
Datenschutz und Datensicherheit DuD 24/12 (2000) 704-710.

# Gliederung und Systematisierung von Schutzzielen in IT-Systemen

Hannes Federrath, Andreas Pfitzmann

TU Dresden, Fakultät Informatik

**Dr. Hannes Federrath**
Wissenschaftlicher Mitarbeiter an der TU Dresden, Fakultät Informatik, Forschungsschwerpunkt ist die Sicherheit in verteilten Systemen
E-Mail: federrath@inf.tu-dresden.de

**Prof. Dr. Andreas Pfitzmann**
TU Dresden, Fakultät Informatik, Forschungsschwerpunkt ist technischer Datenschutz durch verteilte Systeme
E-Mail: pfitza@inf.tu-dresden.de

## Kurzfassung

Dieser Beitrag gliedert und systematisiert mögliche Schutzziele in IT-Systemen, d. h. Anforderungen an den Schutz von Menschen, die sich in Kommunikationsnetzen "bewegen". Jede der vorgestellten Gliederungen beleuchtet verschiedene Seiten des gleichen Problems unter bestimmten Gesichtspunkten und schafft dadurch ein Modell für den Begriff der Sicherheit.

## 1 Motivation

Seit vielen Jahrzehnten wird über zur Sicherheit und Zuverlässigkeit von IT-Systemen nachgedacht, geforscht und an Lösungen entwickelt. Dabei stiegen die Anforderungen an sichere Systeme mit der technischen Leistungsfähigkeit und den Anwendungsbereichen der Systeme. Im klassischen zentralisierten Rechenzentrum spielten und spielen Fragen der Verfügbarkeit, Ausfallsicherheit, und Fehlertoleranz von Systemen und Daten eine große Rolle. Der Trend zu verteilten Systemen führt hingegen zu einer stärkeren Beachtung der Kommunikationssicherheit, d. h. der Sicherung von Daten z. B. gegen Verfälschung, Manipulation und unbefugtes Mitlesen während der Übertragung.

In einem komplexen IT-Systemen, wie es unsere heutigen und zukünftigen Kommunikationsnetze sind, handeln verschiedene Subjekte (Organisationen, Personen). Sie können dabei nicht nur kooperieren, sondern auch (kommunizieren), konkurrieren (z. B. um Betriebsmittel), sabotieren (z. B. Kommunikation behindern, stören, blockieren, lahmlegen), fingieren (z. B. Identitäten vortäuschen, Daten verändern), ) oder abhören (z. B. bespitzeln, lauschen) und vieles mehr.

Um Funktion und Eigenschaften eines Systems beim Auftreten der Konfrontation mit von nicht erwünschten Ereignissen aufrecht zu erhalten, sind also daher Schutzmaßnahmen erforderlich.

IT-Systeme (einschließlich der Übertragungsstrecken) müssen dazu gegen unbeabsichtigte Fehler und Ereignisse (z. B. höhere Gewalt, technische Fehler, Fahrlässigkeit, Programmierfehler, Verschleiß, Havarien) und beabsichtigte Angriffe (z. B. Abhören, Manipulation und Zerstören von Informationen, aber auch von Software und Hardware) von außen (z. B. Hacker oder Terroristen mit Sprengstoff) und innen (z. B. Administratoren, Programmierer) gesichert werden.

Im Englischen werden die Begriffe *security* für den Schutz vor beabsichtigten und *safety* für den Schutz vor unbeabsichtigten Ereignissen verwendet (Tabelle 1).

| Security<br>Schutz gegen beabsichtige Angriffe | | Safety<br>Schutz gegen unbeabsichtigte Ereignisse | |
|---|---|---|---|
| Vertraulichkeit: | Anonymität<br>Unbeobachtbarkeit<br>Unverkettbarkeit<br>Pseudonymität<br>Abhörsicherheit<br>Sicherheit gegen unbefugten Gerätezugriff | Verfügbarkeit: | Funktionssicherheit<br>Technische Sicherheit |

| | | | |
|---|---|---|---|
| Integrität: | Unabstreitbarkeit<br>Übertragungsintegrität<br>Abrechnungssicherheit<br>Übertragungssicherheit | Sonstige Schutzziele: | Maßnahmen gegen hohe Gesundheitsbelastung |
| Verfügbarkeit: | Ermöglichen von Kommunikation | | |
| Abwehr der Angriffe gegen Insider und Outsider | | | |

Tabelle 1: Abgrenzung von security und safety

Die Sicherheitsanforderungen können für die handelnden Subjekte unterschiedlich sein: So will beispielsweise eEin Netzbetreiber und Dienstanbieter will entstandene Kommunikationskosten abgedeckt wissen und fordert daher Schutz gegen vor unberechtigten unberechtigtem Zugang zum System. Ein Teilnehmer hingegen möchte Dienste möglicherweise anonym nutzen und er möchte nichtverhindern, daß dass Kommunikationsinhalte an Dritten zur Kenntnis gelangen.

Eine weitere wichtige Forderung ist, dass dDie zugesicherten Eigenschaften eines Systems müssen von jedermann überprüft werden können. Ähnlich wie die Sicherheitsanforderungen der Subjekte unterschiedlich sind, fällt die Art der Überprüfungsmöglichkeiten sehr unterschiedlich aus:

- Der *Hersteller* eines Systems will z. B.beispielsweise eine unabhängige zertifizierte Zertifizierung der Sicherheit des von ihm vertriebenen Systems. Zur Zertifizierung ist wird eine genaue Beschreibung Katalog nötig, der die Sicherheitseigenschaften des Systems genau beschreibtbenötigt. Das zwingt den Hersteller zum Offenlegen innerer Mechanismenvon Teilen der Architektur seines Systems. Dies kann Trotzdem hat er jedoch ein mit seinem berechtigtes berechtigten Interesse an der Wahrung von Firmengeheimnissen konfligieren.
- Der *Nutzer* von IT-Systemen will beispielsweise sichere Systeme, ohne hinter *alle* Mechanismen schauen zu *müssen*. Er will eine eingängige, aber seriöse Beurteilung durch Experten, z. B. als verbale High-Llevel-Beschreibung, die insbesondere auf seine Interessen eingeht, z. B. auf korrekte Abrechnung und oder Datenschutz.

Dabei ist zu beachten, wer (Hersteller oder Nutzer) der Initiator für das Design eines sicheren Systems ist, denn dieser stellt i.d.R. auch den Katalog an Sicherheitsanforderungen auf. Ein Nutzer mag sich auf eine Expertise einer unabhängigen Stelle verlassen. Er wird aber nie ganz sicher sein können, daß die zugesicherten Eigenschaften und nur diese durch das System erbracht werden, es sei denn, er kann die Einhaltung der Anforderungen selbst überprüfen (teilnehmerüberprüfbarer [Daten-] Schutz).

# 2 Beschreibungs- und EinteilungsGliederung nachder Schutzzielenmöglichkeiten für Sicherheit

Im folgenden sollen die Schutzziele für sichere IT-Systeme gegliedert werden, d. h. Anforderungen an den Schutz von Menschen, die mit Hilfe von IT-Systemen kommunizieren.

Im Verlauf der Darstellung soll jeweils eine Verfeinerung und Präzisierung von Begriffen vorgenommen werden. Wir beginnen mit eher groben und umgangssprachlichen Formulierungen und wollen Schritt für Schritt exakter werden.

## 2.1 Subjektive Sicht der Nutzer von IT-Systemen

Fragt man den (potentiellen) Benutzer eines IT-Systems nach seinen wichtigsten Anforderungen an sichere Systeme, stehen die Zugriffskontrolle ("Gewährleistung des ausschließlich autorisierten Datenzugriffs", [FlLJ_98, S. 479]) und Mißbrauchskontrolle Missbrauchskontrolle ("Ich kann darauf vertrauen, daß dass der Online-Dienstanbieter mit meinen Daten keinen Mißbrauch Missbrauch betreibt.", [LBDF_98, S.105f]) an vorderster Stelle.

Überträgt man dieses Ergebnis auf die zur Verfügung stehenden technischen Mechanismen in offenen verteilten Systemen, so sind offenbar die Zugangs- und Zugriffskontrolle und ferner die Verschlüsselung (im Sinne des Schutzes der übertragenen Daten vor unberechtigtem Zugriff) aus Nutzersicht am wichtigsten. Dies deckt sich schließlich auch mit den bisher am weitesten

entwickelten und verbreiteten Schutzmechanismen.

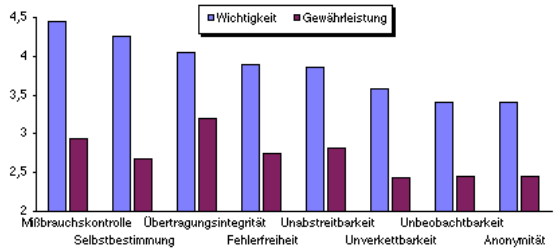


Abbildung 1. Subjektive Wichtigkeit und Gewährleistung von Sicherheitskriterien (nach [LBDF_98, S. 106f]); Skala: 1 (unwichtig bzw. sehr wahrscheinlich nicht gewährleistet) bis 5 (sehr wichtig bzw. sehr wahrscheinlich gewährleistet)

## 2.2 Ereignisse sollen geschehen / dürfen nicht geschehenarten

Ganz grob kann die Funktionalität von IT-Systemen eingeteilt werden nach Ereignissen, die geschehen sollen, und solchen, die nicht geschehen dürfen. Man kann die Ereignisse, die geschehen sollen, auch als die *Primärfunktionalität* des IT-Systems bezeichnen.

Beispielsweise sollen für einen berechtigten Benutzer Daten rechtzeitig und korrekt verfügbar sein ("soll geschehen"). Umgekehrt gesagt, soll niemand in der Lage sein, Aktionen unberechtigt auszuführen ("darf nicht geschehen").

Die Gliederung der Ziele eines IT-Systems nach Ereignissen, die geschehen sollen und solchen, die nicht geschehen dürften, ist nicht beschränkt auf Schutzziele. Sie ist insofern zwar umfassend, aber noch schlecht zu handhaben.

## 2.3 "Klassische" Schutzziele

Bereits in den frühen 80er Jahren findet man eine Dreiteilung von Schutzzielen [VoKe_83]:

- Schutz der Vertraulichkeit (confidentiality),
- Schutz der Integrität (integrity),
- Schutz der Verfügbarkeit (availability).

Der Vorteil dieser Dreiteilung ist ihre Einprägsamkeit. Sie ist jedoch nicht eindeutig bezüglich. der Bedeutung der Begriffe. So kann der "Schutz der Vertraulichkeit" sowohl Nachrichteninhalte umfassen, aber auch den Schutz der Vertraulichkeit des Sendens, Empfangens oder der Kommunikation an sich. Gleiches gilt für den "Schutz der Integrität", der sich nicht nur auf Nachrichteninhalte, sondern ebenfalls auf die Zuordnung von Nachrichteninhalten zu ihrem Absender beziehen kann, aber auch auf korrekte (unfälschbare und unabstreitbare) Rechnungen. Integrität ist dann jedoch sehr weit gefaßt gefasst., und es Ddaher bietet sich eine Verfeinerung an, wie sie in den folgenden Abschnitten erfolgen wird.

[Scha_92] führt neben den drei klassischen Schutzzielen noch den Schutz der Originalität (keine unbefugte Duplikation von Informationen) ein. Diese Forderung ist

- einerseits ein Teil von Vertraulichkeit, d. h. dem Schutz vor (unbefugter Kenntnisnahme von Informationen) und
- andererseits ein Teil von Integrität, d. h. dem Schutz vor einer Verbreitung von (Information nicht unter falscher Identität bzw. Urheberschaft verbreiten zu können, soweit ein Urheber überhaupt bekannt sein soll).

Nach [Eber_98] muß muss man zwischen der Sicherstellung der Zuverlässigkeit einerseits und der Gewährleistung der Informations- und Kommunikationssicherheit, d. h. der informationstechnischen Sicherheit und des Datenschutzes) andererseits unterscheiden:

- Sicherstellung der Zuverlässigkeit:
  - *Fehlertoleranz*: Fähigkeit der eines SystemeSystems, bei Auftreten von Fehlern und Störungen selbständig so zu reagieren, daß dass die Funktionalität des Gesamtsystems aufrecht erhalten oder zumindest möglichst wenig beeinträchtigt wird.
  - *Bedienbarkeit*: Die Bedienbarkeit Nutzung eines der Systeme Systems muß muss auch für Benutzer sichergestellt möglich sein, die keine Experten sind.
- Gewährleistung der Informations- und Kommunikationssicherheit (bzw. der informationstechnischen Sicherheit und des Datenschutzes):

- *Vertraulichkeit* gespeicherter und transportierter Informationen: Gespeicherte und transportierte Daten sind zu sichern vor dem Zugriff durch Unbefugte zu sichern.
- *Unbeobachtbarkeit*: Kommunikationsvorgänge sollten durchführbar sein, ohne daß dass Dritte davon erfahren.
- *Anonymität* des Zugriffs und der Kommunikation: Bei Bedarf sollten Benutzer die Möglichkeit haben, auch ohne Preisgabe ihrer Identität Informationen zu erhalten und kommunizieren zu können.
- Gewährleistung der *Unversehrtheit* (Integrität) von Daten: Daten dürfen nicht unerlaubt und unbemerkt verändert werden.
- Gewährleistung der *Authentizität von Absendern und Empfängern* von Daten: Es muß muss verhindert werden, daß dass sich jemand als ein anderer ausgibt.

Mit besonderem Fokus auf den Schutz der Verfügbarkeit kann man unterscheiden:

- Verfügbarkeit des Basissystems, auf dem den Benutzern konkrete Dienste für die Nutzer erbracht werden, deren Vertraulichkeit und Integrität umfassend zu schützen ist. Verfügbarkeit wird in diesem Kontext gewissermaßen als Voraussetzung für die Erbringung von Diensten auf dem Basissystem gesehen.
- Verfügbarkeit der Diensterbringung selbst. Hierbei ist Verfügbarkeit nicht auf die generische Funktionalität des Basissystems, sondern auf die konkrete Diensterbringung bezogen. Beispielsweise bedeutet Verfügbarkeit der konkreten Diensterbringung bei einem Kommunikationssystem, daß dass die gesendete Nachricht den Empfänger tatsächlich erreicht, während Verfügbarkeit der generischen Funktionalität bedeutet, daß dass weiterhin Nachrichten mit gewisser Wahrscheinlichkeit zum Empfänger transportiert werden.

Mit besonderem Fokus auf den Schutz der Integrität lassen sich ebenfalls Schutzziele gliedern:

- "schwache" Integrität, d. h. das Erkennen, daß dassob etwas gefälscht wurde,
- "starke" Integrität, d. h. schwache Integrität und zusätzlich die Möglichkeit, herausfinden zu können, wer bzw. was den Verlust der Integrität herbeigeführt hat,
- "stärkste" Integrität, d. h. das System arbeitet ein stets korrektes und integres Arbeiten eines Systemser, bei dem . Es kommt also es gar nicht erst zu einem Integritätsverlust kommt. Eine solche Forderung bedeutet eigentlich, Integrität und Verfügbarkeit in einem zu erreichen. (Obwohl in IT- Systemen prinzipiell nicht zu erreichen, ist diese stärkste Definition von Integrität die, die beispielsweise in den europäischen ITSEC-Kriterien, Version 1.2, Juni 1991, gegeben wird.)

Führt man diesen Gedanken weiter, ließe sich Sicherheit lediglich durch zwei Schutzziele beschreiben, nämlich:

- Vertraulichkeit und
- totale Korrektheit,

wobei vorausgesetzt wird, daß dass stets ausreichend Betriebsmittel zur Verfügung stehen, um alle (legalen) Anfragen an das System zu befriedigen.

### 2.4 Mehrseitige Sicherheit

Die bisherigen Gliederungen berücksichtigen vor allem, was geschützt werden soll, jedoch in geringerem Maß, welche Beteiligten zu schützen sind.

Bei der dem Sicherheitsziel einer mehrseitigen Sicherheit geht es insbesondere darum, den bzw. die "Schwächeren" bei der Kommunikation zu stärken. Die Grundidee dabei ist, daß dass jeder Nutzer selbst entscheiden können soll, wem er vertraut, d. h. wem bzw. welchem Gerät er seine Daten anvertraut. Sobald ein System vermeidbares Vertrauen erzwingt, erfüllt es die Anforderungen mehrseitiger Sicherheit nicht.

Mehrseitige Sicherheit bedeutet die Berücksichtigung der Sicherheitsanforderungen aller beteiligten Parteien. Die Schutzziele werden beispielsweise in vier Hauptbereiche gegliedert (nach [RaPM_97]):

- Vertraulichkeit (confidentiality)
  - Schutz der Nachrichteninhalte vor allen Instanzen außer ausser dem Kommunikationspartner
  - Schutz von Sender und/oder Empfänger
  - Schutz Verbergen der Identität vor dem Kommunikationspartner: (*Anonymität*)

    - Schutz vor Dritten: (*Unbeobachtbarkeit* der Kommunikation)
    - Schutz Geheimhaltung des momentanen Aufenthaltsorts, auch gegenüber dem Netzbetreiber
- Integrität (integrity)
    - Schutz der Nachrichteninhalte
- Zurechenbarkeit (accountability)
    - Empfänger soll gegenüber einem Dritten nachweisen können, daß dass Instanz x die Nachricht y gesendet hat
    - Absender soll Absenden einer Nachricht mit korrektem Inhalt beweisen können, möglichst sogar den Empfang
    - Niemand kann dem Dem Netzbetreiber können keine Entgelte für erbrachte Dienstleistungen vorenthalten werden – zumindest erhält (z. B. indem der Netzbetreiber bei Dienstinanspruchnahme entsprechende Beweismittel erhält). Umgekehrt kann der Netzbetreiber nur für korrekt erbrachte Dienstleistungen Entgelte fordern.
- Verfügbarkeit (availability)
    - Netz ermöglicht Kommunikation zwischen allen Partnern, die dies wünschen (und denen es nicht verboten ist).

Bezogen auf die oberste Gliederungsebene wurde eine Verfeinerung der Integrität vorgenommen, und zwar nach Nachrichtenintegrität und Zurechenbarkeit. Ansonsten werden in den Schutzzielen der mehrseitigen Sicherheit einige Aspekte explizit genannt, die in andere Gliederungen hinein interpretiert werden könnenimplizit enthalten können.

Die Umsetzung mehrseitiger Sicherheit besitzt eine technische und eine organisatorische Komponente. Auf der organisatorischen Seite wird mehrseitige Sicherheit z. B. durch die Verteilung von Information auf nicht als Angreifer zusammenarbeitende Instanzen realisiert, auf der technischen Ebene z. B. durch Offenlegen des Entwurfs von Soft- und Hardware mit der Möglichkeit zur Inspektion durch jeden Interessierten (ein wichtiger Sicherheitsaspekt von *Open Source*). Wie und nach welchen Kriterien so etwas ablaufen kann, ist in [Rann_98] beschrieben. Zu Open Source sei [KöKP_00] empfohlen.

Die Philosophie der Überprüfung durch jeden Interessierten, also auch durch den Nutzer selbst, wird auch "Teilnehmerüberprüfbarkeit" genannt. Handelt es sich um Datenschutzinteressen, deren Einhaltung ein Teilnehmer selbst überprüfen können soll, wird dies "teilnehmerüberprüfbarer Datenschutz" [Pfit_90] genannt. Diesen teilnehmerüberprüfbaren Datenschutz kann man als Teil der mehr und mehr in Mode kommenden "Datenschutzfreundlichen Technologien" (*privacy enhancing technology*) auffassen. Beispiele hierfür sind:

- Schutz der Nutzer vor Erstellung von Kommunikationsprofilen (im Internet, z. B. [GoRS_96] oder im ISDN, z. B. [Pfit_90]),
- Schutz gegen die Erstellung von Bewegungsspuren im Mobilfunk, z. B. [Fede_99],
- Schutz gegen Verfolgung von Zahlungstransaktionen im elektronischen Zahlungsverkehr, z. B. [Chau_89, PWP_90].

## 2.5 Berücksichtigung des Kommunikationsumfelds

Die Schutzziele mehrseitiger Sicherheit differenzieren nur die Integritätseigenschaften (i1, z1-z3), nicht jedoch die Vertraulichkeitseigenschaften. So könnten ebenfalls die Vertraulichkeitseigenschaften untergliedert werden (c1 in die eine und c2, c3 in die andere Spalte), vgl. Tabelle 2. Ebenfalls differenziert werden kann Verfügbarkeit in Verfügbarkeit von Inhalten und die Umfeldeigenschaft *Erreichbarkeit von Subjekten*, beispielsweise Menschen.

| | Inhalte | Umfeld |
|---|---|---|
| Erwünschtes leisten | Integrität | Zurechenbarkeit<br><br>Abrechenbarkeit |
| | Verfügbarkeit | Erreichbarkeit |
| Unerwünschtes verhindern | Vertraulichkeit | Anonymität<br><br>Unbeobachtbarkeit |

Tabelle 2: Gliederung nach zu schützenden Inhalten und dem Umfeld der Kommunikation [FePf1_98, FePf_99, WoPf_99]

Integrität, Zurechenbarkeit, Abrechenbarkeit, Verfügbarkeit und Erreichbarkeit werden üblicherweise positiv formuliert, d. h. es wird jeweils gesagt, was geschehen soll. Diese Schutzziele sollen also *das Erwünschte leisten*. Die Schutzziele Vertraulichkeit, Anonymität und Unbeobachtbarkeit werden üblicherweise negativ formuliert, z. B. Unbefugte sollen Inhalte, Identitäten und Kommunikationsereignisse nicht erfahren. Diese Schutzziele sollen also *Unerwünschtes verhindern*.

Eine interessante Frage ist, ob auf die Formulierung einer Kategorie von Schutzzielen vollkommen verzichtet werden kann:

- Auf "Unerwünschtes verhindern" kann verzichtet werden, wenn alles implizit verboten ist, was nicht explizit erwünscht ist. Dann wären beispielsweise Daten, für die nicht explizit gesagt ist, daß dass sie einer bestimmten Person verfügbar sein sollen, vor dieser Person vertraulich zu halten.
- Umgekehrt kann auf "Erwünschtes leisten" verzichtet werden, wenn alles implizit erwünscht ist, was nicht explizit unerwünscht ist. Dann müßten müssten beispielsweise Daten, für die nicht explizit gesagt ist, daß dass sie gegenüber einer bestimmten Person vertraulich bleiben sollen, dieser Person verfügbar sein.

Hinter der Unterscheidung nach "Erwünschtes leisten" und "Unerwünschtes verhindern" steckt auch, daß dass es

- Bedrohungsmodelle gibt, die explizit formulieren, wer von wem als Angreifer angenommen wird, und
- Vertrauensmodelle, die formulieren, wer wem vertraut.

Im *Bedrohungsmodell* (als Modell für "Unerwünschtes verhindern") wird dann ein System gebaut, das gegen die Bedrohungen (bzw. unterstellten Angreifer) hilft. Falls im Bedrohungsmodell eine Bedrohung vergessen wurde, ist das System u.U. unsicher.

Im *Vertrauensmodell* (als Modell für "Erwünschtes leisten") wird dagegen formuliert, wer wem vertraut. Alle anderen werden folglich als Angreifer gesehen, gegen die das zu entwickelnde System schützen mußmuss. Auf diese Weise kann man keinen Angreifer vergessen, man kann lediglich zu vertrauensselig gewesen sein.

In einer geschlossenen Welt mag der Verzicht auf die Formulierung einer Kategorie von Schutzzielen theoretisch möglich sein. In einer offenen Welt – oder wenn es auf eine knappe und übersichtliche Formulierung von Schutzzielen ankommt – sind aus unserer Sicht beide Kategorien unverzichtbar. Außerdem Ausserdem geben die Abläufe, die weder explizit erwünscht noch explizit unerwünscht sind, den Freiraum, der verschiedene Implementierungen ermöglicht und damit für Effizienz und faktische Implementierbarkeit der Systeme wichtig ist. Nicht zuletzt aus diesem Grund wird geht man bei praktischen Systemen sehr häufig von Bedrohungsmodellen ausgegangen, die mit dem Bekanntwerden neuer Angriffe nachgebessert werden, während Vertrauensmodelle häufig einen "Alles-oder-Nichts-Ansatz" verfolgen, der entsprechend aufwendig und teuer ist.

Das Ordnungssystem von Tabelle 2 ist offen für weitere Schutzziele: Ergänzt man in der Spalte Inhalte *Verdecktheit* von Nachrichteninhalten (etwa durch Steganographie) als zu Unbeobachtbarkeit von Kommunikation korrespondierendes Schutzziel sowie *Unstörbarkeit* der Inhalte (etwa durch direct sequence spread spectrum Übertragungstechnik) als duale Eigenschaft zu Verdecktheit, so ergibt sich Tabelle 3.

| | Inhalte | Umfeld |
|---|---|---|
| Erwünschtes leisten | Integrität<br><br>Unstörbarkeit | Zurechenbarkeit<br><br>Abrechenbarkeit |
| | Verfügbarkeit | Erreichbarkeit |
| Unerwünschtes verhindern | Vertraulichkeit<br><br>Verdecktheit | Anonymität<br><br>Unbeobachtbarkeit |

Tabelle 3: Gliederung nach zu schützenden Inhalten und dem Umfeld der Kommunikation erweitert um zusätzliche Schutzziele

Das Ordnungssystem von Tabelle 2 läßt lässt sich weiter verfeinern bezüglich der Schutzziele,

die Kommunikationsumstände betreffen. Dabei entstehen formalere Begriffe für den Schutz der jeweiligen Funktion, d. h.:

- Primärfunktion eines Kommunikationsnetzes: z. B. Inhalte austauschen; das bedeutet, die Inhalte müssen geschützt werden, daraus folgt
- Sekundär schützenswerte Informationen: Niemand soll das Kommunizieren beobachten können.

Die genannte Aufteilung orientiert sich dabei vor allem an der Sicht des Benutzers eines Systems. Interessanterweise repräsentiert diese Diese Sicht entspricht jedoch nur zum Teil die der Sicht eines Netzbetreibers. Dieser möchte z. B. Geld verdienen mit der Bereitstellung eines Kommunikationsmediums. Das bedeutet, er benötigt primär Funktionen, mit denen es möglich ist, erbrachte Dienstleistungen unabstreitbar ihren Verursachern zuzuordnen.

Damit wird aber die aus der Sicht der Benutzer sekundäre Schutzfunktion der Zurechenbarkeit zu der primären des Netzbetreibers. Zusätzlich werden die sekundären Schutzfunktionen bezüglich der Vertraulichkeit, d. h. Anonymität und Unbeobachtbarkeit, zum potentiellen Problem, da der Netzbetreiber beispielsweise primär eine unabstreitbare Abrechnung wünscht.

Somit stellt die in Tabelle 4 genannte Aufteilung nur eine ganz bestimmte Sicht dar, nämlich z. B. die eines Benutzers, dem es primär darauf ankommt, daß dass Daten vor Manipulation und unbefugter Kenntnisnahme geschützt sind (Primärfunktion), der darüber hinaus möglichst sicher sein will, daß dass die Nachrichten ihren Absendern zurechenbar sind, aber möglichst niemand mitbekommt, mit wem (Anonymität) und ob er kommuniziert (Unbeobachtbarkeit). Schließlich möchte der Benutzer natürlich, daß dass die in Rechnung gestellten Dienstleistungen korrekt sind (*Abrechenbarkeit*).

| | Primärfunktion | Sekundärfunktion | Tertiärfunktion |
|---|---|---|---|
| Aktionen sollen geschehen | **Integrität** der ausgetauschten Inhalte | **Zurechenbarkeit** von Inhalten zu Kommunikationspartner | Zurechenbarkeit aller Kommunikation, um Kommunikationskosten abzurechnen, d. h. **Abrechenbarkeit** |
| | **Verfügbarkeit** von Daten und Prozessen | | |
| Aktionen dürfen nicht geschehen | **Vertraulichkeit** der ausgetauschten Inhalte | Vertraulichkeit der eigenen Identität, d. h. **Anonymität**<br>Vertraulichkeit ob eigene Kommunikation, d. h. **Unbeobachtbarkeit** | Vertraulichkeit der **Netzauslastung** |
| | **Unverfügbarkeit** von Daten und Prozessen | | |

Tabelle 4: Gliederung nach Primär-, Sekundär- und Tertiärfunktionen aus der Sicht der Benutzer eines Systems

In dieser Gliederung lassen sich auch Schutzziele einordnen, die so heute (noch) gar nicht formuliert werden. So könnte z. B. ein Netzbetreiber sekundär wünschen, daß dass niemand außer ihm selbst mitbekommt, wie hoch die Auslastung seines Netzes ist, d. h. wieviel Kommunikation er vermittelt, welche Kunden er hat etc., also Schutzfunktionen bezüglich der Unbeobachtbarkeit seiner Primärfunktion.

Eine Erweiterung der Einträge von Tabelle 4 um die Schutzziele von Tabelle 3 und einige weitere ergibt Tabelle 5.

| | Primärfunktion | Sekundärfunktion | Tertiärfunktion |
|---|---|---|---|
| Aktionen sollen geschehen | **Integrität** der ausgetauschten Inhalte<br><br>**Unstörbarkeit der Inhalte** | **Zurechenbarkeit** von Inhalten zu Kommunikationspartner<br><br>**Unstörbarkeit der Sender-/Empfängerzuordnung** | Zurechenbarkeit aller Kommunikation, um Kommunikationskosten abzurechnen, d. h. **Abrechenbarkeit**<br><br>Zurechenbarkeit der **Sicherheitspolitikfestlegung** |

| | | | |
|---|---|---|---|
| | **Verfügbarkeit** von Daten und Prozessen | **Erreichbarkeit** des Kommunikationspartners | **Durchsetzbarkeit** von Zusagen des Kommunikationspartners |
| Aktionen dürfen nicht geschehen | **Vertraulichkeit** der ausgetauschten Inhalte<br><br>**Verdecktheit** der<br><br>Ausgetauschten Inhalte | Vertraulichkeit der eigenen Identität, d. h. **Anonymität**<br><br>Vertraulichkeit ob eigene Kommunikation, d. h. **Unbeobachtbarkeit** | Vertraulichkeit der **Netzauslastung** |
| | **Unverfügbarkeit** von Daten und Prozessen | **Ungestörtheit** des Kommunikationspartners | |

Tabelle 5: Gliederung nach Primär-, Sekundär- und Tertiärfunktionen aus der Sicht der Benutzer eines Systems erweitert um zusätzliche Schutzziele

Mit zunehmender Verfeinerung der Schutzziele, wie etwa im Verlauf dieses Papiers von Kapitel 2.2 über Kapitel 2.3 und Kapitel 2.4 zu Tabelle 2 und Tabelle 5 entwickelt, werden generische Schutzziele zunehmend anwendungsspezifisch konkretisiert. Dies geschieht nicht nur im Verlauf dieses Papiers, sondern (siehe auch in den die Tabellen 2, 3, 4 und 5: jeweils spaltenweise von links nach rechts. Je nach Anwendung sind die rechten Spalten weitgehend zu ändern, während die linke Spalte nahezu unverändert bleiben dürfte).

## 2.6 OSA-Modell

Die bisher vorgestellten Gliederungen bezogen sich meist auf verschiedene Parteien (Benutzer, Betreiber, Hersteller etc.) im Zusammenhang mit von IT-Systemen. In der vorangegangenen Gliederung war auch schon die Rede von Aktionen, die geschehen sollen oder auch nicht, damit ein Schutzziel erreicht wird.

| | **Vertraulichkeit** | **Integrität** | **Verfügbarkeit** |
|---|---|---|---|
| **Objekt (O)** | Vertraulichkeit | Integrität | Verfügbarkeit |
| **Subjekt (S)** | Anonymität | Identifizierung, Authentizität | Erreichbarkeit |
| **Aktion (A)** | Unbeobachtbarkeit | Zurechenbarkeit | Durchführbarkeit |

Tabelle 6: Gliederung nach objekt-, subjekt- und aktionsbezogenen Schutzzielen

Konsequenterweise könnte man nun versuchen, alle Dinge, die geschützt werden sollen, in drei Kategorien einzuteilen:

- Objekte, die geschützt werden sollen; : dies werden meist Daten sein;
- Subjekte, die deren Rechte oder Interessen geschützt werden sollen; : hierbei handelt es sich um Menschen;
- Aktionen, die geschützt bleiben erfolgen sollen; : hierbei soll eine Aktion gegenüber vor einem oder allen anderen Subjekten geschützt sein.

In der Tabelle 6 wird dies jeweils für die drei klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit versucht.

## 2.7 Kooperationsmodell

Insbesondere bei der effizienten Realisierung von Sicherheitsfunktionen spielt die Frage, wer wem vertraut, eine besondere Rolle. So lassen sich mache Schutzziele nur erreichen, wenn die Kommunikationspartner sich gegenseitig vertrauen. So ist es beispielsweise nicht möglich, ein System zu bauen, bei dem eine Nachricht vor allen Außenstehenden vertraulich bleibt und sie nicht einmal ein böswilliger Kommunikationspartner weitererzählen kann. Bei anderen Schutzzielen wird dagegen explizit vorausgesetzt, daß dass die Kommunikationspartner sich mißtrauenmisstrauen. Beispielsweise ist der Empfänger einer digital signierten Nachricht (Schutzziel Zurechenbarkeit) unter bestimmten Umständen in der Lage, jedem einem Dritten zu beweisenbelegen, daß dass der Sender (und nur er) die Nachricht signiert hat.

Die in der Tabelle 7 dargestellte Gliederung versucht nun zuzuordnen, welche Ziele jeweils miteinander erreicht werden müssen ("kooperativ") und welche auch gegeneinander bzw. mit unterschiedlichen Interessen ("nicht kooperativ") erreicht werden können.

In vielen Fällen kommt es vor, daß dass zwei Kommunikationspartner Schutzziele auch gegen einen Dritten (oder sogar gegen alle Außenstehenden) habendurchsetzen möchten. Deshalb wird jeweils noch einmal danach unterschieden, ob Dritte bezüglich des Schutzzieles beteiligt sind. Das wird insbesondere dann klar, wenn ein Schutzziel nicht erreicht bzw. verletzt wird. Beispiele sind:

- Wenn eine Kommunikation zwischen zwei Kommunikationspartnern A und B nicht zustande kommt, weil das Netz nicht verfügbar ist, haben A und B ein gemeinsames (kooperatives) Interesse gegenüber dem Netzbetreiber, der die Kommunikation ermöglichen soll.
- Wenn A und B unbeobachtbar kommunizieren wollen, d. h. niemand außer ausser A und B ist in der Lage festzustellen können soll, daß dass A und B miteinander kommunizieren, dann wünschen sie dieses Schutzziel gegen alle Dritten. Unbeobachtbarkeit erreichen zu wollen, ist unabhängig davon, ob A und B sich ver- oder mißtrauenmisstrauen. Falls sie sich mißtrauen misstrauen und gegenseitig ihre Identitäten verbergen wollen, wünschen sie zusätzlich Anonymität.

## Zusammenfassung

| Kommunikationspartner agieren ... | | | |
|---|---|---|---|
| ... kooperativ bzw. sie vertrauen sich | | ... *nicht* kooperativ bzw. mißtrauen misstrauen sich | |
| ... ohne Dritte | ... auch gegen Dritte | ... ohne Dritte | ... auch gegen Dritte |
| Integrität der Inhalte | Verfügbarkeit | Zurechenbarkeit | Abrechenbarkeit |
| Vertraulichkeit der Inhalte | Unbeobachtbarkeit | Anonymität | Unbeobachtbarkeit |

Tabelle 7: Gliederung nach dem Grad an Kooperationswilligkeit und -bedarf

Dieses Papier unternimmt den Versuch, verschiedene Gliederungen von Schutzzielen miteinander in Beziehung zu setzen. Die Zusammenstellung wird dabei stets unvollständig gebleieben sein. Jedoch lassen sich verschiedene Strukturen erkennen, die teilweise wiederkehren. Hierzu gehören zum Beispiel die Gegensätze "Erwünschtes leisten" (bzw. "Aktionen sollen geschehen") versus. "Unerwünschtes verhindern" (bzw. "Aktionen dürfen nicht geschehen") sowie die Frage nach dem Vertrauen oder Mißtrauen Misstrauen der beteiligten Instanzen.

Es ist nicht verwunderlich, daß dass sich im Spannungsfeld von Sicherheit Gegensätze auftun, sobald die Beteiligten divergierende Schutzziele haben:

- **Verfügbarkeit ist das Dual Gegenstück zu Vertraulichkeit**. Auf Inhalte bezogen ist dies einleuchtend: Verschlüsselte Inhalte sind für Angreifer nicht verfügbar.
- **Integrität ist das Dual Gegenstück zu MißinformationFehlinformation**. Fehlinformation soll eine bei Geheimdiensten beliebte Sache sein, die normalerweise in zivilen Systemen nicht betrachtet wird.(Fehlinformation ist bei Geheimdiensten üblich, wird aber normalerweise für zivile Systemen nicht betrachtet.)
- **Zurechenbarkeit ist das Dual Gegenstück zu Anonymität**. In diesem Problemfeld sind z. B. Verfahren zur Pseudonymität angesiedelt.
- **Abrechenbarkeit ist das Dual Gegenstück zu Unbeobachtbarkeit durch den Diensterbringer**.
- **Unstörbarkeit ist das Dual zu Verdecktheit.** Dieses Problem spielt z. B. beim Design von Watermarking-Systemen eine große Rolle.

Es zeigt sich, daß dass die ursprüngliche Bedeutung der Begriffe Vertraulichkeit, Integrität und Verfügbarkeit mehr und mehr erweitert wird, was letztlich mit den gestiegenen Sicherheitsanforderungen an die IT-Systeme zu erklären ist.

## Danksagung

Ein Großteil der niedergeschriebenen Gedanken wurde innerhalb des Kollegs "Sicherheit in der Kommunikationstechnik" der Gottlieb-Daimler- und Karl-Benz-Stiftung entwickelt. Ein Dank geht an alle Beteiligten, die die Diskussion mit ihrer Sicht der Welt mit in die Diskussion gebracht bereichert haben. Insofern sehen sich die Autoren dieses Papiers eher als Editoren und denn als Urheber mancher Gedanken. Eine Liste der beteiligten Institutionen kann unter [SiKo_99] abgerufen werden. Extern "getestet" wurden diese Gedanken im Workshop "Begriffsbildung" auf der Fachtagung VIS'99 in Essen. Allen Diskutanten sei herzlich gedankt.

## Literatur


Chau_89 David Chaum: Privacy Protected Payments — Unconditional Payer and/or Payee Untraceability. SMART CARD 2000: The Future of IC Cards, Proceedings of the IFIP WG 11.6 International Conference; Laxenburg (Austria), 19.-20. 10. 1987, North-Holland, Amsterdam 1989, 69-93.

Eber_98 Jörg Eberspächer: Digital, multimedial, global — Telekommunikation für die Menschen des 21. Jahrhunderts. Bayerischer Monatsspiegel 3/98 — Abenteuer Kommunikation, 44-48.

Fede_99 Hannes Federrath: Sicherheit mobiler Kommunikation. DuD Fachbeiträge, Vieweg, Wiesbaden 1999.

FePf_99 Hannes Federrath, Andreas Pfitzmann: Stand der Sichereitstechnik. in: Kubicek et. al. (Hrsg.): "Multimedia@Verwaltung", Jahrbuch Telekommunikation und Gesellschaft 1999, Hütig, 124-132.

FePf1_98 Hannes Federrath, Andreas Pfitzmann: Die Rolle der Datenschutzbeauftragten bei der Aushandlung von mehrseitiger Sicherheit. in: Helmut Bäumler (Hrsg.): "Der neue Datenschutz" — Datenschutz in der Informationsgesellschaft von morgen. Luchterhand, Berlin 1998, 166—172.

FlLJ_98 Michael Florian, Rolf Lührs, Malte Lehmann-Jessen: Zukunftseinschätzungen zur Sicherheit in der Kommunikationstechnik — Ergebnisse aus der Ladenburger TeleDelphi-Befragung. in: Günter Müller, Kurt-Herrmann Stapf (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik (Bd.2), Addison-Wesley-Longman 1998, 465-494.

FÜV_95 Fernmeldeverkehr-Überwachungsverordnung - FÜV: ENTWURF einer Verordnung über die technische Umsetzung von Überwachungsmaßnahmen des Fernmeldeverkehrs in Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind (Stand 02.05.95). FoeBuD e.V., 1995.

GoRS_96 David M. Goldschlag, Michael G. Reed, Paul F. Syverson: Hiding Routing Information. in: R. Anderson (Hrsg.), Information Hiding, LNCS 1174, Springer-Verlag, Berlin 1996, 137-150.

KöKP_00 Kristian Köhntopp, Marit Köhntopp, Andreas Pfitzmann: Sicherheit durch Open Source? Chancen und Grenzen. Datenschutz und Datensicherung DuD 24/9 (2000) 508-513.

LBDF_98 Ernst-Dieter Lantermann, Brigitte Ballhause, Andreas Döring, Dagmar Fuhr, Irene Schicker-Ney: Werte, subjektive Sicherheit und Nutzung moderner Kommunikationstechniken. in: Günter Müller, Kurt-Herrmann Stapf (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik (Bd.2), Addison-Wesley-Longman 1998, 99-117.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Heidelberg 1990.

Pfit8_93 Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen. Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

Rann_98 Kai Rannenberg: Zertifizierung mehrseitiger IT-Sicherheit. DuD-Fachbeiträge, Vieweg, Wiesbaden 1998.

RaPM_97 Kai Rannenberg, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige IT-Sicherheit. in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 21-29.

Scha_92 Ingrid Schaumüller-Bichl: Sicherheitsmanagement — Risikobewältigung in informationstechnologischen Systemen. BI Wissenschaftsverlag, Mannheim 1992.

SiKo_99 Kolleg "Sicherheit in der Kommunikationstechnik" der Gottlieb-Daimler- und Karl-Benz-Stiftung. Im Internet verfügbar unter http://www.iig.uni-freiburg.de /dbskolleg/.

VoKe_83 Victor L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols. ACM Computing Surveys 15/2 (1983) 135-171.

WoPf_99 Gritta Wolf, Andreas Pfitzmann: Empowering Users to Set their Protection Goals. in: Günter Müller, Kai Rannenberg (Ed.): Multilateral Security in Communications, Addison-Wesley-Longman 1999, 113-135.