DuD
Datenschutz und Datensicherheit

Taxonomie und Modellbildung in der Informationssicherheit

Hartmut Pohl

Im Bereich der Sicherheit der Informationsverarbeitung finden sich im internationalen Bereich eine ganze Reihe von präzise abgegrenzten und durch Konvention gefestigten Benennungen und Definitionen, die die Begriffswelt von safety und security integrieren. Hartmut Pohl stellt einen auf dieser Grundlage erarbeiteten Vorschlag für eine deutsche Begriffsnorm und für ein Zusammenwachsen der bisher getrennten Begriffswelten safety und security zur Diskussion. Die Begriffe werden darin in einen strukturellen Zusammenhang gebracht und es werden ein Schichtenmodell für die Informationssicherheit und ein generisches Bedrohungs-/Schadenmodell vorgeschlagen.

Prof. Dr. Hartmut Pohl
Fachbereich Informatik, Fachhochschule Bonn-Rhein-Sieg.

E-Mail: Hartmut.Pohl@sang.net

Zusammenfassung

Normen legen nicht nur technische Anforderungen fest, sondern definieren auch (zugehörige) Begriffe [DIN EN ISO 1990]. Im Bereich der Sicherheit der Informationsverarbeitung ist bisher keine grundlegende – wesentliche Begriffe definierende – deutsche oder internationale Norm veröffentlicht. Allerdings finden sich im internationalen Bereich eine ganze Reihe von präzise abgegrenzten und durch Konvention gefestigte Benennungen und Definitionen, die die Begriffswelt von safety und security integrieren.

Sie bilden damit eine Grundlage für eine zu erarbeitende deutsche Begriffsnorm und für ein Zusammenwachsen der bisher getrennten Begriffswelten safety und security.

1 Schadenursachen

Bei den Ursachen für Schäden der Informationsverarbeitung können höhere Gewalt und Fahrlässigkeit sowie Missbrauch unterschieden werden [Pfitzmann 2004]. Meist wird suggeriert, dass diese Ursachen im Schadensfall identifiziert werden können [ISO/ IEC 2002b]. Allerdings ist häufig nur schwer oder gar nicht entscheidbar, ob ein absichtliches Vorgehen vorliegt oder nur ein fahrlässiges oder grob fahrlässiges; daher sollen die Ursachen hier nicht weiter betrachtet werden.

2 Unterscheidung: safety und security

In der internationalen Literatur wird zwischen security und safety unterschieden:

- **Safety**: Zustand eines Systems, in dem Maßnahmen zum Schutz (zur Vermeidung von Schäden) wirksam sind.

In diesem Zustand ist das System frei von – vom Betrieb der Hardware oder Software ausgehenden – Gefahren, die dem System oder (außerhalb:) der Umwelt[1] drohen – gekennzeichnet durch Begriffe wie Betriebssicherheit und Arbeitssicherheit [DIN EN 1999, ISO/IEC TR 1996, Shirey 2000]. Safety wird auch einschränkend als Funktionssicherheit des IT–Systems bezeichnet [Eckert 2003].

- **Security**: Zustand eines IT–Systems[2], in dem Maßnahmen zum Schutz des IT–Systems wirksam sind [Shirey 2000]; Absicherung Informationen verarbeitender Systeme (IV-Systeme[3]): Informationssicherheit (information security) [ISSO 1996, Eckert 2003].

Damit erscheint safety als übergreifender, die Umwelt (soziotechnisches System: Gesellschaftliche, unternehmerische und politische Strukturen) beinhaltender Begriff.

IV-Systeme bestehen aus IT–Systemen als technischen Systemen sowie den zugehörigen organisatorischen und personellen Systemen. IT-Systeme stellen damit eine Untermenge der IV-Systeme dar [DIN 44 300]. Die Absicherung der IT-Systeme wird als IT-Sicherheit bezeichnet (Computer Security) [ISSO 1996, Shirey 2000]. Detaillierter definiert [ISO/IEC 2000]: Zustand eines IT–Systems, in dem vom Betreiber, Anwender oder Sicherheitsbeauftragten festgelegte Sachziele erreicht werden (s. u.). Vereinfachend lässt sich damit

- **Safety** als Schutz der Rechnerumgebung vor ‚unerwünschtem Verhalten' des Rechners (Output) bezeichnen [DIN EN 1999, ISO/IEC TR 13335-1 1996, Shirey 2000] und

[1] Z. B. Mautsystem, Gesundheitstelematik, automat. Operateur, Stellwerk der Eisenbahn.

[2] Funktionseinheit zur Verarbeitung von Daten nämlich zur Durchführung mathematischer, umformender, übertragender und speichernder Operationen. [DIN 44 300]

[3] Das IT-System zusammen mit der technischen Infrastruktur (Stromversorgung, Klimatisierung, Vernetzung etc.), den unterstützenden Personen (Bedienung, Programmierung etc.) sowie den zugehörigen organisatorischen Regelungen.

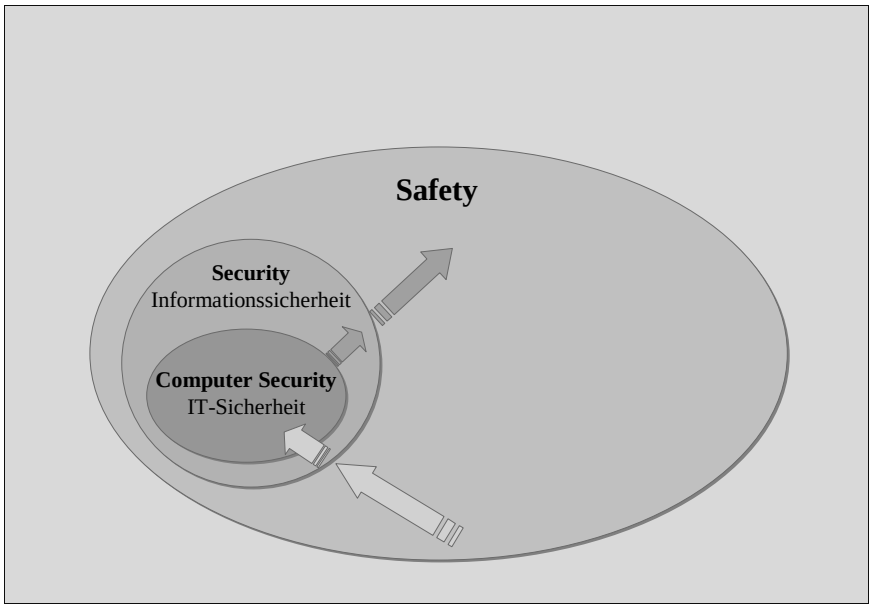

Abb. 1: Zusammenhang von Safety, Security und Computer Security[4]

- **Security** als Schutz des Rechners vor ‚unerwünschtem Verhalten' der Rechnerumgebung (Input) [ISO/IEC 2000, Shirey 2000] bezeichnen.

Die Inhalte der Informationssicherheit sind in Abb. 2 dargestellt.

Im Folgenden werden die Aspekte der Informationssicherheit behandelt.

3 Schichtenmodell Informationssicherheit

Die Überlegungen der Informationssicherheit zielen auf ein vertrauenswürdiges System, in dem Folgendes verhindert oder doch erschwert bzw. angestrebt wird:

- Unberechtigte Nutzung von Informationssystemen (Vertraulichkeit, Integrität)
- Verfügbarkeit von Daten[5] und Prozessen
- Verbindliche Verarbeitung (zurechenbare und nicht-rückweisbare Kommunikation – non-repudiation)

Es sollen berechtigte Zugriffe unterstützt und unberechtigte wie Kenntnisnahme und Veränderung von Daten (Nutzdaten, Programme, Systemparameter), sowie die Täuschung während der gesamten Verarbeitung (Speicherung und Übertragung) erschwert werden.

3.1 Sachziele der Informationssicherheit

Als sachliche Ziele der Informationssicherheit – auch als Schutzziele und Eigenschaften bezeichnet [Eckert 2003, ISO/IEC 2002 b, ISO/IEC 2003, Wolf, Pfitzmann 2000] – werden im engeren Sinne die folgenden vier gesehen [ISO/IEC DIS 14980]. Jedenfalls sind diese vier Sachziele unabhängig und orthogonal (z. B. können Daten verfügbar, müssen aber nicht integer sein).

- **Vertraulichkeit** (confidentiality): Informationen sind nur für Berechtigte zugreifbar [ISO/IEC 2382, ISO/IEC 7498, ISO/IEC 2003, Shirey 2000].
- **Integrität** (integrity): Genauigkeit und Vollständigkeit von Informationen und Verfahren (Validität) [ISO/IEC 7498-2, ISO 8732, ISO/IEC 2382-14, ISO/IEC 9797 2nd ed., ISO/IEC TR 13335-1, ISO/IEC 2002b, ISO/IEC 2003, Shirey 2000]. Daten werden nicht unberechtigt verändert, gelöscht oder zerstört.
  Synonym Validität: Übereinstimmung eines Werts hinsichtlich Genauigkeit, Korrektheit und Vollständigkeit mit dem tatsächlichen Sachverhalt. Die Daten sind richtig (fehlerfrei), regelgemäß (z. B. formatiert) und auf dem aktuellen Stand [Canadian System Security Centre 1993, ISO 17799, ISO 7498-2, ISO 8732, ISO/IEC 9797 2nd ed., ISO/IEC TR 13335-1].
  - Übereinstimmung, Konsistenz (consistency): Grad der Übereinstimmung zwischen dem tatsächlichen Wert eines Objekts (einer Variablen) und dem verarbeiteten Wert; Widerspruchsfreiheit. [Carnegie Mellon 2004, IEEE 1990]
  - Genauigkeit (accuracy): Quantitative Messung der Fehlergröße [Carnegie Mellon 2004]. Anzahl fehlerhafter Daten bedingt durch fehlerhafte Programmierung oder Darstellung [ISO TC 215 EG 4].
  - Korrektheit (correctness): Grad der Fehlerfreiheit [Carnegie Mellon 2004, IEEE 1990] (z. B. eines Programms).
  - Vollständigkeit (completeness): Geschlossenheit, Ganzheit [Carnegie Mellon 2004].

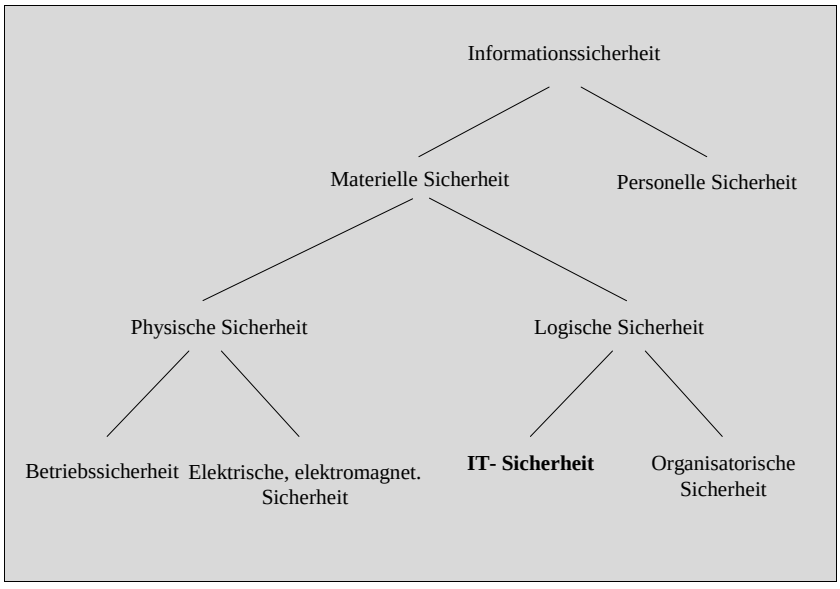

Abb. 2: Inhalte der Informationssicherheit

[4] ⇒:= wirkt auf'. Die Pfeile kennzeichnen die Auswirkungen von IT-Systemen über IV-Systeme auf die Umwelt und umgekehrt.

[5] Der Begriff Daten beinhaltet i. S. der Norm DIN 44300 auch Programme.

Schicht	Zustand	Verhalten des Systems
4	go	System- und Anwendungsprogramme sicher und korrekt
3	fail operational	System fehlertolerant ohne Leistungsminderung
2	fail soft	Sicherer Systembetrieb, verminderte Leistung
1	fail safe	Nur Systemsicherheit
0	fail unsafe	Unvorhersehbares Systemverhalten

Abb. 3: Fehlerverhalten fehlertoleranter Systeme

- Plausibilität (plausibility): Programmgesteuerte Kontrolle von Daten zur Erreichung sinnvoller (verständlicher, einleuchtender, begreiflicher) Daten und zur Vermeidung unsinniger Daten. [Duden 2001].

- **Verfügbarkeit** (availability): Objekte sind bei Bedarf durch Berechtigte zugreifbar und nutzbar [DIN 40 041, DIN 40 042, ISO/IEC 2382, ISO/IEC 7498, ISO/IEC 9126, ISO/IEC 2003, NTG 3004, Shirey 2000].

Die folgenden Komponenten werden gesehen:

- Zuverlässigkeit (reliability): Eigenschaft eines Systems Zuverlässigkeitsforderungen während vorgegebener Zeitspannen bei vorgegebenen Anwendungsbedingungen zu erfüllen [DIN 40 041, DIN 55 350]. Funktionskontinuität – quantitativ gekennzeichnet durch Überlebenswahrscheinlichkeit oder Ausfallwahrscheinlichkeit [Görke 1989].
- Fehlertoleranz (fault tolerance): Eigenschaft eines Systems spezifische Funktionen mit einer begrenzten Zahl fehlerhafter Subsysteme zu erfüllen [Laprie 1992] (Fehlererkennung, -diagnose und -behandlung) mit u. a. den folgenden Ausfallmodi:

  Fail safe: Ein Ausfall überführt das System in einen sicheren Zustand – möglicherweise mit dem Verlust der gesamten Funktionalität [Shirey 2000].

  Fail soft: Bei Ausfällen wird ein sicherer, reduzierter Betrieb aufrechterhalten [Bretthauer 2003, Shirey 2000]. Bei der graceful degradation werden die Funktionen des Systems schrittweise reduziert.

Das Verhalten von Systemen lässt sich wie folgt darstellen [Görke 1989]:

- Robustheit (robustness): Eigenschaft eines Systems, eine bestimmte Mindestmenge an Funktionen der Gesamtfunktionalität abzuwickeln (graceful recovery) [ISSO 1996].
- Wiederherstellbarkeit (recovery): Eigenschaft eines Systems, von fehlerhafter zu korrekter Leistungserbringung zu gelangen [Laprie 1992] und die betroffenen Daten wiederzugewinnen.

Verfügbarkeit wird von einer weiteren (nicht notwendigen) Eigenschaft unterstützt.

- Flexibilität (flexibility): Eigenschaft eines Systems, unterschiedliche Funktionen auszuführen. Anpassungsfähigkeit.

- **Verbindlichkeit** (liability): Zurechenbare (nicht-rückweisbare), rechtsverbindliche Kommunikation [UK online, ISO/IEC 2382-08, ISO 7498-2, ISO/IEC TR 13335-1, ISO/IEC 2003, Shirey 2000].

Grundlage für die Verbindlichkeit sind die beiden folgenden Begriffe.

- Authentizität (authenticity): Ein Subjekt oder Objekt ist echt, entspricht den Behauptungen [ISO/IEC TR 13335-1, ISO/IEC 2002b, ISO/IEC 2003]. Vergleiche aber:
  - Authentisieren: Ein Subjekt weist seine Identität nach[6] [Pohl 1989].
  - Authentifizieren: Eine behauptete Identität verifizieren und ggf. auch beglaubigen[7]. Teil des zweistufigen Verfahrens Identifizieren, Authentifizieren [ISO/ IEC 2002b, Pohl 1989]. Authentifizierung (authentication).
- Beherrschbarkeit (governance): Darunter können die folgenden Aspekte eines Systems verstanden werden: Steuerung (controlling), (eindeutige) Identifizierung (identification) der Handlungsfolgen, Zurechenbarkeit (accountability) der ergriffenen Handlungen.

Damit erscheint Beherrschbarkeit – neben der Authentizität als ein wesentlicher Teil der Verbindlichkeit – als Begriff der safety, der den Schwerpunkt auf den Verursacher und die Auswirkungen seiner Aktivitäten legt.

- Revisionsfähigkeit (auditability)

Eigenschaft eines Systems, die Funktionsweise lückenlos nachvollziehen und damit feststellen zu können, wer, wann, welche Daten in welcher Weise verarbeitet hat. Prüfende Wiederdurchsicht [Duden 2001].

Zusammenfassend lässt sich der in Abb. 4 grafisch dargestellte Begriffsbaum für IT-Sicherheit aufstellen.

IT-Sicherheit synonym Vertrauenswürdigkeit beinhaltet die Sachziele der Informationssicherheit und wird synonym benutzt mit dem Begriff Verlässlichkeit (dependability) [Laprie 1992]. Bei einigen Sachzielen kann ein unterschiedlich hohes

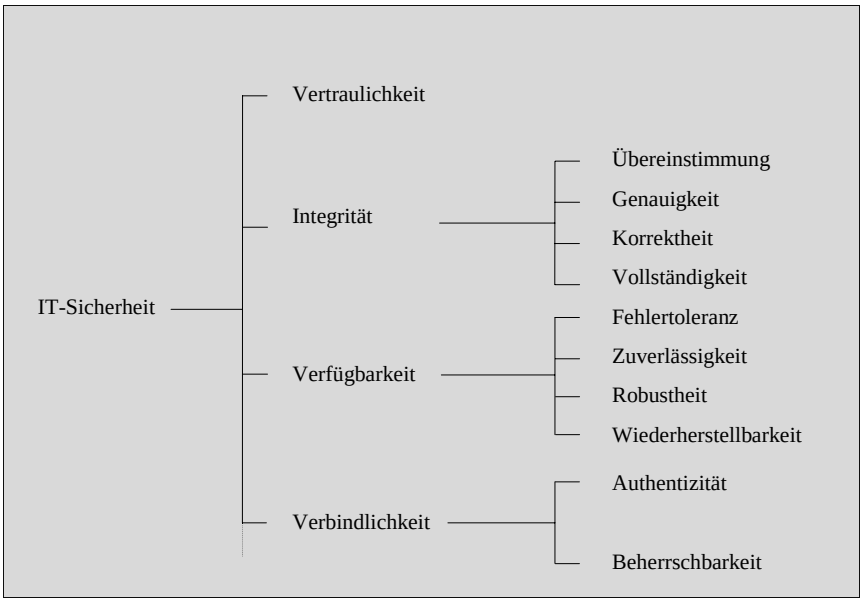

Abb. 4: Sachziele der IT-Sicherheit und Komponenten

[6] So authentisiert sich ein Bürger (nach Vorlage seines Personalausweises) durch den Authentikator ‚Fotografie' auf dem Ausweis – ggf. auch durch die aufgedruckte Unterschrift.

[7] Ein Notar beglaubigt bei Vorlage des Personalausweises und Prüfung auf Übereinstimmung von Fotografie und tatsächlichem Gesicht.

Sachziel	Anglo-amerikanischer Fachbegriff	Schutz gegen
Anonymität	anonymity	Identifizierung
Pseudonymität	pseudonymity	Namentliche Identifizierung
Unbeobachtbarkeit	untraceability	Protokollierung
Nicht-Vermehrbarkeit	non-propagation	'Viren'-Aktivitäten
Netz-Verfügbarkeit	net availability	Angriffe auf Netze
Transparenz	transparency	Fehlende Nachvollziehbarkeit

Abb. 5: Weitere mögliche Sachziele

Sicherheitsniveau erreicht werden (z. B. Verfügbarkeit) – andere Sachziele sind binär (z. B. Integrität). Weitere Sachziele können hinzukommen vgl. Abb. 5.

Nicht alle aufgeführten Sachziele sind unabhängig; vielmehr können sich einige verstärken (Unbeobachtbarkeit – Anonymität) und auch (zumindest partiell) gegenseitig ausschließen (Anonymität – Verbindlichkeit). Jedenfalls werden die relevanten Sachziele vom Benutzer in Abhängigkeit von der Nutzung des Informationssystems festgelegt; dies gilt auch für Kommunikationsteilnehmer zur Wahrung gegenseitiger Interessen (mehrseitige Sicherheit) [Wolf, Pfitzmann 2000].

3.2 Grundfunktionen

Der Einsatz von Grundfunktionen soll sicherstellen, dass nur Berechtigte auf Daten zugreifen. Subjekten werden – nach Identifizierung und Authentifizierung – Rechte zugewiesen; die Rechte werden im System verwaltet und geprüft. Da die Funktionen nicht vollständig sicher arbeiten, soll eine Protokollierung aller sicherheitsrelevanten Vorfälle Überprüfungen ermöglichen [Pfitzmann, Rannenberg 1993].

Grundfunktionen unterstützen ein Erreichen der Sachziele. Die folgenden Grundfunktionen sind relevant: Identifizierung/Authentifizierung, Rechteverwaltung, Rechteprüfung, Protokollierung und Auswertung [BSI 1989].

3.3 Mechanismen

(Sicherheits-)Mechanismen stellen ein implementiertes (algorithmisch fassbares) Lösungsprinzip zur Abdeckung von Grundfunktionen dar. Mehrere Mechanismen werden zu einer Sicherheitsmaßnahme zusammengefasst [BSI 1991, Fries 1993].

Mechanismen wie Passworte, Token, Biometrie, Policies, Kryptographie werden eingesetzt, um die Grundfunktionen technisch zu erreichen.

3.4 Modell

Daraus folgend lässt sich das Schichtenmodell in Abb. 6 formulieren [nach ZSI 1989, Dierstein 2002]. Zur Erreichung vertrauenswürdiger Systeme werden jeweils angemessene Sachziele der IT-Sicherheit ausgewählt, die auf Grundfunktionen und diese wiederum auf Mechanismen aufbauen.

Das Modell ermöglicht nach einer Auswahl und Festlegung der für ein IT-System notwendigen oder angemessenen Sachziele eine Festlegung der zur Erreichung der ausgewählten Sachziele notwendigen Grundfunktionen und die Auswahl der Mechanismen als implementierbare Funktionen zur Unterstützung der Grundfunktionen.

4 Bedrohung, Angriff, Schaden

Neben Bedrohungen durch höhere Gewalt und fahrlässigem oder grob fahrlässigem Handeln können beabsichtigte Angriffe auf IT-Systeme Ursache für Schäden sein.

Im Folgenden wird ein Modell entwickelt, das von den Bedrohungen bis zum Schaden reicht. Dargestellt wird das Modell als Zustandsdiagramm. Die möglichen Zustände werden erläutert. Die Zustandsübergänge sind in die Abbildungen eingetragen.

4.1 Höhere Gewalt-/Schadenmodell

Ein einfaches Modell der Auswirkungen höherer Gewalt ist das folgende.

Bedrohung (threat)
Mögliche unerwünschte oder unberechtigte Aktivitäten, die ein IT-System negativ beeinflussen können: Mögliche Verletzung der IT-Sicherheit und damit Ursache für ein unerwünschtes Ereignis [ISSO 1996, ISO/IEC 2382-08, ISO 7498-2, ISO/IEC TR 13335-1, ISO/IEC 1996, ISO/IEC 2002b, ISO/IEC 2003, Shirey 2000]. Bedrohungen werden unterschieden nach

- Höherer Gewalt,
- Fahrlässigkeit oder
- absichtlichem Vorgehen (Spionage oder Sabotage) wie Wirtschaftsspionage durch Mitbewerber und illegaler Technologietransfer.

Höhere Gewalt wirkt direkt auf das IT-System (vgl. Abb. 7). Früher wurden Bedrohungen – oder auch Grundbedrohungen – partiell im Sinne von Angriffsverfahren

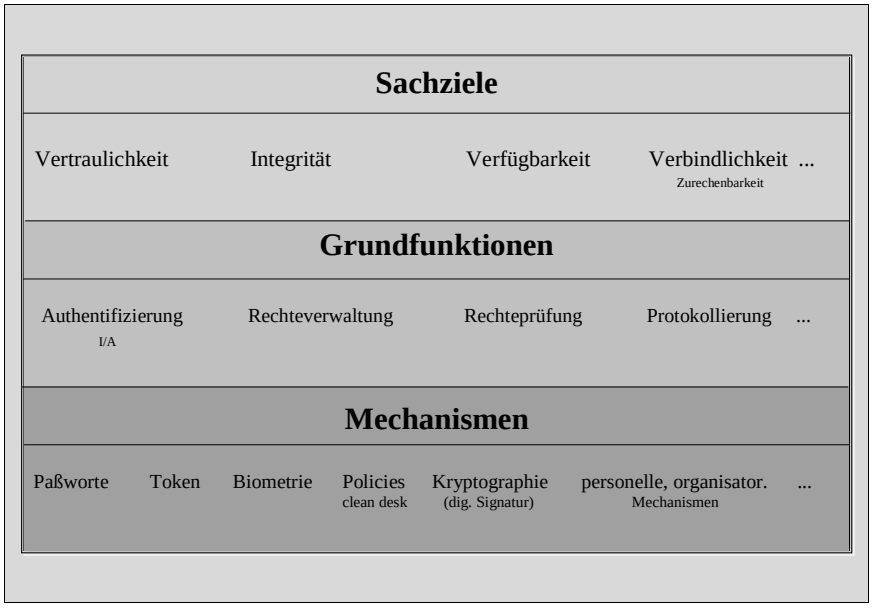

Abb. 6: Drei-Schichtenmodell der Informationssicherheit

oder Schaden verstanden[8] [Zentralstelle 1989, BSI 1991, BSI 2001]; der Begriff wird mittlerweile im hier dargestellten Sinne benutzt [BSI 2003].

Ereignis (event)
Tatsächliches Eintreten einer Bedrohung: Unglück, Unfall, Katastrophe.

Gefahr (danger)
Mögliches Eintreten einer Bedrohung gegen ein IT-System – unabhängig vom Vorhandensein eventueller Schwachstellen oder Sicherheitsmaßnahmen.

Risiko (risk)
Quantitative Bewertung der Möglichkeit einer Ausnutzung einer Schwachstelle und damit Möglichkeit der Schadensverursachung [ISO/IEC TR 13335-1, ISO/IEC 2002b, ISO/IEC 2003].

Auch: Verhältnis aus Eintritt eines Schadensereignisses und dem bei Ereigniseintritt zu erwartenden Schadensausmaß [DIN/IEC 880] sowie Kombination aus Eintrittswahrscheinlichkeit und Konsequenzen eines Ereignisses [ISO/IEC 2002a].

Sicherheitsmaßnahme – security measure
Sicherheitsmaßnahmen sind materielle oder personelle Maßnahmen (vgl. Abb. 2).

Schwachstelle (vulnerability)
Sicherheitsrelevante Fehler eines IT-Systems – speziell eines Mechanismus [ISO/IEC 2003, Shirey 2000]. Schwachstellen können meist auf Fehler zurückgeführt werden. Fehler können sporadisch oder permanent wirksam sein. Sie können erkannt oder nicht erkannt sein. Synonym Verwundbarkeit, Sicherheitslücke [ISO/IEC TR 13335-1, ISO/IEC 2003].

Schaden (damage)
Minderung des Werts eines Objekts. Allgemein werden materielle (Sach- und Personenschäden) und immaterielle Schäden (z. B. Schmerzen) unterschieden.

Materielle Schäden lassen sich auch mit dem Nicht-Erreichen von Sachzielen beschreiben: Dem Verlust der Verfügbarkeit, der Integrität, der Vertraulichkeit oder anderer Sachziele [BSI 2003]. Ein Schaden kann also sowohl im IT-System auftreten als auch außerhalb (Umwelt).

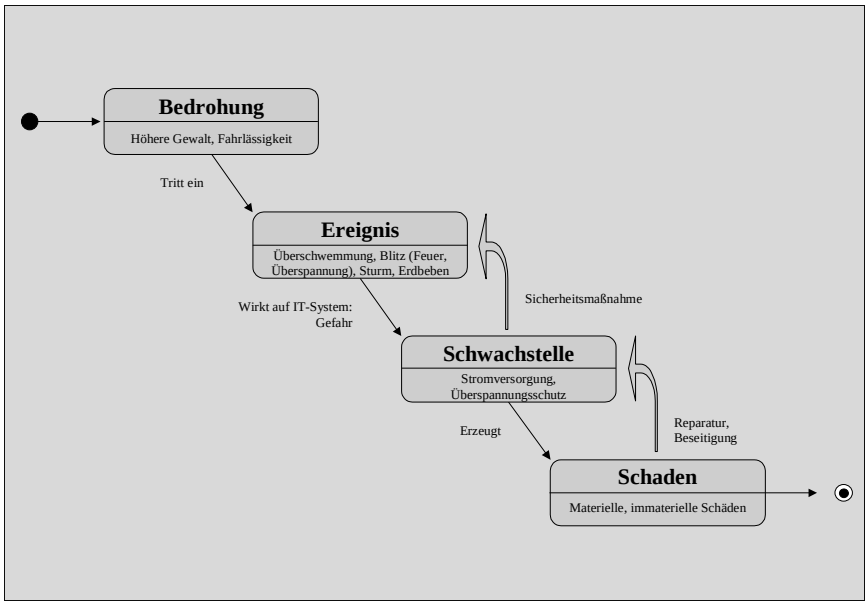

Abb. 7: Höhere Gewalt/Schadenmodell

4.2 Angriffs-/ Schadenmodell

Im Angriffs-/Schadenmodell haben die Zustände die folgende Bedeutung:

Bedrohung (threat)
Bei einer Bedrohung durch unberechtigte Interessen wie Mitbewerber, Mitarbeiter generiert ein entsprechend motivierter Täter unter Einsatz ausgewählter Angriffswerkzeuge einen Angriff gegen ein IT-System. Im Folgenden wird daher ein Angriffs-/ Schadenmodell als Zustandsdiagramm dargestellt. Die Zustände werden erläutert.

Angriff (attack)
Ein Angriff stellt eine versuchte oder gelungene – jedenfalls unerwünschte oder unberechtigte – Verletzung der Sicherheit dar. Der Erfolg eines Angriffs hängt ab von der Qualität der Schwachstelle, der Wirksamkeit von Sicherheitsmaßnahmen und der Angriffsstärke [ISO/IEC 2382-08]. Synonym: Intrusion. Ein Angriff setzt an einem Angriffspunkt (breach) an.

Angriffswerkzeug (attack tool)
Methoden und Werkzeuge zur Ausnutzung einer Schwachstelle eines Systems [ISSO 1996, ISO/IEC 15408].

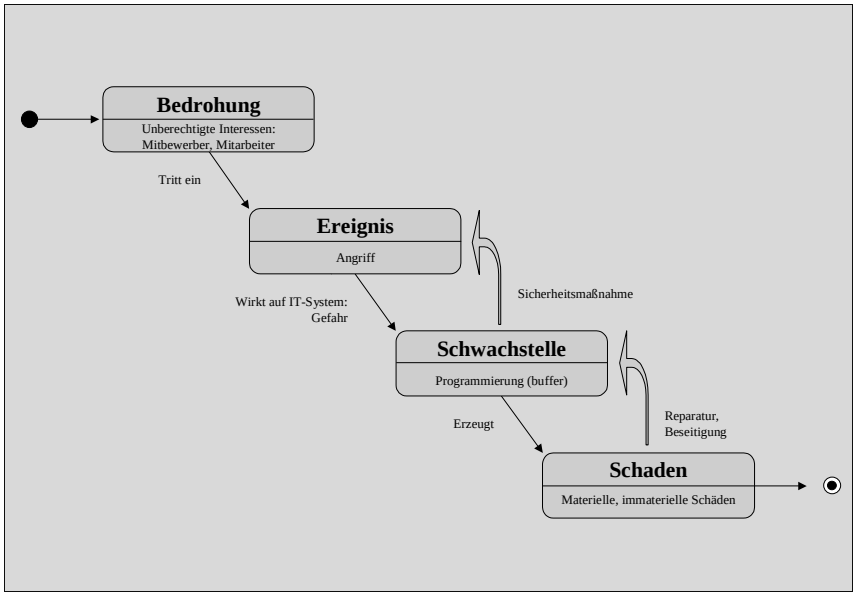

Abb. 8: Angriffs-/Schadenmodell

[8] ‚... klassische Bedrohungen des Verlusts der Verfügbarkeit von Daten und Dienstleistungen, Vertraulichkeit von Informationen, Unversehrtheit / Integrität von Daten ...'

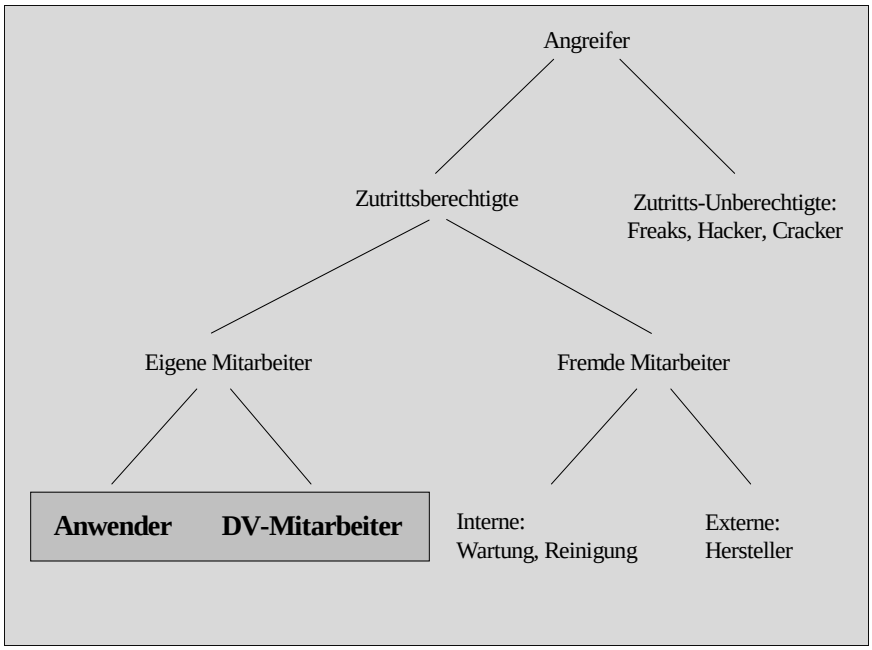

Abb. 9: Tätertypisierung

Täter, Motive (perpetrator, motives)
Als Täter kommen vor allem Zutrittsberechtigte (Innentäter) des angegriffenen Unternehmens oder der angegriffenen Behörde in Betracht [Computer Security Institute 2003]; das sind Mitarbeiter, die bereits Zugriffsrechte besitzen oder Außenstehende, die die Behörde oder das Unternehmen betreten dürfen, weil sie vertragsgemäß Aufgaben abwickeln. Oder es sind zwar Dritte, die aber von Mitarbeitern, die für den Angriff notwendigen sicherheitsrelevanten Informationen erhalten (vgl. Abb. 9).

Zur Motivation der Täter liegen unveröffentlichte begrenzte Untersuchungen vor. Die relevanten vier Motive sind:

- Spieltrieb.
- Geltungsbedürfnis (offen – verdeckt).
- Geldgier (mit den Ursachen: Anspruchsniveau, Bedürfnisbefriedigung, Beschaffungsdruck, Unzufriedenheit).
- Zerstörungswut und Vandalismus.

Zusammenfassend können diese Motive als unzulässige und kriminelle Machtausübung bezeichnet werden. Als Untermodell zum Angriffs-/Schadenmodell wird ein genaueres Angriffsmodell formuliert [vgl. Steiner 2003] als Verfeinerung des Zustands ‚Ereignis' (vgl. Abb. 10).

4.3 Generisches Bedrohungs-/Schadenmodell

Das Höhere Gewalt/Schadenmodell und das Angriffs-/Schadenmodell können verallgemeinert werden zu einem generischen Bedrohungs-/Schadenmodell für alle Fälle von Datenverlust durch höhere Gewalt oder Fahrlässigkeit sowie von absichtlichem Vorgehen. Das Modell wird als Zustandsdiagramm dargestellt (vgl. Abb. 11).

Die generischen Komponenten sind Bedrohung, Ereignis, Schwachstelle und Schaden. In diesem verallgemeinerten Modell geht die Bedrohung entweder von höherer Gewalt oder von Angriffen aus. Im Fall der Bedrohung kommt es ggf. zu einem Ereignis. Das Ereignis richtet sich gegen eine mögliche Schwachstelle, die evtl. durch installierte Sicherheitsmaßnahmen geschützt ist. In jedem Fall kann ein Schaden im IT-System (z. B. Durchbrennen, Verändern von Daten) und auch außerhalb des IT-Systems (z. B. Weiche falsch gestellt) entstehen.

Schlussbemerkung

Andere – hier nicht weiter ausgeführte – Begriffsgebäude von safety und security finden sich unter anderen Aspekten wie unter dem Oberbegriff dependability (Zuverlässigkeit) [Laprie 1992] oder es werden die Begriffe safety (Sicherheit), reliability (Funktionsfähigkeit), Überlebenswahrscheinlichkeit, maintainability (Instandhaltbarkeit), availability (Verfügbarkeit) und security (Vertraulichkeit, Daten-Sicherheit) auch als Attribute der Vertrauenswürdigkeit (dependability) genannt [Hanxleden 2002]; eine andere Sichtweise findet sich in [Dierstein 2004]. Weiterhin finden sich graphische Modelle der Begriffsbeziehungen Bedrohung, Restrisiko, Risiko, Schwachstelle und Sicherheitsmaßnahme [ISO/IEC 2003].

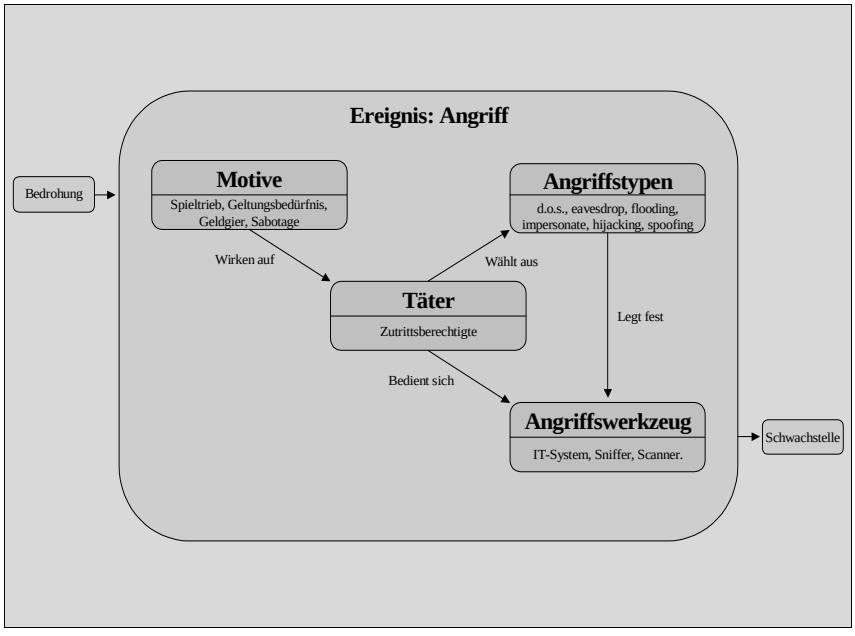

Abb. 10: Angriffsmodell

Literatur

G. Bretthauer, G.: Vorlesung Technische Informatik. Karlsruhe 2003 http://www.rz.uni-karlsruhe.de/~aia/download/TI/ti_vorlesung-kap5.pdf

Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.): Handbuch für die sichere Anwendung der Informationstechnik (IT). IT-Sicherheitshandbuch. Bonn 1991

Bundesamt für Sicherheit in der Informationstechnik – BSI: BSI-Zertifizierung. Hinweise für Hersteller und Vertreiber. Bonn 2001

Bundesamt für Sicherheit in der Informationstechnik – BSI: IT-Grundschutzhandbuch. 5. EL Bonn Oktober 2003

Canadian System Security Centre – Communications Security Establishment (CSE) – Government of Canada: The Canadian Trusted Computer Product Evaluation Criteria. V3.0e Ottawa 1993

Carnegie Mellon Software Engineering Institute: Glossary Software Technology Roadmap. Pittsburgh 2004 http://www.sei.cmu.edu/str/indexes/glossary

Computer Security Institute (CSI) – Federal Bureau of Investigation (FBI): Computer Crime and Security Survey. San Francisco 2003

Dierstein, R.: IT-Sicherheit und ihre Besonderheiten – Duale Sicherheit – München 2002. http://www3.informatik.tu-muenchen.de/lehre/WS2002/IST-dierstein/DualSi.pdf

Dierstein, R.: Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit. Informatik Spektrum 27, 3, 2004

DIN 40 042: Zuverlässigkeit elektrischer Geräte, Anlagen und Systeme – Begriffe. Berlin 1970. Diese Norm wurde 1986 zurückgezogen.

DIN 44 300: Funktionaler Aufbau digitaler Rechensysteme. Berlin 1972

DIN 40 041: Zuverlässigkeit. Begriffe. Berlin 1990

DIN 55 350: Begriffe zu Qualitätssicherung und Statistik. Berlin 1995

DIN (Hrsg.): DIN-TERM Informationstechnik. Begriffe aus DIN-Normen. Berlin 1997

DIN EN ISO 45014: Allgemeine Kriterien für Konformitätserklärungen von Anbietern. (ISO/IEC Guide 22. 1996). Berlin 1998

DIN EN 61508-4: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbar elektronischer Systeme Teil 4: Begriffe und Abkürzungen. VDE 0803-4 Berlin 1999 – auch erschienen als IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.

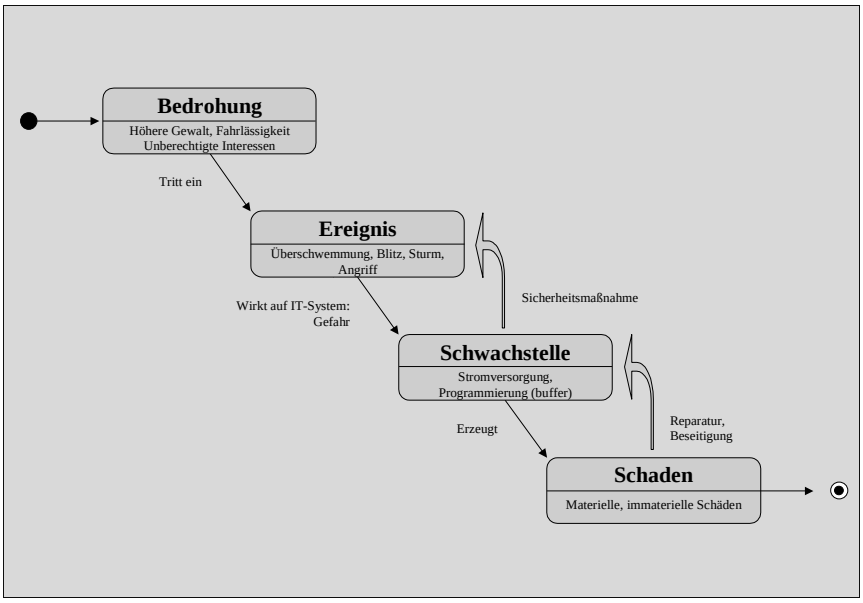

Abb. 11: Generisches Bedrohungs-/Schadenmodell

Duden Redaktion (Hrsg.): Das Fremdwörterbuch. Mannheim 2001

Eckert, C.: IT-Sicherheit. München 2003

Federrath, H.; Pfitzmann, A.: Gliederung und Systematisierung von Schutzzielen in IT-Systemen. Datenschutz und Datensicherheit DuD 24, 12, 704 – 710, 2000

Fries, O.; Fritsch, A.; Kessler, V.; Klein, B. (Hrsg.): Sicherheitsmechanismen. Bausteine zur Entwicklung sicherer Systeme. REMO-Arbeitsgebiete. München 1993

Görke, W.: Fehlertolerante Rechensysteme. München 1989

Grimm, R.; Großpietsch, K.-E.; Keller, H.; Münch, I.; Rannenberg, K.; Saglietti, F.: Technische Sicherheit und Informationssicherheit. Unterschiede und Gemeinsamkeiten. (Diskussionspapier) http://www.ada-deutschland.de/ada_mail/archiv%20-%20geschlossen%20-/291_Sicherheit%202003.04.pdf

Hanxleden, R.v.: Real-Time Systems Programming. Introduction to Dependability. Kiel 2002 http://www.informatik.uni-kiel.de/inf/von-Hanxleden/teaching/ws02-03/v-rt1/lectures/Lecture_09notes.pdf

IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. S. DIN EN 61508-4 1999

Institute of Electrical and Electronics Engineers – IEEE (Ed.): IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York 1990

Irvine, C.; Levin, T.: Toward a Taxonomy and Costing Method for Security Services. IEEE: Proc. 15th Annual Computer Security Applications Conference Phoenix 1999

ISO 8732: Banking – Key Management. Genf 1988

ISO/IEC 7498-2: Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. Genf 1989

ISO/IEC 10181-2: Information technology – Open Systems Interconnection – Security Frameworks for Open Systems – Part 2: Authentication Framework. Genf 1995

ISO/IEC DIS 14980: Information technology. Code of practice for information security management. Genf 1995

ISO/IEC TR 13335-1: Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security. Genf 1996 ersetzt durch ISO/IEC JTC1/SC 27: Text for ISO/IEC FDIS 13335-1

ISO/IEC 2382-14: Information technology – Vocabulary – Part 14: Reliability, maintainability and availability. Genf 1997

ISO/IEC 2382-8: Information technology – Vocabulary – Part 8: Security. Genf 1998

ISO/IEC 9797: Information technology – Security Techniques – Message Authentication Codes (MACs). Genf 1999

ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation (CC 2.1). Genf 1999

ISO/IEC 17799: Information technology – Code of practice for information security management. Genf 2000

ISO/IEC 9126: Software Engineering – Product Quality. 2001

ISO/IEC Guide 73: Risk management – Vocabulary – Guidelines for the use in standards. Genf 2002

ISO/IEC JTC1/SC 27: Standing Document 6 (SD 6), Glossary of IT Security Terminology (SC 27 N 2776): Terminology

used in SC27 standards and drafts. Genf 2002b

ISO/IEC JTC1/SC 27: Text for ISO/IEC FDIS 13335-1 – Information technology – Security techniques – Management of information and communications technology security (MICTS) – Part 1: Concepts and models for managing and planning ICT security. N 3757, WG1 N13758 replaces N3548. Genf 2003

ISO TC 215 / WG 4: Glossary (Rev 1) Security and related definitions. Genf o.J.

ISSO (ed.): Glossary of INFOSEC and INFOSEC related Terms. Information Systems Security Organization. Washington 1996

Laprie, J.C. (ed.): Dependability: Basic concepts and Terminology. Wien 1992

NTG 3004: Zuverlässigkeitsbegriffe im Hinblick auf komplexe Software und Hardware. Entwurf. ntz 35, 325 – 333, 1982

Pfitzmann, A.: Why Safety and Security should and will merge. In: 23nd Intern. Conference SAFECOMP 2004, Potsdam, LNCS 3219, Heidelberg 2004

Pfitzmann, A.; Köhntopp. M.: Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology. Information Hiding Workshop Pittsburgh, 2001 http://marit.koehntopp.de/pub/anon/Anon_Terminology.txt

Pfitzmann, A.; Rannenberg, K.: Staatliche Initiativen und Dokumente zur IT-Sicherheit – eine kritische Würdigung. Computer und Recht 9, 3, S. 170 – 179, 1993 http://www.iig.uni-freiburg.de/~kara/publications/CompRecht9303.pdf

Pohl, H.: Taschenlexikon Sicherheit der Informationstechnik (information security) und anglo-amerikanisch/deutsches, deutsch/anglo-amerikanisches Wörterbuch: Sicherheit in der Datenverarbeitung, klassisch-materielle Sicherheit, Verschlüsselungssicherheit, Übertragungssicherheit, personelle Sicherheit, Fernmeldesicherheit. Köln 1989

Schreck, J.: Security and Privacy in User Modeling. Essen 2000

Shirey, R.: Internet Security Glossary. RFC 2828 (informational). o.O. 2000

Steiner, M.: Simulation von Bedrohungen und deren Auswirkungen anhand eines Sicherheitsszenarios. Diplomarbeit Darmstadt 2003 http://www.sec.informatik.de/lang_neutral/diplomarbeiten/docs/steiner_diplom.pdf

UK online (ed.): Information Security Glossary. London o.J. http://ukonlineforbusiness.gov.uk

Voges, U.: Definitionen von Begriffen im Kontext 'Sicherheit (safety)'. http://www.m-lehrstuhl.de/veranstaltung/GI/ _WS_07_02/Voges.doc

Wolf, G.; Pfitzmann, A.: Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen. Informatik Spektrum 3, 173-191, 2000

Zentralstelle für Sicherheit in der Informationstechnik – ZSI (Hrsg.): IT-Sicherheitskriterien: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT). Bonn 1989