Wie sicher ist eigentlich Sicherheit ?

Mit Evaluation nach ITSEC mehr Vertrauen in IT-Sicherheit gewinnen.

von Claus Stark
Veröffentlicht in: F!fF Kommunikation September 1997 (leicht überarbeitet)

Unsichere Software ist heute der Normalfall. Selbst kleine Programmpakete haben oft große "Macken", an Programmabstürze und Viren haben wir uns schon gewöhnt:

- Eingeschleppte Computerviren zerstören wertvolle Datenbestände und programmieren unsere Bürosoftware gezielt um.
- Durch das Betriebssystem verschlüsselte Dateien und Paßwortdateien lassen sich oft genug mit kostenlosen Freeware-Programmen auslesen.
- Zugangssicherungssysteme für PCs lassen sich z.T. durch einfaches Booten vom Diskettenlaufwerk aus umgehen.
- Firewalls lassen sich gelegentlich von außen umkonfigurieren.
- Paßworte und elektronische Briefe werden im Internet oft unverschlüsselt übertragen.

Unsichere - oder vermeintlich sichere - Systeme führten bisher in der Praxis nicht zwangsläufig zum "GAU", da sie oft in unkritischen Bereichen eingesetzt wurden. In kritischen Bereichen - wie beispielsweise dem Militär, dem Geheimdienst und in der Medizin - wurden Computersysteme allerdings seit jeher auf Sicherheit überprüft, bevor sie eingesetzt werden durften.

Die Frage nach der Sicherheit von Computersystemen wird aber in Zukunft immer wichtiger, denn nun werden auch Bereiche informatisiert, die vorher - u.a. auch wegen der mangelhaften Sicherheit herkömmlicher IT-Konzepte - als nicht computerisierbar galten. Das Standardbeispiel ist hier die "Rechtsverbindliche Telekooperation": Das zum 1.8.1997 inkraftgetretene Signaturgesetz stellt die Grundlage der rechtsverbindlichen elektronischen Unterschrift dar - die Informationsgesellschaft will endlich erwachsen werden. Aber das führt langsam zu einer Sensibilisierung in der Bevölkerung und bei den Entscheidungsträgern in Wirtschaft und Politik.

Es soll der Beitrag "geprüfter IT-Sicherheit" für eine "sichere Informationsgesellschaft" diskutiert werden. Welche Rolle spielt das Konzept "Evaluation" beim Aufbau von Sicherungsinfrastrukturen? Dazu wird ein Blick in

die tägliche Evaluationspraxis geworfen: Was ist IT-Sicherheit? Wie wird sie geprüft? Und was kann von einem Sicherheitszertifikat erwartet werden?

Was heißt hier "sicher" ?

Heute versteht die Fachwelt unter Sicherheit - genauer: IT-Security - vorwiegend drei Dinge:

- **Vertraulichkeit**: Schutz vor unbefugter Einsichtnahme in Informationen
- **Integrität**: Schutz vor unbefugter Änderung von Informationen
- **Verfügbarkeit**: Schutz vor unbefugter Vorenthaltung von Informationen und Betriebsmitteln

Man mag darüber streiten, ob dieser Kanon erweitert werden sollte oder nicht. Der Begriff ist momentan genau definiert und umfaßt z.B. nicht "Safety", den Schutz von Leib und Leben vor wildgewordenen Computersystemen. Safety - zu Deutsch ebenfalls mit "Sicherheit" zu übersetzen - spielt z.B. bei medizinischen Geräten eine große Rolle. Dafür gibt es eigene Experten, Prüfkriterien und Laboratorien.

Sicherheit in Form von "Security" kann in Computersysteme eingebaut werden. Wenn man das nicht könnte:

- Würden Sie als Patient Ihre sensiblen medizinischen Daten einer Patientenchipkarte anvertrauen, wenn jedermann sie leicht lesen könnte?
- Würden Sie als Bankmanager einer Geld-Chipkarte trauen, wenn der auf ihr gespeicherte Betrag mit jedem PC manipuliert werden kann?
- Würden Sie einem TrustCenter ohne auf Einbruchssicherheit ausgelegte Computeranlage ihre kryptographischen Schlüssel zur Verwaltung anvertrauen?
- Würde Sie als Arbeitgeber einem unsignierten elektronischen Zeugnis eines Bewerbers glauben?

Sicher nicht! Zum Glück bauen ja die meisten Hersteller viele "Security-Features" in ihre Produkte ein! Aber - können wir dieser Sicherheit trauen?

Können wir der Sicherheit vertrauen ?

Ohne IT-Sicherheit, ob Safety oder Security (oder auch noch anderer Aspekte wie z.B. Privacy), wird es schwer sein, tragfähiges Vertrauen für die von vielen

angestrebte "Informationsgesellschaft" zu gewinnen. Daten wollen wirksam vor fremden Blicken, Systeme vor unberechtigtem Zugriff geschützt werden, sollen sich Computersysteme erfolgreich in vielen relevanten gesellschaftlichen Bereichen durchsetzen. Elektronische Unterschriften sollten sich nicht fälschen lassen. Ohne Sicherheit geht es also nicht - aber sind die "sicheren" Systeme wirklich sicher, sicher genug für unsere Gesellschaft, um darauf eine "Kulturrevolution" wie die Einführung der Digitalen Signatur aufbauen zu können? Oder sind sie gar *zu* sicher? Diese eher demokratietheoretische Frage wird am Schluß dieses Beitrags kurz angerissen und soll hier nicht weiter diskutiert werden. Es gibt einige Produkte, die viel versprechen - und wenig halten. Und manchmal nutzt die beste Security nichts, wenn der Systemverwalter sie aus Bequemlichkeit leicht ausschalten kann. Die Herstellererklärungen sollten stets kritisch hinterfragt werden. Der Kunde ist aber (meistens) überfordert, die Produkte selber adäquat zu prüfen.

Es ist daher unverzichtbar, die technische Sicherheit von IT-Systemen von unabhängigen und fachkundigen Dritten prüfen ("evaluieren") und zertifizieren zu lassen. "Evaluation" ist somit ein wichtiger Baustein beim Aufbau und Betrieb von (Infrastruktur-)Einrichtungen der "Informationsgesellschaft". Eine Reihe von Institutionen und Firmen bieten Sicherheitsevaluation als Dienstleistung an[1].

Immer mehr Hersteller lassen ihre Systeme - ob Chipkartenbetriebssystem oder PC-Sicherheitssoftware - nach anerkannten Kriterien wie die im Sicherheitsbereich wichtigen ITSEC, den im Finanzbereich relevanten ZKA-Kriterien ("Zentraler Kreditausschuß") oder nach anderen Kriterienwerken evaluieren. Die Hersteller nehmen die Zertifizierung als Chance einer zusätzlichen Qualitätskontrolle wahr, und sie erhoffen sich dadurch einen Marktvorteil gegenüber den Konkurrenten, oder überhaupt den Marktzugang beim Kunden: Viele Anwendungsanbieter wie Banken oder große Telekommunikationsunternehmen verlangen von ihren Zulieferern die unabhängige Evaluation ihrer Produkte. Keine Bank würde einem Chipkartenhersteller für eine Geldkartenanwendung auch nur eine Chipkarte ohne unabhängige Prüfung abnehmen: Sie könnte ja durch Hacker - oder einfach nur durch eine Fehlfunktion - leicht kompromittiert werden, und das kann und will man sich nicht leisten. Die Evaluation bietet ein Maß, inwieweit der versprochenen IT-Sicherheit getraut werden kann. Die Bundesregierung beschäftigte sich übrigens im Signaturgesetz und in der dazugehörigen Signaturverordnung zum ersten Mal mit der ITSEC: Für rechtsverbindliche Konzepte zur Digitalen Signatur werden "vertrauenswürdiger Produkte und Systeme" gefordert. Die Hersteller

---

[1] Eine vollständige Liste der akkredierten Prüfstellen ist beim Bundesamt für Sicherheit in der Informationstechnik (BSI) erhältlich.

entsprechender Systeme - von der Chipkarte bis zum ganzen TrustCenter - werden im Gesetz zur unabhängigen Prüfung nach ITSEC verpflichtet.

Kriteriengestützte Evaluationen von IT-Sicherheit geben Auskunft über die Vertrauenswürdigkeit, die man "objektiv" in die technische Sicherheit eines konkreten Produktes haben kann. Sie versprechen die Meßbarkeit von IT-Sicherheit. Das europäische Kriterienwerk, das diese Prüfung erlaubt, ist die 1991 vorgelegte ITSEC, die "Information Technology Security Evaluation Criteria" - Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik. Sie bieten 7 Stufen der Vertrauenswürdigkeit: Die Skala reicht von E1 (Basisvertrauen in die implementierte Sicherheit) bis hoch zu E6 (höchste Vertrauenswürdigkeit) - E0 (unzureichende Vertrauenswürdigkeit) sei der Vollständigkeit halber erwähnt. Je höher diese Stufe ist, umso tiefergehende und höherwertige Dokumente muß der Hersteller für die Evaluation bereitstellen. Die meisten zertifizierten Produkte pendeln momentan bei E2/E3 - eine langsame Verschiebung in Richtung E4/E5 wird erwartet. Nach E6 wurde in Europa noch kein Produkt evaluiert. In Deutschland und Europa wird vorwiegend nach ITSEC evaluiert - und vom BSI (dem Bundesamt für Sicherheit in der Informationstechnik in Bonn) zertifiziert. Ein etwas älteres Kriterienwerk ist das "Orange Book", die US-amerikanischen "TCSEC" ("Trusted Computer Security Evaluation Criteria") von 1985. Die ITSEC gilt allerdings als abstrakt und bürokratisch, die TCSEC schlicht als veraltet: Die Zukunft soll nun den CC gehören, den "Common Criteria for IT-Security Evaluation" - sie soll von der Standardisierungsorganisation ISO als weltweite Norm anerkannt werden und die aktuellen Kriterienkataloge langfristig ablösen.

Die Prüfung nach ITSEC - Ein Blick über die Evaluatorschulter

Mittelfristig gilt in Europa und in Deutschland die ITSEC als das Maß aller IT-Sicherheit. Aber was kann praktisch von erfolgreich evaluierten Produkten erwartet werden? Ist beispielsweise ein nach E4 zertifiziertes Chipkartenbetriebssystem geeignet, medizinische Daten vertrauenswürdig zu speichern? Ein Blick in die Evaluationspraxis soll helfen, eine Zertifizierung besser einzuschätzen.

Die ITSEC umfaßt vorrangig die Bewertung technischer Sicherheitsmaßnahmen. Organisatorische, personelle, administrative Maßnahmen stehen nicht im Mittelpunkt der Analyse, werden aber berücksichtigt. Das Kriterienwerk ist dabei so allgemein gehalten, daß sowohl Hardware, Software und Firmware (sowie deren Kombination) evaluierbar ist. Jede ITSEC-Evaluation soll objektiv und

unvoreingenommen sein - darauf sind die deutschen vom BSI akkreditierten Prüfstellen geprüft und verpflichtet.

Die konkrete Prüfung eines Produktes (oder eines Systems) nach ITSEC erfolgt auf Initiative des Herstellers bzw. eines seiner (potentiellen) Kunden. Der Antragsteller sucht sich dazu eine von der nationalen Zertifizierungsbehörde (in Deutschland: BSI) akkreditierten Prüfstellen aus. Die Evaluation erfolgt in enger Kooperation zwischen Antragsteller[2], Hersteller, Prüfstelle - und ggfs. dem BSI.

Der Hersteller beschreibt möglichst genau sein zu evaluierendes Produkt oder System, den "Evaluationsgegenstand" (EVG). Nur dieser EVG wird evaluiert. Ist ein System zu komplex, um es als Ganzes zu evaluieren, wird ein geeigneter Teil des Produktes als EVG bestimmt. Diese Abgrenzung muß sehr sorgfältig erfolgen, denn die Abhängigkeiten von anderen Systemkomponenten, die auch von Drittherstellern stammen können, lassen oft eine genaue Aufteilung der "Sicherheitsverantwortung" nur schwer zu: Baut beispielsweise ein Sicherheitsprodukt seine Sicherheitsfunktionalität auf Leistungen des darunterliegenden (ungeprüften?) Betriebssystems auf oder stellt es diese selbst zur Verfügung? Die Schnittstellen des EVG mit seiner (technischen) Umwelt und die Einsatzbedingungen spielen naturgemäß eine besondere Rolle in der Evaluation.

Der Hersteller hat mit dem EVG auch die Ziele, die er mit ihm nachprüfbar erreichen möchte, definiert: Welche Sicherheitsziele werden angestrebt? Welche Funktionalität soll durch das Produkt bereitgestellt werden? Was sind die angenommenen Bedrohungen, denen entgegengewirkt werden soll? Für ein PC-Sicherheitsprodukt ist es vielleicht die Vertraulichkeit von Dateien, die es vor unbefugten Blicken schützen soll, für eine Firewall ist sicherlich ein unverzichtbarer Aspekt die "Einbruchssicherheit". Die ITSEC schlägt einige Sicherheitsfunktionen in Form von Funktionalitätsklassen (wie "F-C2") vor. Dem Hersteller steht es aber frei, die zu evaluierende Sicherheitsfunktionalität individuell zu wählen - die ITSEC ist in dieser Hinsicht sehr flexibel: Aus generischen Oberbegiffen wie "Identifikation & Authentisierung" oder "Beweissicherung" lassen sich eine Vielzahl konkreter Sicherheitsfunktionalitäten für eine Vielzahl von Produkten und Systemen ableiten. Die Sicherheitsvorgaben und die Festlegung des EVG stellen die Basis für die gesamte Evaluation dar.

Die ITSEC sieht verschiedene Stufen der Evaluation vor: E1 (Basisvertrauen in die realisierte Sicherheit) bis hoch zu E6 (höchstes Vertrauen in die realisierte Sicherheit). Diese Stufen bestimmen die Prüftiefe: Für niedrige Stufen (E1 / E2)

---

[2] Da die Rolle des Antragstellers oft mit der Rolle des Herstellers zusammenfällt, sei der Einfachkeit halber im Folgenden nur noch vom Hersteller die Rede.

stellen die Hersteller den Evaluatoren informelle Dokumentation zur Verfügung - damit kann aber mit der Evaluation natürlich nur eine niedrige Stufe der Vertrauenswürdigkeit bescheinigt werden. Soll nach höheren E-Stufen (E3 - E6) evaluiert werden, werden Dokumente wesentlich höherer Qualität vom Hersteller gefordert - das geht bis zur Bereitstellung von nachvollziehbar dokumentiertem Quellcode, semiformalen Spezifikationsdokumenten und beweisbaren formalen Sicherheitsmodellen. Schon bei niedrigen Stufen ab E2 wird der Entwicklungsprozeß selbst überprüft: Wird Konfigurationsmanagement betrieben und mit einer definierten Entwicklungsumgebung gearbeitet? Ab E3 müssen die verwendeten Programmiersprachen klar definiert sein (z.B. nach ISO). Die Anforderungen an die vorzulegenden Dokumente hängen von der angestrebten Evaluationsstufe ab.

Die Evaluatoren beginnen damit, die Korrektheit der Dokumente zu prüfen: Sind die Sicherheitsziele in den Sicherheitsvorgaben eindeutig festgelegt? Von welchen Bedrohungen wird ausgegangen? Wie werden vom EVG adäquate Sicherheitsfunktionen bereitgestellt, die den angenommenen Bedrohungen entgegenwirken sollen? Lassen sich die definierten Sicherheitsfunktionen im Architektur- und im Feinentwurf des EVG wiederfinden und vom Rest des EVG abgrenzen? Im Prinzip wird so geprüft, ob die in der obersten Stufe aufgestellten globalen Sicherheitsfunktionen und -mechanismen in allen Dokumenten, die - immer feiner werdend - bis auf Quellcodeebene gehen können, eindeutig nachverfolgt und identifiziert werden können ("traceability"). Neben den Entwicklungsdokumenten wird u.a. noch die Benutzer- und Administrator-Dokumentation daraufhin untersucht, ob sie den Umgang mit den sicherheitsrelevanten Komponenten des Produktes auch adäquat erklärt. Treten Brüche in den Korrektheitsuntersuchungen auf, muß nachgebessert werden: Der Hersteller wird in solchen Fällen empfohlen, entsprechende Änderungen an seinem Produkt und in seiner Dokumentation vorzunehmen - oder einer Rückstufung in der angestrebten E-Stufe zuzustimmen. Gilt nämlich auch nur ein Aspekt als nicht erfüllt, kommt es zum Ergebnis "E0 - unzureichende Vertrauenswürdigkeit" - die ITSEC ist kompromißlos!

Nach diesen Korrektheitsuntersuchungen wird überprüft, ob die implementierten Mechanismen den Bedrohung auch wirksam entgegenwirken können (Wirksamkeitsanalyse). Lassen sie sich schon durch einfache Handgriffe durch Laien "aushebeln" oder braucht man Know-How, Spezialwerkzeug und sehr, sehr viel Zeit? Jeder einzelne Mechanismus wird auf seine Stärke, den Bedrohungen entgegenzuwirken, hin bewertet. Hier müssen Szenarien entwickelt und gedanklich durchgespielt werden, wo konstruktive oder operative Schwachstellen vorhanden sind - und wie diese in der Praxis ausgenutzt werden können.

Liegen alle Erkenntnisse über Funktionsweise, Architektur, Feinentwurf und Schwachstellen des EVG vor, kann mit den direkten Tests am Produkt begonnen werden: Die Prüfstelle führt eigene Tests durch, um vorhandene Schwachstellen auf Ausnutzbarkeit zu prüfen ("Penetrationstests") - lassen sich die Sicherheitsfunktionen direkt oder indirekt austricksen? Die Prüfstelle untersucht auch die Benutzerfreundlichkeit des Produktes - unter "Benutzerfreundlichkeit" versteht ITSEC die Nichtvortäuschbarkeit "sicherer Zustände" in unsicheren Situationen. Daneben werden die Funktionstests der Hersteller nachvollzogen oder eigene Tests durchgeführt, um beispielsweise zu prüfen, ob spezielle Mechanismen auch korrekt implementiert wurden (wie spezielle Verschlüsselungsalgorithmen). Die Testphase kann daher sehr aufwendig sein.

Sind schließlich alle Dokumente erfolgreich geprüft, alle Tests zur Zufriedenheit der Prüfstelle verlaufen, wird das Ergebnis durch die Prüfstelle mit dem Sicherheitsgutachten bescheinigt. Im Falle einer BSI-Zertifizierung erfolgt mit der Ausstellung des Zertifikats der Eintrag in die offizielle "Liste zertifizierter Produkte" und der Hersteller darf das Produkt mit dem Attribut "BSI-zertifiziert nach ITSEC" anbieten.

Das Zertifikat ist kein Freibrief !

Einige Grenzen des Zertifikats wurden bereits deutlich: Es wird bescheinigt, daß die vom Hersteller definierten Sicherheitsziele mit der zur Verfügung gestellten Sicherheitsfunktionalität des EVG erreicht werden. Ob die Funktionalität und die Vertrauenswürdigkeit für konkrete Einsatzgebiete ausreicht oder nicht, muß in jedem Einzelfall vom Kunden selbst geprüft werden. Es ist auch stets zu prüfen, wie alt das Zertifikat ist - bei zu alten Produkten haben es Angreifer vielleicht in der Zwischenzeit gelernt, die Sicherheitsbarrieren zu umgehen.

Das (BSI-)Zertifikat gilt nur für die "eine" evaluierte Version der Software. Bei Versionsänderung des Produktes gilt das Zertifikat nicht mehr - es muß eine Re-Evaluation durchgeführt werden. Hersteller - vor allem die kleineren Firmen - stöhnen hier zwar im Hinblick auf die hohe Innovationsrate im Softwarebereich und auf die Kosten, aber bei intelligenter und kooperativer "entwicklungsbegleitender Evaluation" sollte das kein Handikap darstellen. Es ist auf jeden Fall kein Fehler, "Sicherheit" von Anfang an als explizites Gestaltungsmerkmal in der Entwicklung zu berücksichtigen - und entsprechend explizit zu dokumentieren und zu testen.

Zertifikate gelten nur in Verbindung mit dem dazugehörigen Zertifizierungs-report, der vom Hersteller an Interessenten und Kunden ausgegeben wird. Darin werden Auflagen und Voraussetzungen zum "sicheren Betrieb des EVG" gemacht, ohne deren Erfüllung das Zertifikat nicht gilt. Hier böte sich an, bei komplexeren Systemen oder in sensiblen Bereichen die korrekte und sichere Installation des EVG und seinen sicheren Betrieb beim Kunden durch eine - die Evaluation ergänzende - "Systemakkreditierung" zu bescheinigen.

Es sollte klargeworden sein, daß ein Zertifikat kein Ersatz für den gewissenhaften Umgang mit der konkreten Technologie darstellt. Nachlässigkeit beim Definieren und Umsetzen von Sicherheitsstrategien werden auch durch Zertifikate nicht tolerierbar. Zertifizierte Produkte - gewissenhaft eingesetzt - können aber ein hohes Maß an Sicherheit garantieren.

Security ist gesellschaftlich nicht unumstritten

Nun noch kurz zum gesellschaftspolitischen Aspekt von Sicherheit, denn Security ist nicht unumstritten: Durch sie würden Machtstrukturen gefestigt, die gesellschaftlich unerwünscht seien. Spielte doch "Security" bislang vor allem im militärischen und geheimdienstlichen Bereichen (Geheimhaltung) eine tragende Rolle - hier haben ITSEC und "Orange Book" schließlich auch ihren Ursprung. Wie aber sind "militärische" Sicherheitskonzepte mit der "anarchischen" Freiheit des Internet (welches übrigens einst auch ein militärisches Projekt war) vereinbar? Würde es nicht dem stromlinienförmigen und "abgesicherten" Datasuperhighway weichen, auf der sich dann nur noch Behörden und Industrie in ihren rechtsverbindlichen geschlossenen Intranets tummeln würden? Ärzte könnten nur noch mit gültiger und von der Bundesärztekammer herausgegebener Health Professional Card eine Patientenakte einsehen. Das könnte das Gleichgewicht der Kräfte auf technokratische Weise unzulässig in eine Richtung verschieben und im schlimmsten Fall unsere Demokratie gefährden.

Diese Diskussion ist sehr wichtig und muß heute offensiv geführt werden, damit wir morgen nicht eine "Kontroll- und Steuerinfrastruktur" haben, vor der Kritiker zu Recht warnen. Sozial verträgliche und gesellschaftlich gewünschte Sicherungsinfrastrukturen sind aber möglich: "Privacy", Konzepte zu pseudonymen Handeln und zur Nichtverfolgbarkeit (d.h. die Vermeidung von personenbezogenen Datenspuren), heute große Themen der Datenschützer und Informationsökologen, werden bald auch Themen der "technischen Security" sein!
Diese so im gesellschaftlichen Prozeß gewonnenen Erkenntnisse müssen aber letztendlich auch wieder adäquat in Technik gegossen werden. Und da schließt sich der Kreis bei der Evaluation, der unabhängigen Prüfung von Zielen und

Implementierung! IT-Sicherheitsevaluation ist auch unter dieser Prämisse ein unverzichtbarer Baustein auf dem Weg in die sichere und gesellschaftlich gewünschte Informationsgesellschaft.

Die „E-Stufen“ der ITSEC - Maß des Vertrauens in die Korrektheit

- **E0**: unzureichende Vertrauenswürdigkeit
- **E1**: es wurden Sicherheitsziele und -funktionalität definiert (Sicherheitsvorgaben), eine informelle Beschreibung des Systems wurde geprüft (Architekturentwurf). Es finden Tests zur Überprüfung der Sicherheitsfunktionalität statt.
- **E2**: zusätzlich zu E1 muß ein Designentwurf vorgelegt werden (Feinentwurf). Die Entwicklungsumgebung wird überprüft.
- **E3**: zusätzlich zu E2 muß der Hersteller den Quellcode zur Verfügung stellen.
- **E4**: zusätzlich zu E3 müssen zu den Sicherheitsvorgaben ein formales Sicherheitsmodell, zu den sicherheitsspezifischen Funktionen semiformale Spezifikationsdokumente zur Verfügung gestellt werden.
- **E5**: zusätzlich zu E4 muß der enge Zusammenhang zwischen Feinentwurf und Quellcode nachgewiesen werden.
- **E6**: zusätzlich zu E5 müssen sicherheitsspezifische Funktionen und der Architekturentwurf in formaler (beweisbarer) Notation vorliegen, die konsistent mit dem formalen Sicherheitsmodell sind.

Die Mechanismenstärke nach ITSEC als Maß der Wirksamkeit

- **niedrig**: Sicherheitsmechanismus ist durch Laien schnell zu überwinden
- **mittel**: es wird Expertenwissen und Zeit zum Überwinden benötigt
- **hoch**: Sicherheitsmechanismus ist praktisch nicht zu überwinden

Phasen der Evaluation nach ITSEC

- Vorstudie (optional)
- Festlegen des EVG und der Sicherheitsvorgaben
- Festlegen der angestrebten E-Stufe und der Mechanismenstärke
- ggfs. Antrag auf Zertifizierung beim BSI
- Korrektheitsuntersuchungen
- Wirksamkeitsuntersuchungen
- Tests am Produkt in der definierten Einsatzumgebung
- Zertifikat, ggfs. durch das BSI
- Ggfs. Re-Evaluation bei Änderungen am Produkt

IT-Security-Evaluation im Internet

- www.bsi.bund.de
- ITSEC: http://www.itsec.gov.uk
- CC: http://csrc.ncsl.nist.gov/nistpubs/cc/