnahme veranlaßt[39], die noch weitere Kritikpunkte enthält.

e) Aktivitäten in der internationalen Normung

Im Oktober 1990, also etwa gleichzeitig mit der Diskusion der ITSEC V1.0, begann innerhalb der internationalen Normung (SC 27)[40] die Diskussion um „Evaluation Criteria for IT Security", und ein entsprechendes Normungsprojekt[41] wurde initiiert. Die entstehende Norm soll aus drei Teilen bestehen, einer Einleitung und je einem Teil zu den Themen Funktionalität (Functionality) und Qualitätssicherung (Assurance, offiziell übersetzt mit „Vertrauenswürdigkeit"). Die als erste Entwürfe für Teil 2 und 3 in den Normungsprozeß eingebrachten Dokumente stimmten fast wortwörtlich mit den entsprechenden Teilen der ITSEC überein und haben sich bisher nur redaktionell geändert.

Allerdings sind die Entwürfe bislang nicht über den Status eines „Working Draft"[42], der ersten von vier Stufen auf dem Weg zu einem ISO-Standard, hinausgekommen. Ein Grund dafür sind

die für März 1992 erwarteten, aber erst zur Herbstsitzung des SC27 in Gaithersburg (USA) vorgelegten Kommentare der US-amerikanischen Vertreter. Sie orientieren sich bereits an der Struktur der Entwürfe zu einer Überarbeitung der TCSEC, die im folgenden Abschnitt f) beschrieben werden, bleiben aber zumindest derzeit formal im Rahmen der bisherigen Struktur des Normprojektes.

Neben den USA haben auch andere Staaten modifizierende Kommentare eingereicht. Belgien hat die Ergänzung der „generischen Oberbegriffe" um „Anonymität" gefordert, Kanada ihre vollständige Umstrukturierung entsprechend der Struktur der kanadischen Kriterien (vgl. Abschnitt g). Die Kommentare aus Japan deuten an, daß auch dort IT-Sicherheitsevaluationskriterien entworfen werden, auch wenn über ihre Struktur bislang kaum Informationen vorliegen.

Als Ergebnis der Diskussion in Gaithersburg werden die „generischen Oberbegriffe" in Teil 2 (Funktionalität) voraussichtlich geändert; dabei werden auch „Unbeobachtbarkeit" und „Pseudonymität" – zumindest in der Form eines informativen Anhangs – enthalten sein. Funktionalitätsklassen wird der Teil 2 voraussichtlich nicht oder nur als Beispiele enthalten. Geplant ist derzeit, sie in einem internationalen Register zu verzeichnen; die Regelungen für eine Aufnahme in das Register sollen in einem neuen Normprojekt entwickelt werden.

Künftige Entwicklungen in der internationalen Normung werden vermutlich auch durch zwei gemeinsame Arbeitsgruppen zwischen kanadischen, US-amerikanischen und europäischen Experten zu den Themen „Funktionalität" (Functionality) und „Evaluationsmethoden" (Evaluation Methods) beeinflußt werden.

f) Das „Federal Criteria"-Projekt in den USA

1991 etablierte das „*National Institute of Standards and Technology*" (*NIST*) der USA zusammen mit der „*National Security Agency*" (*NSA*) das sogenannte „Federal Criteria Project" zur Entwicklung von „Federal Information Processing Standards" (FIPS) für die Entwicklung, Spezifikation und Evaluierung sicherer IT-Systeme (U.S. Information Security Standard, USISS). Erstes publiziertes Ergebnis des Projektes sind die „Minimum Security Requirements for Multi-User Operating Systems" (MSR), deren zweite Entwurfsfassung seit August 1992 veröffentlicht ist[43]. In ihnen werden die leicht um Anregungen aus dem kommerziellen Bereich erweiterten Anforderungen des TCSEC-Levels C2, das von mehreren Rechnerbetriebssystemen erreicht wurde und künftig als minimale Anforderung gelten soll, in eine Ordnung gemäß der generischen Überschriften der ITSEC gebracht, also Funktionalitäts- und Qualitätssicherungsanforderungen getrennt spezifiziert.

Die mit den MSR vorgelegte Neugliederung eines Teiles der TCSEC dokumentiert das Interesse der USA, internationalen Marktanforderungen gerecht zu werden und die Basis für eine gegenseitige Anerkennung von Evaluationsergebnissen zwischen den USA und der EG zu legen. Gleichzeitig liefern die MSR als vorweg veröffentlichtes Beispiel Hinweise auf die Struktur des neuen USISS. Erster Schwerpunkt bei der Entwicklung der USISS wird die Schaffung eines Rahmens zur strukturierten Formulierung von Sicherheitsanforderungen sein. „Schutz- " oder „Sicherheitsprofile" („Protection Profiles" bzw. „Security Profiles") sollen die gemeinsamen Anforderungen wichtiger Anwendungsbereiche beschreiben. Von den Funktionalitätsklassen der ZSIEC und ITSEC unterscheiden sich die „Protection Profiles" dahingehend, daß sie nicht nur Funktionalitäts-, sondern auch Qualitätssicherungsanforderungen enthalten.

Von den ITSEC übernommen wird das Prinzip, Funktionalitäts- und Qualitätssicherungsanforderungen zu trennen; die Trennung wird allerdings durch einen dritten Abschnitt über Abhängigkeiten („Dependencies") relativiert. Abhängigkeiten bestehen nach Ansicht der Autoren zwischen einzelnen Funktionalitäts- bzw. Qualitätsanforderungen sowie zwischen Funktionalitäts- und

Qualitätsanforderungen. Ob die Befürchtung mehrerer europäischer Experten zutrifft, die „Protection Profiles“ würden lediglich eine verfeinerte, aber ansonsten unveränderte Neudefinition der TCSEC-Level werden, muß die weitere Entwicklung zeigen.

Zu den langfristigen Zielen des „Federal Criteria“-Projektes gehört auch die Entwicklung von Kriterien, die den Anforderungen offener und verteilter IT-Systeme gerecht werden.

g) „Canadian Trusted Computer Product Evaluation Criteria“ (CTCPEC)

Die „Canadian Trusted Computer Product Evaluation Criteria“ (CTCPEC) sind in ihrer Version 3.0 am 30. April 1992 erschienen. Auch sie trennen Funktionalitäten sicherer IT-Systeme und Qualitätssicherungsmaßnahmen voneinander. Jedoch werden die Funktionalitäten neu gegliedert: Die Troika „Vertraulichkeit, Integrität, Verfügbarkeit“ wird um den vierten Aspekt „Zurechenbarkeit“ (Accountability) ergänzt, der damit gegenüber den ZSIEC oder ITSEC „eine Etage nach oben befördert“ worden ist. Den 4 Ordnungsmerkmalen auf höchster Ebene sind insgesamt 16 Funktionen jeweils einzeln zugeordnet, so daß die Struktur der CTCPEC einen deutlichen Fortschritt gegenüber der der ITSEC oder ZSIEC darstellt: Weder ITSEC noch ZSIEC enthalten eine Zuordnung zwischen den Ordnungsmerkmalen und den „generischen Oberbegriffen“ bzw. den „Grundfunktionen sicherer IT-Systeme“.

Der Schutz der Daten von Teilnehmern oder Benutzern ist – wie in den anderen Kriterienkatalogen auch – in den CTCPEC kaum berücksichtigt. Allerdings werden immerhin Bedrohungen durch den Systembetreiber an relativ prominenter Stelle, nämlich durch eine der 16 Funktionen („Separation of Duties“ bzw. „Aufteilung von Verantwortung“ innerhalb des Ordnungsmerkmals „Integrität“) behandelt. Wegen dieser relativen inhaltlichen Offenheit, der vergleichsweise guten Begründung von Entwurfsentscheidungen und ihrer Lesefreundlichkeit können die CTCPEC derzeit als die fortschrittlichsten Kriterien gelten.

4. Evaluationshandbücher

Zwei Evaluationshandbücher hatten bzw. haben in Deutschland Bedeutung:

(1) das IT-Evaluationshandbuch der ZSI[44]

(2) das Information Technology Security Evaluation Manual (ITSEM) in seiner aktuellen Entwurfsfassung V0.2[45]

Das IT-Evaluationshandbuch war das Handbuch für Evaluationen gemäß der ZSIEC. Das ITSEM ist als Handbuch für Evaluationen gemäß der ITSEC gedacht. Es ist wesentlich umfangreicher als das IT-Evaluationshandbuch und seit der Ablösung der ZSIEC durch die ITSEC auch wichtiger.

ITSEM gibt Erläuterungen zum Evaluationsprozeß, zur Idee und den Prinzipien der Evaluation gemäß ITSEC sowie zur Evaluationsmethode. Weiterhin enthält es Hinweise zu den seitens des Herstellers abzuliefernden Informationen, zum Inhalt der Evaluationsberichte und zu den während der Evaluation einzusetzenden Werkzeugen und Techniken. Schließlich werden Aspekte der Re-Evaluation und der Wiederverwendung von Evaluationsergebnissen behandelt.

Der Präsidiumsarbeitskreis „Datenschutz und Datensicherung“ der GI hat eine kritische Stellungnahme zum ITSEM verfaßt und diese aufgrund der Erfahrungen mit seiner ITSEC-Stellungnahme bereits veröffentlicht[46]. Kritisiert werden vor allem sieben Punkte. Vier rühren aus der nahen Verwandtschaft des ITSEM mit Version 1.2 der ITSEC her (vgl. III.2 c). Ein fünfter Punkt ist das ungeklärte Problem der Beaufsichtigung der Zertifizierungsstellen (vgl. III.1).

Als sechster Punkt wird die im ITSEM beschriebene Methode kritisiert, Bedrohungen und Maßnahmen aufzuzählen, um die Sicherheit eines IT-Systems zu dokumentieren: Im Bereich der Sicherheitstechnik werden sich nie alle Bedrohungen vollständig aufzählen lassen. Weit bessere Erfahrungen bestehen mit der Strategie, erst festzulegen, welche Teilsysteme eines komplexen Systemes wogegen als gesichert angenommen werden, und dann daraus Annahmen über die Sicherheit des Gesamtsystems herzuleiten.

Ein siebter Kritikpunkt sind die unzureichenden Anforderungen an Werkzeuge und Techniken in den ITSEM. Werkzeuge, insbesondere Software-Werkzeuge, können ihrerseits Sicherheitsrisiken, etwa Entwurfsfehler oder Trojanische Pferde[47], enthalten. Werden solche Werkzeuge zum Entwurf und besonders zur Prüfung von IT-Systemen eingesetzt, sind Evaluationsergebnisse wenig aussagefähig. Mindestens zur Erlangung höherer Evaluationsstufen sollte eine genaue Prüfung der Evaluations- und Entwurfswerkzeuge vorausgesetzt werden.

Die Version 0.2 des ITSEM wurde im September 1992 auf einem Workshop der *Direktion XIII D* der EG-Kommission kontrovers diskutiert. Welchen Einfluß dies auf die nächste Version (vermutlich 1.0) des ITSEM haben wird, ist noch unklar.

5. Evaluationserfahrungen

Seit 1983 wurden in den USA 16 Produkte evaluiert; 30 Produkte befinden sich in der Evaluierung[48]. Nach Aussagen des BSI[49] wurden bis zum zweiten Quartal 1992 drei Produkte gemäß der ZSIEC evaluiert und zertifiziert. Mindestens vier weitere befinden sich in der Evaluierung gemäß ZSIEC oder ITSEC[50]. Drei dieser Produkte können als PC-Sicherheitsprodukte bezeichnet werden, drei sind als Betriebssysteme einzuordnen, eines ist ein „Viren-Scanner“. Zu allen zertifizierten Systemen sind Zertifizierungsberichte bei den Herstellern zu beziehen.

Nach Aussagen eines Vertreters des Herstellers eines Betriebssystems, dessen Evaluierung kurz vor dem Abschluß steht, wird das System in seiner evaluierten Konfiguration vermutlich nie in einer echten Anwendung zum Einsatz kommen, da zu viele im Alltagsbetrieb nützliche Bestandteile nicht mitevaluiert werden konnten. Der wesentliche Nutzen der Evaluation sei, daß jetzt eine einheitlich strukturierte Dokumentation aller Betriebssystemteile vorliege.

Der Hersteller des ersten zertifizierten PC-Produktes bietet neben der als zertifiziert gekennzeichneten Version eine weiterentwickelte Version mit höherer Versionsnummer an. Beide Versionen haben nach Aussagen eines Vertreters der Firma „ihren Markt“, wobei die zertifizierte Version überwiegend von Kunden aus dem Behördenbereich abgenommen wird. Die Kosten für die Evaluierung sollen im 6-stelligen DM-Bereich gelegen haben und sich dank der erhöhten Aufmerksamkeit für Hersteller und Produkt rentieren. Andere Evaluationen haben mehr als 10 Millionen DM gekostet; nicht zuletzt deswegen wird herstellerseitig gefordert, die Evaluationsprüfungen in die Qualitätssicherungsprozeduren der Hersteller zu integrieren[51].

Auch die ersten Erfahrungen mit Evaluationen gemäß der ITSEC liegen inzwischen vor. Ein Beispiel illustriert, daß sich die mangelnde Berücksichtigung des Persönlichkeitsschutzes bei der Formulierung der Sicherheitsziele in den ITSEC in den Evaluationsergebnissen niederschlägt[52]: Eine Funktion zur ausgewählten Protokollierung der Aktivitäten *einzelner* Benutzer wurde als unkritischer und nicht zu bewertender Mechanismus eingestuft, weil ihr Versagen nach Ansicht der Prüfer keine Schwächen verursachte: Ist sie nicht aktiv, werden automatisch die Aktivitäten *aller* Benutzer protokolliert.

IV. Ausblick

1. Notwendige Maßnahmen

Sämtliche Dokumente zur IT-Sicherheit weisen erhebliche und bereits vielfach veröffentlichte Schwächen auf:

Das IT-Sicherheitshandbuch bedarf dringend einer grundlegenden Überarbeitung. Vorher sollte es nicht als verbindliche Grundlage für Sicherheitskonzepte dienen.

Wenigstens folgende Maßnahmen müssen ergriffen werden, damit die ITSEC zu einem echten Beitrag zur IT-Sicherheit werden:

(1) Entweder Titel und Anwendungsbereich müssen enger gefaßt werden, oder es ist wesentlich mehr und breiter angelegte Arbeit als bisher in die Kriterien zu investieren.

(2) Funktionalitätsklassen, die einer demokratischen Gesellschaft nützen, müssen entwickelt werden. Dabei sind das informationelle Selbstbestimmungsrecht des Bürgers und das Recht auf unbeobachtbare Kommunikation[53] zu beachten.

(3) Die Kriterien müssen hinsichtlich ihrer praktischen Verwertbarkeit geprüft werden, etwa ob sie sich zur Beschreibung der Probleme vernetzter Systeme mit verteilter Verantwortung bei öffentlichen Anwendern überhaupt eignen.

(4) Die u.a. durch den GI-Präsidiumsarbeitskreis „Datenschutz und Datensicherung“ kritisierten[54] und hier aus Platzmangel im Detail nicht aufgeführten technischen Schwächen sind zu beseitigen.

2. Änderung der Entscheidungsabläufe

Ebenso wie wirklich überzeugende Grundlagendokumente zur IT-Sicherheit fehlt auch noch eine europaweit überzeugende und harmonisierte Regelung für Evaluation, Zertifizierung und Akkreditierung. In Deutschland hat die Vielfachfunktion des *BSI* als

(1) Evaluierungsstelle,

(2) Akkreditierungsstelle,

(3) Zertifizierungsstelle,

(4) Entwickler von Schutzmechanismen im Auftrag staatlicher Stellen und

(5) Zulassungsinstanz von Mechanismen für die Anwendung im Behördenbereich, insbesondere bei Kryptoalgorithmen sowie Maßnahmen und Vorschriften zur Vermeidung kompromittierender elektomagnetischer Abstrahlung (Transient ElectroMagnetic Pulse Emanation STandard (TEMPEST))

bislang nicht zu der erhofften wesentlichen Steigerung der IT-Sicherheit beigetragen, sondern eher die dringend nötige und offene Diskussion von Problemen und Lösungsansätzen erschwert (vgl. III.2). Dies und die Intransparenz wesentlicher Entscheidungen bzw. Entscheidungsprozesse bezüglich der „Grundlagenwerke zur IT-Sicherheit“ zwischen dem *Bundesministerium des Innern*, dem *BSI* und bevorzugt einbezogenen Unternehmen legen eine Entflechtung der Kompetenzen in einem überarbeiteten IT-Sicherheitsrahmenkonzept und eine stärkere parlamentarische Kontrolle der Aktivitäten zur IT-Sicherheit nahe. Ähnliches gilt für die Intransparenz der Entscheidungsprozesse auf EG-Ebene, die ebenfalls durch eine stärkere

Beteiligung der Legislative, also des *Europäischen Parlamentes*, aufgehellt und auf eine datenschutzverträglichere Grundlage gestellt werden sollten.

Wer für die Folgen unzureichender Evaluierungen auf der Grundlage unzureichender Dokumente im Einzelfall haftet, ist uns unklar. Zu befürchten bleibt, daß die Gesamtfolgen vom demokratischen Gemeinwesen getragen werden müssen, das gleichzeitig zwei Dinge riskiert:

(1) Seine Wirtschaftskraft (auch im Vergleich zu anderen Staaten), weil unverzichtbare Teile der Informationstechnik, von denen das Funktionieren unserer Volkswirtschaft abhängt, unsicher sind und fortschrittliche Konzepte weder umgesetzt noch erprobt werden,

(2) die Demokratie selbst, da die IT-Sicherheitsdokumente bisher nur die Interessen der IT-Betreiber und – in Grenzen – der IT-Nutzer berücksichtigen, keineswegs aber die legitimen und für das Funktionieren jeder Demokratie essentiellen Datenschutzbelange der Bürger, deren Daten „gesichert" werden.

---

1 Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik (IT) – IT-Sicherheitsrahmenkonzept, beschlossen vom *Bundeskabinett* am 23.11.1989, Vorlage des Bundesministerium des Innern erschienen in Datenschutz und Datensicherung DuD 13. Jg., Heft 6, 1989, S. 291-299.

2 *Bundesamt für Sicherheit in der Informationstechnik*: IT-Sicherheitshandbuch, Handbuch für die sichere Anwendung der Informationstechnik, Version 1.0 – März 1992, BSI 7105, viii + 329 Seiten, Zitat auf S. iii.

3 *Kersten, H.*: Neue Aufgabenstellungen des Bundesamtes für Sicherheit in der Informationstechnik, Datenschutz und Datensicherung, 16. Jg, Heft 6, 1992, S. 293-297.

4 Aus Platzgründen können technische Details teilweise nur andiskutiert werden. Der hieran interessierte Leser sei auf die folgenden Texte verwiesen: *Meyer, M./Rannenberg, K.*: Eine Bewertung der „Information Technology Security Evaluation Criteria", Proc. Verläßliche Informationssysteme (VIS'91), März 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, S. 243-258; *Rihaczek, K.*: Bemerkungen zu den harmonisierten Evaluationskriterien für IT-Systeme, Proc. Verläßliche Informationssysteme (VIS'91), März 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, S. 259-276; *Rihaczek, K.*: The Harmonized ITSEC Evaluation Criteria, Computers & Security 10. Jg., 1991, S. 101-110; *Brunnstein, K./ Fischer-Hübner, S.*: Möglichkeiten und Grenzen von Kriterienkatalogen, Wirtschaftsinformatik 4/92, 34. Jahrgang, August 1992, S. 391-400; *Gehrke, M./Pfitzmann, A./Rannenberg, K.*: Information Technology Security Evaluation Criteria (ITSEC) – a Contribution to Vulnerability? Proc. of the IFIP 12th World Computer Congress, Madrid, September 1992, Hrsg. R. Aiken, North Holland 1992, S. 579-587, die Originaldokumente und die im folgenden zitierten Stellungnahmen des *Präsidiumsarbeitskreises „Datenschutz und Datensicherung" der Gesellschaft für Informatik* (FN 14 und FN 27).

5 FN 1.

6 FN 3.

7 FN 2.

8 Handbuch für die sichere Anwendung der Informationstechnik (IT) – IT-Sicherheitshandbuch – 4. Entwurf vom 26. Juli 1991.

9 Jahresbericht 1991 des *Berliner Datenschutzbeauftragten* zum 31.12.1991, S. 16, vgl. auch CR, 8. Jg. S. 381.

10 *Voßbein, R.*: IT-Sicherheitskonzeptionen – Do-it-yourself?, Recht der Datenverarbeitung, 8. Jg, Heft 4, 1992, S. 162-166.

11 Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz – BSIG) vom 17.12.1990, in Bundesgesetzblatt Jg. 1990, Teil I, S. 2834-2836, Nr. 71 vom 22.12.1990.

12 Die Abstimmung der Begriffe der deutschen und englischen Fassung der ITSEC ist (noch) nicht völlig schlüssig. „Evaluation" ist im deutschen „Glossar" der ITSEC als spezielle Form von „Bewertung" definiert, im englischen „Glossary" als spezielle Form von „Assessment" (vgl. III.3.d). Dem widerspricht der Vergleich zwischen englischem und deutschem Titel – aus englischer „Evaluation" wird deutsche „Bewertung". Auflösen ließe sich dieser Konflikt, wenn aus den „Kriterien zur Bewertung" einfach „Evaluationskriterien" würden.

13 „UK IT Security Evaluation and Certification Scheme, Publication No.1 – Description of the Scheme", Issue 1.0, 1 March 1991, Hrsg. Communications-Electronics Security Group & Department of Trade and Industry.

14 Stellungnahme zum Evaluationshandbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) V0.2 des *Präsidiumsarbeitskreises Datenschutz und Datensicherung der Gesellschaft für Informatik*, Datenschutz-Berater 15. Jg., Heft 8, 1992, S. 8-11.

15 *Department of Defense* Standard: Department of Defense Trusted Computer System Evaluation Criteria, December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225,711.

16 *Informal EC advisory group SOG-IS*: Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1.2, 28 June 1991.

17 *National Computer Security Center*: Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-005 Version 1, 31 July 1987, nach seiner Umschlagsfarbe „Red Book" genannt.

18 *Schütz ig, R.*: Evaluierung komplexer Systeme – Folgerungen für Sicherheitskriterien, VIS'91 – Verläßliche Informationssysteme, Informatik-Fachberichte 271, März 1991, Springer-Verlag, Berlin, S. 116-132.

19 *Chokhani, S.*: Trusted Products Evaluation, Communications of the ACM 35. Jg., Heft 7, 1992, S. 64-76.

20 Entscheidung des *BVerfG* zum Schutz des Kommunikationsvorgangs, abgedruckt in CR 8. Jg., Heft 7, 1992, S. 431-435.

21 *Zentralstelle für Sicherheit in der Informationstechnik* (Hrsg.): IT-Sicherheitskriterien, Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT), 1. Fassung vom 11.1.1989, Köln, Bundesanzeiger 1989.

22 FN 3.

23 *Clark, D./Wilson, D.*: A Comparison of Commercial and Military Computer Security Policies, Proc. 1987 IEEE Symp. on Security and Privacy, April 27-29, 1987, Oakland, California, S. 184-194.

24 *Voydock, V./Kent, S.*: Security Mechanisms in High-Level Network Protocols, ACM Computing Surveys 15 Jg., Heft 2, 1983, S. 135-171.

25 vgl. *Rannenberg, K.*: Technischer Datenschutz in CIM-Systemen und anderen verteilten Anwendungen, Bericht 1988/16, TU Berlin, Fachbereich Informatik.

26 *Pfitzmann, A.*: Statement of Observations concerning the Draft of the Information Technology Security Evaluation Criteria (ITSEC) Version 1, 02 May 1990, Institut für Rechnerentwurf und Fehlertoleranz, University of Karlsruhe, Sept. 3, 1990; *Pfitzmann, A.*: Statement of Observations concerning the Draft of the Information Technology Security Evaluation Criteria (ITSEC) Version 1.1, 10 January 1991, Institut für Rechnerentwurf und Fehlertoleranz, University of Karlsruhe, March 29 and April 18, 1991; *Rannenberg, K.*: VIS '91: IT-Sicherheit – Bewertungskriterien, CR 7. Jg, Heft 11, 1991, S. 699-701; *Pfitzmann, A.*: Statement of Observations – ITSEC V1.2, ACM SIGSAC Review 10. Jg., Heft 1, 1992, S. 44-53, vgl. auch FN 4.

27 *Präsidiums-Arbeitskreis "Datenschutz und Datensicherung" der Gesellschaft für Informatik*: Stellungnahme zu den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) V1.2, Datenschutz-Berater 15. Jg., Heft 4, 1992, S. 7-12 und Datenschutz und Datensicherung DuD 16. Jg., Heft 5, 1992, 233-236.

28 Protokollierung kann zusätzlich zu den in den IT-Sicherheitskriterien und ITSEC beschriebenen Aufgaben auch die Funktion eines (hoffentlich vertrauenswürdigen) Dritten übernehmen. Beispielsweise kann sie zum Schlichten des Disputs zwischen zwei Teilnehmern, ob der eine eine Nachricht an den anderen gesendet hat, verwendet werden.

29 *ISO7498-2*: Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, INTERNATIONAL STANDARD ISO IS 7498-2, First edition 1989-02-15.

30 *Chaum, D.*: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, CACM 24. Jg., Heft 2, 1981, S. 84-88; *Chaum, D.*: Sicherheit ohne Identifizierung, Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen, Informatik-Spektrum 10. Jg., Heft 5, 1987, S. 262-277 und Datenschutz und Datensicherung DuD 12. Jg., Heft 1, 1988, S. 26-41; *Pfitzmann, B./Waidner, M./Pfitzmann, A.*: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen, CR 3. Jg., Hefte 10,11,12, 1987, S. 712-717, 796-803, 898-904; *Pfitzmann, A./Pfitzmann, B./Waidner, M.*: Datenschutz garantierende offene Kommunikationsnetze, Informatik-Spektrum 11. Jg., Heft 3, 1988, S. 118-142; *Pfitzmann, A./Pfitzmann, B./Waidner, M.*: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2•64 + 16)-kbit/s-Teilnehmeranschluß, Datenschutz und Datensicherung DuD 13. Jg., Heft 12, 1989, S. 605-622; *Pfitzmann, A.*: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz, IFB 234, Springer-Verlag, Heidelberg Jan. 1990.

31 *Der Bundesminister des Innern* (ed.): Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1, 02 May 1990; *Department of Trade and Industry*: Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1.1, London, 10 January 1991; *Informal EC advisory group SOG-IS*: Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1.2, 28 June 1991.

32 *Informal EC advisory group SOG-IS*: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik, Information Technology Security Evaluation Criteria (ITSEC), Vorläufige Form der harmonisierten Kriterien, Version 1.2, 28 June 1991.

33 In der offiziellen deutschen Übersetzung der ITSEC (FN 32) wird nicht, wie bei den ZSIEC, von Qualitätssicherung, sondern von Vertrauenswürdigkeit geschrieben. Trotzdem behalten wir im folgenden auch für die ITSEC den eingeführten Begriff Qualitätssicherung bei.

34 ITSEC deutsch (FN 32), § 6.57.

35 Anonymität eines Handelnden *H* gegenüber einem „Angreifer" *A* bedeutet, daß aus Sicht von *A* die Handlungen von allen, zumindest aber sehr vielen, als Urheber in Frage Kommenden begangen worden sein können. *A* erfährt durch die Handlungen also nichts, oder zumindest nur sehr wenig, über die zivile Identität ihres Urhebers. Für viele von IT-Systemen zu erbringende Dienste müssen als „Angreifer" auch der Systemhersteller, -betreiber und Kommunikationspartner betrachtet werden. Für die Gestaltung von IT-Systemen und -Diensten wichtig ist, daß Identifikation und Anonymität sich nicht ausschließen, wenn man die Identifikation nicht auf die zivile Identität, gleichsam ein globales Personenkennzeichen, bezieht, sondern auf Pseudonyme von ansonsten anonymen Rollenträgern. Man spricht dann von Pseudonymität. Mehr hierüber ist in *Pfitzmann, B./Waidner, M./Pfitzmann, A.*: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen, CR 3. Jg., Hefte 10,11,12, 1987, S. 712-717, 796-803, 898-904 zu finden.

36 Unbeobachtbarkeit eines Ereignisses *E* (z.B. einer Handlung) durch einen „Angreifer" *A* bedeutet, daß die Wahrscheinlichkeit des Auftretens von *E* vor und nach jeder für *A* möglichen Beobachtung gleich ist. Dies kann natürlich nur für an *E* unbeteiligte Angreifer der Fall sein. Mehr hierüber ist in *Pfitzmann, A.*: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz, IFB 234, Springer-Verlag, Heidelberg Jan. 1990 zu finden.

37 In vielen Anwendungen der IT, insbesondere wenn mehrere Menschen kooperativ arbeiten und für die Anwendung Verfügbarkeitsforderungen bestehen, genügt es nicht, Benutzern des IT-Systems Rechte einzuräumen, d.h. bestimmte Aktionen zu erlauben. Es ist auch nötig, ihnen Pflichten aufzuerlegen, d.h. von ihnen gewisse Aktionen innerhalb vorgegebener Zeit zu erwarten und die Konsequenzen (zumindest teilweise im IT-System automatisiert) des Unterlassens dieser Aktionen festzulegen.

38 Der Originaltext aus § 2.33 der englischen Fassung der ITSEC (FN 31, Version 1.2, 28 June 1991) lautet: „It is recommended that these standard headings are used whenever possible. Their use will simplify comparison with other security targets and make it easier to determine whether or not a particular security target includes, or precludes, functions of a particular type." (Die Unterstreichungen sind in den ITSEC nicht enthalten).

39 Deutsche Fassung in Datenschutz und Datensicherung DuD 16. Jg., Heft 5, 1992, S. 233-236 und Datenschutz-Berater 15. Jg., Heft 4, 1992, S. 7-12.

40 Zuständig ist die „Working Group 3" (WG3) des „Scientific Committee" 27„Security Techniques" (SC 27) des „Joint technical Committee 1" (JTC1) von ISO und IEC, kurz ISO/IEC JTC1/SC27/WG3.

41 Später erhielt es die Nummer JTC1.27.16.

42 Die 4 Stufen sind „Working Draft" (WD), „Committee Draft" (CD), „Draft International Standard" (DIS) und „International Standard" (IS).

43 „Minimum Security Requirements for Multi-User Operating Systems – A Protection Profile for the U.S. Information Security Standard", Issue 2, August 7, 1992 und „Minimum Secure Functionality Requirements for Multi-User Operating Systems" (MSFR), Issue 1, January 16, 1992, beide veröffentlicht durch: Computer Security Division, Computer Systems Laboratory, *National Institute of Standards and Technology*, Gaithersburg, Maryland 20899, USA.

44 *Zentralstelle für Sicherheit in der Informationstechnik* (Hrsg.): IT-Evaluationshandbuch – Handbuch für die Prüfung der Sicherheit von Systemen der Informationstechnik (IT) – 1. Fassung vom 22. Februar 1990, Bundesanzeiger Verlag, Köln.

45 Information Technology Security Evaluation Manual (ITSEM) Draft V0.2 vom 2.4.1992, erhältlich bei der Kommission der Europäischen Gemeinschaften, Direktorat XIII F, Rue de la Loi 200, B-1049 Brüssel.

46 FN 14.

47 Trojanische Pferde sind Programme oder Programmteile, die ähnlich der aus der griechischen Mythologie bekannten Holztrophäe neben ihrer eigentlichen und dem arglosen Nutzer bekannten Aufgabe weitere unbekannte Aufgaben haben, etwa die Verbreitung von Viren oder die heimliche Protokollierung von Aktivitäten im System. Besonders gefährlich sind weiter durchdachte Varianten trojanischer Pferde: Transitive trojanische Pferde, etwa Übersetzer von Programmen) erzeugen selbst trojanische Pferde, Universelle trojanische Pferde lassen sich noch nach ihrer Installierung von Außenstehenden programmieren und zu beliebigen Aktivitäten anleiten.

48 12 der 16 evaluierten Produkte wurden mit dem „Level" C2 versehen, bei 18 der 30 zu evaluierenden Produkte wird das „Level" B1 angestrebt, vgl. auch *Chokhani, S.*: Trusted Products Evaluation, Communications of the ACM 35. Jg., Heft 7, 1992, S. 64-76.

49 FN 3.

[50] Vermutlich befinden sich weitere Produkte in der Evaluierung; Hersteller müssen jedoch einer Veröffentlichung dieser Tatsache nicht zustimmen.

[51] *Stiegler, H.*: Stellenwert von Sicherheitskriterien für Lehre und Forschung aus Herstellersicht, vorgetragen auf dem Workshop „Datenschutz und Datensicherheit in Lehre und Forschung" der Fachgruppe „Verläßliche Informationssysteme" der GI am 26. Juni 1992, eine schriftliche Fassung erscheint in Datenschutz und Datensicherung.

[52] *Corbett, C.*: ITSEC in Operation – an Evaluation Experience, Proc. 4th Annual Canadian Computer Security Conference, Mai 1992, Ottawa, Kanada, S. 439-460.

[53] FN 20.

[54] FN 14, FN 26, FN 27.