IT Sicherheit: Einleitung & Grundbegriffe

Dr. Christian Rathgeb

Hochschule Darmstadt, CRISP, da/sec Security Group

22.04.2020

Leitung und Unterlagen

- VO-Leiter (Zug B): C. Rathgeb
- PR-Betreuer: U. Scherhag, J. Priesnitz
- Email-Adressen:
  christian.rathgeb@h-da.de
  ulrich.scherhag@h-da.de
  jannis.priesnitz@h-da.de
- URL der Lehrveranstaltung:
  https://dasec.h-da.de/teaching/it-sicherheit-dr-rathgeb-ss20/
  (Folien und Praktikumsblätter)

Meine Person

- Büro: ~~D19, Raum 2.02~~
- Telefon: +49 6151 16 30085
- Sprechstunde: nach Vereinbarung per Mail
- Persönliche URL:
  https://www.dasec.h-da.de/staff/christian-rathgeb/

Termine und Ablauf

- Termine Vorlesung und Praktikum: 17 + 4, siehe OBS (4 Aufgabenblätter)
- Praktikum (Mi4x, Mi4y):
  - Tutorium ohne Anwesenheitspflicht
  - Bearbeitung der Aufgaben bis Montag Abend vor dem Praktikum
  - Feedback zu den Ausarbeitungen bis vor dem Praktikum
  - Praktikumstermine dienen als Fragestunde (keine Anwesenheitspflicht)
  - Überarbeitung der Aufgaben bis Freitag Abend
- Prüfungsvorleistung: Testate aller Praktikumsaufgaben

Umgang mit Linux Betriebssystem

- Praktikumsaufgaben erfordern den Umgang mit Linux Betriebssystem
- Empfehlung: Kali Linux VM-Image
- Kali Linux: Link auf Website
- Linux Tutorium (Skript) auf Website der Lehrveranstaltung

Inhalt der Vorlesung

- Kapitel-Übersicht:

1. Einleitung & Grundbegriffe
2. Kryptologie
3. Netzwerksicherheit
4. Authentifikation
5. IT-Forensik
6. Benutzbarkeit und IT-Sicherheit
7. IT-Sicherheitsmanagement

Aktuelle Angriffe

Beinahe täglich werden sicherheitskritische Schwachstelle von und Angriffe auf informationsverarbeitende Systeme veröffentlicht (siehe z.B.: www.heise.de/security)

- Februar 2020: Passwort-Wechsel nur bei Passwort-Diebstahl (Bundesamt für Sicherheit in der Informationstechnik).
- Dezember 2019: Mehrheit der kommerziellen Gesichtserkennungssysteme sind nicht “fair” (NIST Studie).
- April 2019: Mangelhafte IT-Sicherheit im Gesundheitssektor (fehlende Verschlüsselung von sensiblen Patientendaten).

Motivation für Angriffe und Hacker

Klassische Angreifer:

- *White-Hats*: verwenden ihr Wissen um Sicherheits-Schwachstellen in IT-Systemen zu identifizieren (ohne Öffentlichkeit).
- *Grey-Hats*: verwenden ihr Wissen um Sicherheits-Schwachstellen in IT-Systemen zu identifizieren und zu veröffentlichen.
- *Black-Hats*: handeln mit krimineller Energie oder im Auftrag von Regierungen oder Organisationen und beabsichtigen beispielsweise, auf Information eines IT-Systems zuzugreifen (Spionage, Überwachung, Schattenwirtschaft) bzw. das IT-System zu beschädigen (Sabotage).

Angriffsarten

Wir erleben unterschiedliche Arten von Angriffen:

- *Ungezielte Angriffe*, meist über Spam-Mails oder Web-basiert werden z.B. Viren und Trojaner versandt oder Phishing-Angriffe durchgeführt.
- *Gezielte Angriffe*, werden gezielt auf IT-Systeme von Institutionen/Personen gerichtet, z.B. mittels DDoS-Angriffe, Vortäuschung falscher Identitäten (Social-Engeneering, CEO-Attacke).

Schwachstellen in IT-Systemen

Gründe für erfolgreiche Angriffe auf IT-Systemen:

- Konfigurationsmängel, z.B. falsch konfigurierte Webserver mit nicht geändert Standardpasswörter $\rightarrow$ Pentesting
- Schwachstellen in (veralteter) Software $\rightarrow$ Identifikation unsicherer Programmierpraktiken und logische Fehler im Programmablauf
  - Statische Codeanalyse des Source-Codes
  - Fuzzing im Zuge von Black-Box-Tests: fehlerhafte Eingabedaten (z.B. automatisiert mit LibFuzzer)
- Idealerweise sollten Tests durch unabhängige Dritte durchgeführt werden.

Grundlegende Begriffe

Definition und Präzisierung der Begriffe

- Information und Daten
- IT-System und IT-Verbund
- Sicherheit (Betriebs- und Informationssicherheit)
- Bedrohung, Gefährdung, Angriff, Risiko
- Schutzziele (z.B. Vertraulichkeit, Integrität, Verfügbarkeit)
- Datenschutz
- Privacy by Design

Motivation

Informationen sind schützenswerte Güter, z.B. hinsichtlich

- Verlust des informationellen Selbstbestimmungsrechts (Datenschutz): Informationen über Krankheiten, Einkommen
- finanzieller Verluste: Geschäftsgeheimnisse, Verträge, Zugangsdaten zum Online-Banking
- persönlicher Unversehrtheit: Fehlfunktionen medizinischer Überwachungsgeräte, Verkehrsleitsysteme

Informationelles Selbstbestimmungsrecht

Das Recht auf informationelle Selbstbestimmung ist das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

IT- und Informationssicherheit

- Informationssicherheit: Sicherheit bzgl. Informationen, unabhängig von ihrer Repräsentation
- IT- Sicherheit: Sicherheit bzgl. Schutz der elektronischen Informationen
- IT-Sicherheit bildet somit ein Teilgebiet der Informationssicherheit!

Daten

Daten sind Repräsentationen von Informationen, z.B.

- als Bytefolge gespeichert auf einer Festplatte
- als Netzwerkpaket bei der Übertragung über das Internet
- ...

Interpretation der Daten ergibt die Information:

- Beispiel: Daten in Bytefolge ASCII (hex): 44 31 34
- Information (interpretiert): D14
- ASCII (hex): 44 $\rightarrow$ Buchstabe (D)

IT-System

Ein IT-System ist ein dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Daten.

Beispiele:

- Computer, Tablets, Smartphones
- Router, Switches, Netze
- Drucker, Scanner

IT-Verbund

Ein Informationsverbund (oder IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.

Ein IT-Verbund kann verschiedene Ausprägungen haben.

Beispiele:

- eine gesamte Institution (z.B. Firma, Behörde)
- einzelne Bereiche einer Institution, die in organisatorische Strukturen (z.B. Abteilungen) gegliedert sind

Sicherheit

Sicherheit ist der Schutz vor negativen Konsequenzen aus vorsätzlichen und berechtigten Handlungen.

Bzgl. IT-Systeme unterschiedet man zwei Arten von Sicherheit:

- Schutz vor negativen Konsequenzen aus berechtigten Handlungen: Betriebssicherheit/Funktionssicherheit (engl. Safety)
  - Ist-Funktionalität stimmt mit der spezifizierten Soll-Funktionalität überein (alles läuft wie geplant)
- Schutz vor negativen Konsequenzen aus vorsätzlichen Handlungen: Informationssicherheit (engl. Security)
  - Resistenz gegenüber Angriffen (keine unautorisierte Informationsveränderung oder -gewinnung möglich)

Prävention

Kernbestandteil von Betrachtungen über Sicherheit ist in erster Linie Prävention.

Beispiele:

- Physikalische Sicherheitsmerkmale auf Geldscheinen (Ziel Fälschungssicherheit), wie z.B. Wasserzeichen, Infrarot- und UV-Farben
- Verschlüsselung von Dokumenten, E-Mails

Schutzziele

Klassische Schutzziele:

- Vertraulichkeit (engl. Confidentiality)
- Integrität (engl. Integrity)
- Authentizität (engl. Authenticity)
- Nichtabstreitbarkeit (engl. Non-Repudiation)
- Verfügbarkeit (engl. Availability)

Schutzziele bzgl. Datenschutz:

- Anonymität
- Pseudonymität

Beispiel I

- Alice sendet die Nachricht „*Hallo Bob, heute um 10 Uhr bei mir? Alice*“ an den Empfänger Bob.
- Wir betrachten nun folgende Szenarien:

1. Lauscherin Eve hört diese Nachricht ab.
2. Angreiferin Eve ändert die Nachricht auf „*Hallo Bob, heute um* **12** *Uhr bei mir? Alice*“ und sendet diese an Bob.
3. Angreiferin Eve ändert die Nachricht auf „*Hallo Bob, heute um 10 Uhr bei mir?* **Anne**“ und sendet diese an Bob. (Signatur wird verändert)

Beispiel II

4. Eve sendet „*Ich bin Alice*“ an Bob. (Vortäuschung anderer Identität)
5. Alice behauptet im Nachhinein, dass 9 Uhr die vereinbarte Zeit war.
6. Eve sendet nichts an Bob. (Nachrichtentransport wird abgebrochen – Denial of Service)

- Aus den gegebenen Szenarien lassen sich verschiedene Schutzziele ableiten!

Schutzziel Vertraulichkeit

Vertraulichkeit soll sicherstellen, dass Informationen nur autorisierten Personen zugänglich sind.

Maßnahmen zur Umsetzung des Schutzziels Vertraulichkeit:

- Kryptographische Verschlüsselungsverfahren
- Überbringen von Dokumenten durch vertrauenswürdigen Kurier
- Zutrittsregeln (Gebäudesicherung, Raumsicherung)
- Zugriffskontrollen (geeignete Leserechte für gespeicherte Dateien/Verzeichnisse)

Schutzziel Integrität

Unter Integrität versteht man die Vollständigkeit und Unverfälschtheit der Daten für den Zeitraum, in dem sie von einer autorisierten Person erstellt, übertragen oder gespeichert wurden. Darin sind sowohl absichtliche als auch unabsichtliche, z. B. durch technische Fehler verursachte, Veränderungen enthalten.

Maßnahmen zur Umsetzung des Schutzziels Integrität:

- Kryptographische Hashfunktionen, etc.
- Sichere Aufbewahrung von Kopien zum späteren Abgleich mit dem Original
- Zugriffs- und Zutrittsregeln

Schutzziel Datenauthentizität

Die Authentizität von Daten ist gewährleistet, wenn der Urheber der Daten vom Empfänger eindeutig identifizierbar und seine Urheberschaft nachprüfbar ist. Dies beinhaltet auch die Integrität der Daten.

Maßnahmen zur Umsetzung des Schutzziels Datenauthentizität:

- elektronische Signaturen
- händisches Unterschreiben eines Dokumentes
- persönliche Übergabe von Daten

Schutzziel Instanzauthentizität

Ein Objekt oder Subjekt wird als authentisch bezeichnet, wenn dessen Echtheit und Glaubwürdigkeit anhand einer eindeutigen Identität und charakteristischer Eigenschaften überprüfbar ist.

Maßnahmen zur Umsetzung des Schutzziels Instanzauthentizität:

- Benutzername/Passwort
- Challenge-Response-Protokolle
- Ableich der Identität auf Basis hoheitlicher Dokumente (Reisepass, Personalausweis)

Schutzziel Nichtabstreitbarkeit

Die Nichtabstreitbarkeit von Daten ist gewährleistet, wenn der Ersteller der Daten die Erzeugung im Nachhinein nicht abstreiten kann (gerade auch gegenüber Dritten).

Maßnahmen zur Umsetzung des Schutzziels Nichtabstreitbarkeit:

- elektronische Signaturen
- händische Unterschrift
- Nutzung vertrauenswürdiger Zeugen (z.B. Notar)

Schutzziel Integrität, Authentizität, Nichtabstreitbarkeit

Abgrenzung der Begriffe Integrität, Authentizität und Nichtabstreitbarkeit:

- Offensichtlich gilt:
  - Aus der Nichtabstreitbarkeit folgt die Authentizität
  - Aus der Authentizität folgt die Integrität
- Die Umkehrung gilt im Allgemeinen nicht:
  - Sicheres Aufbewahren einer Kopie zum späteren Abgleich sorgt für die Integrität, es kann damit aber nicht festgestellt werden, wer die Daten erzeugt hat; Integrität $\not\Rightarrow$ Authentizität
  - Bei einer persönlichen Übergabe weiß der Empfänger, von wem er die Daten hat, kann dies aber gegenüber einem Dritten nicht nachweisen; Authentizität $\not\Rightarrow$ Nichtabstreitbarkeit

Schutzziel Verfügbarkeit

Ein IT-System gewährt Verfügbarkeit, wenn autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.

Die Messung der Verfügbarkeit erfolgt nach folgender Formel:

$$\text{Verfügbarkeit} = \frac{\text{Gesamtlaufzeit} - \text{Ausfallzeit}}{\text{Gesamtlaufzeit}}$$

Maßnahmen zur Umsetzung des Schutzziels Verfügbarkeit:

- Datensicherung
- Vertretungsregeln
- Unterbrechungsfreie Stromversorgung

Schutzziele Anonymität und Pseudonymität

- *Anonymität*: Personenbezogene Daten werden so verändert, dass diese nicht oder nur mit unverhältnismäßigem Aufwand einer Person zugeordnet werden können.
- *Pseudonymität*: Personenbezogene Daten werden so verändert, dass diese nur unter Kenntnis der Zuordnungsvorschrift einer Person zugeordnet werden können.

Anonymität, Pseudonymität

Abgrenzung der Begriffe Anonymität, Pseudonymität

- Beispiel für Anonymität
  - Geheime Abstimmung bei Wahlen: Zuordnung zwischen Wahlzettel und Wähler ist nicht möglich
- Beispiel für Pseudonymität
  - E-Mail Adresse: Kommunikationspartner kennen nicht die reale Identität (aber der Dienstanbieter)

Authentisierung, Authentifizierung

Abgrenzung der Begriffe Authentisierung, Authentifizierung (beide engl. authentification):

- Authentisierung: Nachweis der Identität
  - Ich weise mich durch Eingabe meines Benutzernamens/Passwortes aus
  - Ich weise mich mit meinem Personalausweis aus
- Authentifizierung: Prüfung des Nachweises
  - Benutzername/Passwort wird geprüft
  - Personalausweis und Verknüpfung mit meiner Person werden geprüft

Nach der Authentifizierung ist das Subjekt autorisiert entsprechend seiner Berechtigungen zu arbeiten.

IT-Sicherheit

Ziel der IT-Sicherheit ist die Verfügbarkeit der Daten, Dienste und Anwendungen zu gewährleisten, sowie die Integrität und Vertraulichkeiten der Daten sicher zu stellen.

Hierzu benötigen wir ein Verständnis für die Begriffe,

- Gefahr, Bedrohung, Gefährdung
- Schwachstelle
- Angriff
- Schadensszenario
- Risiko

Gefahr

Eine Gefahr ist ein Sachverhalt, bei dem ohne konkreten zeitlichen, räumlichen oder personellen Bezug bei ungehindertem Ablauf des zu erwartenden Geschehens in absehbarer Zeit mit hinreichender Wahrscheinlichkeit ein Schaden für ein schutzwürdiges Gut eintreten wird.

Beispiele hierfür sind (ohne besonderen Bezug zur IT-Sicherheit):

- Beispiel: Hochwasser
  (Gefahr für Leib und Leben, finanzieller Verlust)
- Beispiel: Pocken (Gefahr für Leib und Leben)

Bedrohung

Eine Bedrohung ist eine Gefahr mit zeitlichem, räumlichem oder personellem Bezug zu einem Schutzziel.

Kurz: Bedrohungen sind potentielle Gefahren

- Beispiel: Hochwasser ist eine Bedrohung für Leib und Leben von Menschen an der Nordsee
  (aber nicht in Darmstadt)
- Pocken sind eine Gefahr für Leib und Leben, aber keine Bedrohung
  (der Pockenerreger ist ausgestorben)

Gefährdung

Eine Gefährdung bezieht sich ganz konkret auf eine bestimmte Situation oder auf ein bestimmtes Objekt und beschreibt die Wahrscheinlichkeit, mit der eine potenzielle Gefahr (d.h. Bedrohung) zeitlich oder räumlich auftritt.

Anders ausgedrückt: Trifft eine Bedrohung auf eine Schwachstelle (z.B. technische oder organisatorische Mängel), so entsteht eine Gefährdung.

- Beispiel: bei zu niedrigen Deichen ist Hochwasser eine Gefährdung für Leib und Leben von Menschen an der Nordsee

Gefährdungskategorien

Gefährdungen finden sich üblicherweise in folgenden Kategorien:

- Höhere Gewalt (z.B. Hochwasser, Blitzeinschlag, globaler Stromausfall)
- Technische Fehler (z.B. defekte Datenträger, Ausfall einer Datenbank)
- Fahrlässigkeit (z.B. Nichtbeachtung von Sicherheitsmaßnahmen, ungeeigneter Umgang mit Passwörtern)
- Organisatorische Mängel (z.B. fehlende oder unzureichende Regelungen, nicht erkannte Sicherheitsvorfälle)
- Vorsätzliche Handlungen (z.B. Abhören und Manipulation von Leitungen, Schadprogramme, Diebstahl)

Angriff

Ein Angriff bezeichnet einen unautorisierten Zugriff bzw. Zugriffsversuch auf ein IT-System oder eine Information.

Technische Angriffe lassen sich in zwei Kategorien unterteilen:

- Passive Angriffe: Zielen auf Informationsgewinnung (Schutzziel Vertraulichkeit)
  z.B. durch Abhören von Datenleitungen
- Aktive Angriffe: Zielen auf Informationsveränderung (Schutzziel Integrität und Verfügbarkeit)
  z.B. Vortäuschen einer falschen Identität, um Zugriff auf ein System zu erhalten

Schadensszenario

Das Brechen der definierten Schutzziele (erfolgreicher Angriff auf ein IT-Systeme durch Ausnutzen einer Schwachstelle) kann unterschiedliche Schäden verursachen.

Üblich ist die Einteilung in folgende Schadensszenarien:

- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Innen- oder Außenwirkung
- Finanzielle Auswirkungen

Risiko I

Ein Risiko ist das Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses und dessen Konsequenz, bezogen auf die Abweichung des gesteckten Zieles.

In Bezug auf IT-Sicherheit, das Produkt aus

- Wahrscheinlichkeit dafür, dass ein Schutzziel gebrochen wird, und
- Höhe des Schadens, der sich daraus ergibt

Die Bestimmung der Risiken hilft bei der Priorisierung umzusetzender Maßnahmen

Risiko II

Eintrittswahrscheinlichkeit und Schadenshöhe lassen sich nur schwer quantifizieren.

- Eintrittswahrscheinlichkeit: Welche Mittel ein Angreifer einsetzt
  - hängt von seiner Motivation ab
  - ist nicht nur abhängig von finanziellen Gewinnaussichten, sondern teilweise auch vom persönlichen Ergeiz (z.B. Whistleblower)
- Schadenshöhe: Abschätzung, welche Folgen ein Angriff hat
  - hängt von der konkreten Institution ab
  - meist sind mehrere Schadensszenarien betroffen

Risiko III

$$\text{Risiko} = \text{Eintrittswahrscheinlichkeit} \cdot \text{Schadenshöhe}$$

Folgende Vereinfachung
(nicht quantitative, sondern qualitative Bewertung):

- Klassifiziere Eintrittswahrscheinlichkeit in niedrig (1), mittel (2), hoch (3)
- Klassifiziere Schadenshöhe in niedrig (1), mittel (2), hoch (3)
- Werte für das Risiko: 1 (unbedeutend) bis 9 (kritisch)

Rechtliche Rahmen

IT-Sicherheit sollte nicht nur im Eigeninteresse einer Institution umgesetzt werden.

Vielfach fordern Gesetze die Umsetzung geeigneter IT-Sicherheitsmaßnahmen, z.B.:

- Bundesdatenschutzgesetz und Datenschutzgesetze der Bundesländer
- Datenschutz-Grundverordnung

Datenschutz

Mit Datenschutz wird der Schutz personenbezogener Daten vor Missbrauch durch Dritte bezeichnet.

- Die Privatsphäre jedes Einzelnen soll geschützt werden.
- Rechtlicher Ausgangspunkt ist das Grundrecht auf informationelle Selbstbestimmung.
- Grundidee ist, dass der Einzelne die Möglichkeit haben soll, selbst zu bestimmen, wer bei welcher Gelegenheit welche Informationen über ihn erhält.

Bundesdatenschutzgesetz

Grundpfeiler des BDSG sind die Prinzipien

- Datenvermeidung und Datensparsamkeit: bei der Datenverarbeitung dürfen nur so viele personenbezogene Daten gesammelt werden, wie für die jeweilige Anwendung unbedingt notwendig sind.
- Das allgemeine Verbot der Verarbeitung personenbezogener Daten: grundsätzlich dürfen personenbezogene Daten nur mit Einwilligung der Betroffenen oder aufgrund gesetzlicher Gestattung verarbeitet werden.
- Es setzt die Datenschutzrichtlinie um, die durch die Datenschutz-Grundverordnung aufgehoben/ ersetzt werden.

Datenschutz-Grundverordnung

Gemeinsamen Datenschutzrahmen in der Europäischen Union (seit dem 25. Mai 2018)

- Die DSGVO ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden.
- Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Privacy by Design

Entwickelt in den 90er Jahren von Ann Cavoukian (Information & Privacy Commissioner der Kanadischen Provinz Ontario)

Grundidee:

- Rechtsvorschriften allein sind nicht ausreichend für die Gewährleistung von Datenschutz

Hierfür wurden sieben Grundprinzipien aufgestellt.

Privacy by Design: Sieben Grundprinzipien

1. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe
2. Datenschutz als Standardeinstellung
3. Der Datenschutz ist in das Design eingebettet
4. Volle Funktionalität
5. Durchgängige Sicherheit - Schutz während des gesamten Lebenszyklus
6. Sichtbarkeit und Transparenz - Für Offenheit sorgen
7. Die Wahrung der Privatsphäre der Nutzer - nutzerzentrierte Gestaltung

Privacy by Design: Wettbewerbsvorteil

Werden solche Produkte von den NutzerInnen honoriert?

- Für Datenschutz und IT-Sicherheit interessierte sich lange Zeit nur eine Minderheit
- Seit Bekanntwerden der massiven Überwachungsprogramme der US-amerikanischen und britischen Geheimdienste ändert sich das
- US-amerikanische Firmen sehen einen klaren Wettbewerbsnachteil durch die Verpflichtung, mit den Geheimdiensten zusammenzuarbeiten

Bewertung von IT-Sicherheit I

- Zur Beurteilung der Sicherheit von IT-Systemen existieren allgemein anerkannte Vorgehensmodelle und Kriterienkataloge
- Diese Vorgehensmodelle und Kriterienkataloge erlauben unterschiedlicher Systeme, die eine ähnliche Funktionalität besitzen, hinsichtlich ihrer Sicherheit vergleichen zu können
- Kriterienkataloge dienen dazu Vertrauen in die Wirksamkeit von IT-Sicherheitsfunktionen von IT-Systemen zu schaffen
- An Hand einer Prüfung auf Basis der Kriterienkataloge (Evaluierung), wird die Wirksamkeit nachgewiesen und mit einem entsprechenden Zertifikat von einer offiziellen Stelle bestätigt

Bewertung von IT-Sicherheit II

- Diese internationale Normung Common Criteria (CC) (www.commoncriteriaportal.org/) ist eine anerkannte gemeinsame Grundlage für Bewertungen der IT-Sicherheit
- CC ist im ISO Standard 15408 "Evaluation criteria for IT security" festgelegt

Vorteile:

- Komponenten oder Systeme müssen NICHT in verschiedenen Ländern mehrfach bewertet und zertifiziert werden

Bewertung von IT-Sicherheit III

- Das grundsätzliche Paradigma der CC ist die Trennung der Betrachtung von
  Funktionalität und *Vertrauenswürdigkeit*
- Es erfolgt durch die Kriterien keine Vorgabe, dass
  - eine bestimmte Funktionalität umgesetzt werden muss
  - eine bestimmte Funktionalität mit einer bestimmten Vertrauenswürdigkeit geprüft werden muss
- Beide Aspekte werden zu Beginn der Evaluation des Produkts in den Sicherheitsvorgaben eines allgemeinen Schutzprofils definiert

Bewertung von IT-Sicherheit IV

- Common Criteria-Zertifikate werden in Deutschland vom BSI als *"ein amtlich bestätigter Nachweis der Sicherheitsleistung eines Produktes"* ausgestellt (in den USA ist die NSA für die Evaluierung nach Common Criteria zuständig)
- Bestandteil des Zertifizierungsverfahrens ist eine technische Prüfung, die von einer vom BSI anerkannten Prüfstelle durchgeführt werden kann
- Das BSI bestätigt mit der Ausstellung des Zertifikates, dass die Prüfstelle korrekt geprüft hat
- Dazu wird dem BSI der Prüfbericht von der Prüfstelle übergeben, die wiederum vom BSI geprüft wird