UNIVERSITÄT LEIPZIG

Institut für Informatik

Vorlesung
Datenschutz und Datensicherheit

Dr. Dieter Sosna

Wintersemester 1999/2000

Hinweise, Anmerkungen und Verbesserungsvorschläge bitte an:

- Dr. Dieter Sosna*
- Heiko Stamer**

Version: 840 vom 25. Mai 2000

*<dieter@informatik.uni-leipzig.de>, http://www.informatik.uni-leipzig.de/~sosna

**<stamer@informatik.uni-leipzig.de>, http://stinfwww.informatik.uni-leipzig.de/~mai97ixb

Vorwort des Lesenden:

Datenschutz und Datensicherheit spielen eine wichtige Rolle im Zusammenleben der Menschen. In der Geschichte lassen sich viele Anwendungen dazu gehöriger Mechanismen belegen, so zum Beispiel die Benutzung kryptographischer Techniken zum Schutz der Vertraulichkeit von Nachrichten in allen Epochen, die Anwendung von (schwer fälschbaren) Siegeln zum Nachweis der Authentizität von Dokumenten. Selbst die Aufbewahrung von Büchern als wichtiges Kulturgut der Menschheit in mehreren über den Erdball verteilten Bibliotheken kann als Beitrag zum Schutz der darin enthaltenen Information vor Verlust durch Naturkatastrophen und Kriege und andere Ereignisse angesehen werden.
Mit der Entwicklung der Mikrorechentechnik und dem Heraustreten des Internet aus der relativ heilen Welt der Forschungseinrichtungen anfangs der 90er Jahre (des vorigen Jahrhunderts) begannen Fragen des Datenschutzes und der Datensicherheit eine neue Dimension anzunehmen. Einmal führte die enorme, jetzt an vielen Orten verfügbare Rechenleistung zu ebensolchen Konzentrationen von elektronisch verfügbaren Daten. Mit der Konzentration der Daten steigen die Auswirkungen eines Datenverlustes. Die Konzentration weckt auch das Interesse Unberechtigter. Die rasante Entwicklung der persönlichen Computer, deren Leistungsfähigkeit heute mit der eines Universitätsrechenzentrums vor 15 Jahren vergleichbar ist, erweitert die Gruppe der potentiellen nichtauthorisierten Interessenten an Daten in bisher ungeahnter Weise und anonymisiert sie zugleich. Hinzu kommt, daß auf Grund der weltweiten Vernetzung ein Fernzugriff auf Rechner erfolgen kann, der keine physischen Spuren vor Ort hinterläßt bzw. hinterlassen muß. Die Initiatoren des Internet hatten die vor etwa 10 Jahre einsetzende umfassende Nutzung dieser Technologie so nicht vorausgesehen und folglich Sicherheitsmechanismen nur in begrenzem Maße eingebaut.
Auch wenn diese Defizite im Nachgang geschlossen werden (sollten), erleidet die Industrie derzeit jährlich Verluste in Milliardenhöhe wegen Mängeln im Bereich Datenschutz und Datensicherheit.
Damit sollte jeder Student der Informatik motiviert sein, sich Grundkenntnisse in diesen Bereich anzueignen bzw. seine im Studium erworbenen Kenntnisse auf anderen Gebieten unter diesem Gesichtspunkt neu zu durchdenken. Dazu soll diese Vorlesung anregen.
Die juristische Seite von Datenschutz und Datensicherheit kann in der vorliegenden Vorlesung nicht behandelt werden.

Dank:

Herrn Stamer danke ich für sein Engagement bei der Umsetzung in LaTeX.

Dieter Sosna

Inhaltsverzeichnis

1 Einführung

1.1 Begriffe

Die Thematik „Datenschutz und Datensicherheit“ umfasst zwei Bestandteile:

Definition 1.1 (Datenschutz)
Schutz vor ungewollter Informationsverbreitung bzw. Schutz vor dem Verlust der Vertraulichkeit der in den Daten enthaltenen Information.

Definition 1.2 (Datensicherheit)
Schutz der Daten vor Verlußt oder Manipulation.

Gelegentlich sind die Grenzen zwischen beiden nicht scharf zu ziehen, bei einer Reihe von Schadensereignissen können auch Verletzungen beider Bestandteile gemeinsam auftreten.

1.2 Maßnahmen

Wo setzen Maßnahmen des Datenschutzes, der Datensicherheit an ?
Datenschutz und Datensicherheit werden durch ein Zusammenspiel von Maßnahmen aus verschiedenen Bereichen eines Unternehmens oder Instituts realisiert, einige Maßnahmen wirken sich in beiden Gebieten aus. Die Maßnahmen ergeben sich als Konsequenzen der im Abschnitt 2.2 auf Seite 17 vorgestellten Analyse der Schutzwürdigkeit der Daten und der Analyse der Bedrohungen.
Die folgenden Beispiele sollen einen Eindruck von den vielfältigen Einflußmöglichkeiten geben:

- **personelle Maßnahmen:** Die Tätigkeit von Menschen stellt einen der größten Risikofaktoren im Bereich Datenschutz und Datensicherheit dar. Auch wenn durch die Medien immer wieder von spektakulären Angriffen auf die Datensicherheit in Unternehmen berichtet wird, die außerhalb der betroffenen Einrichtung gestartet werden, so belegen Statistiken, daß von Mitarbeitern ein hohes Gefahrenpotential ausgeht. Für sie sind ggf. weniger hohe Hürden zu überwinden als für Außenstehende, da sie i.A. über Insiderwissen verfügen und mit Privilegien für den Umgang mit Informationen ausgestattet sind. Weitere das Risiko erhöhende Faktoren sind Unaufmerksamkeit und Routine. Irrationales, fanatisches Handeln von Menschen stellt ein besonderes Risiko dar, da es kaum rational vorherzusehen ist.
  Wie die folgende unvollständige Aufzählung zeigt, ist das Spektrum der Maßnahmen im personellen Bereich sehr breit und zum Teil unspezifisch:
  - Schaffen eines guten Betriebsklimas, Motivierung der Mitarbeiter

- Zahlung eines angemessenen Gehalts
- Ausreichende und angemessene Qualifizierung und Weiterbildung der Mitarbeiter
- Kontrolle der Tätigkeiten[8]
- Prüfung der Lebensumstände der Mitarbeiter
- Persönliche Einschränkungen für Mitarbeiter

Insbesondere die letztgenanten Punkte stellen erhebliche Eingriffe in die Persönlichkeitsrechte der Betroffenen dar. Sie müssen deshalb wohlüberlegt und abgestuft eingesetzt werden. Ihr Einsatz wird sicher sehr von der Schutzbedürftigkeit der Informationen/Daten abhängen und bedarf auch einer juristischen Absicherung.

- **betrieblich-organisatorische Maßnahmen**
  Auch hier wird eine sehr breite Palette von Maßnahmen erfaßt:
  - Analyse und Bewertung der tatsächlich auftretenden Bedrohung der Datensicherheit und der Vertraulichkeit der Information als Grundlage aller anderen Maßnahmen
  - Festlegung von prinzipiellen Entscheidungen (Sicherheitspolitik), Überprüfung bisheriger Lösungen, Einsatz neuer Hilfsmittel und Strukturen
  - Erarbeitung konkreter Entscheidungen, wie Arbeitsabläufe, Notfallpläne, Durchführung von Kontrollen, Auswertung von Protokollen und Kontrollen, Festlegung von Zugangsbeschränkungen, Entsorgungskonzepte, ...
  - Einsatz von Wachdiensten und Werkschutz
- **Auswahl und Bewertung von Software:**
  „Software darf nur das tun, wofür sie bestimmt ist.“
  Der Zugriff auf die Daten einer informationsverarbeitenden Anlage erfolgt i.A. mittels Software. Die Sicherheit der Anlage hängt wesentlich von der Zuverlässigkeit und Mangelfreiheit der Software ab. Die Feststellung dieser Eigenschaft ist aufwendig, erfordert Sachkunde und kann i.A. nicht von den Anwendern der Software geleistet werden. Deshalb kann z.B. die Forderung bestehen, nur zertifizierte Software (Abschnitt 5.3, Seite 47) einzusetzen, diese wurde von einem unabhängigen Gutachter geprüft. Um Mißverständnissen gleich vorzubeugen: Zertifizierte Software allein macht keine DV-Anlage sicher, wie wir bei der Vorstellung der Zertifizierungsprozesses sehen werden. Sie kann aber ein wichtiger Baustein im Komplex sicherheitsrelevanter Maßnahmen sein.

[8] Die Tatsache von Kontrollen soll durchaus bekannt sein.

- **technische Maßnahmen:** Hierunter fallen sowohl Maßnahmen, die die DV-Anlage in engeren Sinn betreffen als auch Maßnahmen im technischen Umfeld der Anlage, beispielsweise
  - bauliche Gestaltung der Anlagen,
  - Schutzvorrichtungen gegen Feuer, Wasser, Magnetfelder, Stromausfall,
  - Hardwareredundanz als Schutz vor Ausfällen (Schutz vor Datenverlust oder Verlust der Funktionalität)
  - Hardware (mit entsprechender Software) zum Schutz der Kommunikation mit der Außenwelt (Firewall)
  - Zutrittskontrollen, Video-Überwachung, Alarmtechnik

  Trotz aller Maßnahmen bleibt stets ein Restrisiko. Perfekten Datenschutz und/oder Datensicherheit wird bzw. kann es **nicht** geben.

  Das Ziel der Maßnahmen besteht darin, dieses Restrisiko zu minimieren bzw. unter ein vorgegebenes Limit zu drücken.

2 Was ist Sicherheit

2.1 Angriffe gegen Datensicherheit und Datenschutz

Definition 2.1 *Mit dem Wort* **Angriff** *wird jede Attacke gegen den Datenschutz, die Datensicherheit bezeichnet, unabhängig von Ursache und Ziel.*

Angriffe können insbesondere nach folgenden Kriterien klassifiziert werden.

2.1.1 Klassifikation nach dem Ziel

Zu den Angriffen gehören unabhängig von der Ursache insbesondere ...

- ... Methoden und Mechanismen, um Daten auszuspähen,
  ... Ereignisse, die Daten offenlegen.
- ... Handlungen, um Daten zu manipulieren,
  ... Ereignisse, die Daten verändern.
- ... die Blockierung von Diensten, um dadurch die korrekte Bearbeitung von Daten zu verhindern. (*Denial-of-Service* Angriff, DoS)

  Nachtrag (Februar 2000): In der zweiten Februarwoche d.J. wurden einige E-Commerce-Sites durch eine Flut von (sinnlosen) Anfragen für einige Stunden lahmgelegt. Es trat das Zwanzigfache der normalen Systemlast auf, darauf kann aus wirtschaftlichen Überlegungen kein Betreiber vorbereitet sein. Zur Vorgehensweise: In mehrwöchigen Vorbereitungen wurden (von Experten übrigens bemerkt) eine Vielzahl von Rechnern „gehackt“ und durch Installation entsprechender Software vorbereitet. Diese wurde zu einem bestimmten Zeitpunkt aktiviert und löste die Massenanfragen aus. Auswertung: Die Möglichkeit solcher Angriffe wird stark verringert, wenn Erkenntnisse der Sicherheitsexperten von Systemadministratoren zur Grundlage von Überprüfungen ihrer Installationen gemacht werden.[9] Rechtliche Bewertung: Paragraph 303b StGB droht eine Freiheitsstrafe bis zu 5 Jahren oder eine Geldstrafe demjenigen an, der *‘eine Datenverarbeitung, die für einen fremden Betrieb ... von wesentlicher Bedeutung ist, dadurch stört, daß er ... eine Datenverarbeitungsanlage ... unbrauchbar macht ... ‘*. Dieser Tatbestand wird bei einen Denial-of-Service-Angriff erfüllt. Der Besitzer eines gehackten Rechners ist solange von Strafverfolgung verschont, wie er nichts von dem Einbruch weiß. Auch bei grober Fahrlässigkeit bei der Systemadministration liegt keine Beihilfe vor. Erlangt er davon Kenntnis, sollte er sich an das BSI[10] wenden. Falsch wäre es, den Eindringling einfach auszusperren und die Angelegenheit zu ignorieren oder die Spuren seiner Tätigkeit einfach zu beseitigen, dies könnte zu Schadenersatzansprüchen führen.

  (Quelle: c't, Heft 5/2000, S.68-70)

[9] Dieses Vorgehen erfordert natürlich personellen und finanziellen Aufwand !
[10] Bundesamt für Sicherheit in der Informationstechnik, `http://www.bsi.de/bsi-cert`

2.1.2 Klassifikation nach Ursache und Vorsatz

– *unabsichtlich* bzw. durch *zufällige* Ereignisse eingetreten

  * **Naturkatastrophen** (Erdbeben, Feuer, Überschwemmungen, Sturm, Blitzschlag) mit Folge der Zerstörung von Hardware, dem Verlust von Datenbeständen, Verlust der Vertraulichkeit oder der Blockierung von Diensten.

  * **Fehler in Hard- und Software** mit der Folge, daß unerlaubte Zugriffe ermöglicht bzw. erlaubte Zugriffe verhindert werden.
    Hierzu zählt speziell auch der **technische Ausfall** eines Gerätes.

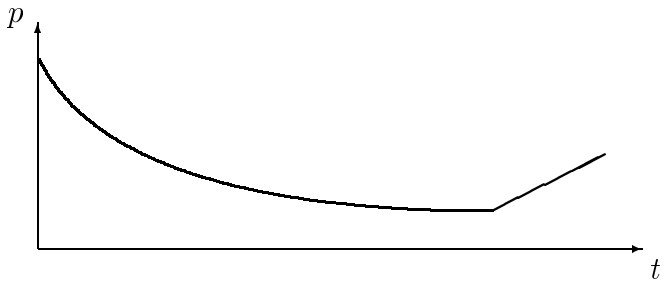


Abbildung 1: Entwicklung der Ausfallwahrscheinlichkeit über der Zeit

    Dabei treten oft Frühausfälle bei Neusystemen und Spätausfälle durch Verschleiß von Hardware (wieder ansteigender Kurventeil) auf, wenn diese nicht rechtzeitig ersetzt wird. Details hierzu finden sich in Vorlesungen zur Technischen Informatik bzw. zur Wahrscheinlichkeitsrechnung. Die Folgen sind wie oben beschrieben.

  * Unter **Menschlichem Versagen** wollen wir eine unabsichtliche Fehlbedienung, wie z.B. *Tastatureingabefehler* verstehen, in deren Folge Daten offengelegt, verändert, vernichtet oder Dienste blockiert werden.

– *absichtlich* bzw. durch *vorsätzlichen Mißbrauch* entstanden

  * **Authorisierte Benutzer** (Administratoren, Programmierer, Benutzer mit/ohne Sonderrechte), die ihre Rechte missbrauchen, können in einem System erhebliche Schäden verursachen und/oder vertrauliche Informationen erlangen.
    Dieser Fall wird oft auch als **Angriff von innen** bezeichnet.

  * Aber auch **unberechtigte Benutzer** können durch gezielte Suche nach Schwachstellen und Ausnutzung dieser Stellen dem System Schaden zufügen. (z.B. durch vorsätzliches Einbringen von

Viren, Manipulation und Erlangung von Privilegien) (auch **Angriff von außen** genannt).

2.1.3 Klassifikation schadenverursachender Software

Als Folge der Vernetzung nimmt der softwarebasierte Angriff stark zu, da durch das Netz schadenverursachende Software verbreitet werden kann. Im folgenden gehen wir auf einige wichtige Angriffsformen ein, die mit Hilfe von Computerprogrammen durchgeführt werden können. Die Herstellung solcher Programme geschieht i.A. vorsätzlich, die Weiterverbreitung kann aus Unkenntnis oder Unachtsamkeit erfolgen.

- **Viren** sind Programme mit zwei typischen Eigenschaften:
  1. Können sich selbst vervielfältigen und eventuell sogar verändern.
  2. Sind fähig, das Wirtssystem dauerhaft und oft irreparabel zu schädigen.
- **Trojanische Pferde** sind Programme, die neben ihrer offiziell bekannten Tätigkeit noch zusätzliche Informationen sammeln, weiterverarbeiten und/oder weiterleiten.
- Unter Programmen mit **Falltürfunktionen** verstehen wir solche, die neben einer offiziellen Funktionalität unter wohldefinierten, aber nicht allgemein bekannten Umständen weitere geheime Funktionalitäten entwickeln. Diese können dann durch spezielle Eingaben o.ä. aktiviert werden.

2.1.4 Angriffe auf den Datenschutz

Ziel dieser Angriffe ist die Gewinnung von nicht allgemein bekannten Daten durch Unberechtigte.

- Gewinnung von Informationen durch das Zusammenführen von Daten aus verschiedenen Quellen (Datenabgleich zwischen Datenbanken, Überschneidungswissen, *Data-Mining*, ...). Selbst wenn die einzelnen Datenquellen keines besonderen Schutzes bedürfen, kann durch das Zusammenführen der Information schutzbedürftige Information entstehen. Insbesondere ist dies zu vermuten, wenn das Zusammenführen sich nicht auf einzelne Datensätze beschränkt, wenn etwa die Grundbuchdaten einer ganzen Ortschaft mit Luftbildaufnahmen der Grundstücke und fotografischen Gebäudeansichten sowie dem Telefonbuch

verbunden werden. Eine Klärung kann nur durch Prüfung der konkreten Umstände jedes Einzelfalls erreicht werden.

– Nutzung von Statistikfunktionen, um Einzeldaten zu gewinnen, falls die statistische Grundgesamtheit zu gering ist. Hier versagt die anonymisierende Wirkung der Funktion - der Benutzer kann Aussagen zu einzelnen Datensätzen machen. Der triviale Extremfall, daß es sich nur um einen Eintrag handelt, verdeutlicht die Sachlage:

  Beispiel 2.1 *Anfrage über alle Datensätze einer Personaldatenbank:*
  Durschnittliches Gehalt **aller** *Personen* **mit** *Name*= 'Dieter Sosna'

  In der Realität wird dabei die Tatsache, daß die Antwortmenge nur ein Element enthält, durch eine andere Formulierung der Anfrage ggf. verschleiert.

  Lösung 2.1 *Um diesen Angriffen auf den Datenschutz zu begegnen, gibt es mehrere Möglichkeiten. Einmal kann die Grundgesamtheit, auf die die Statistikfunktion anzuwenden ist, auf ausreichende Kardinalität vom System geprüft werden. Ist sie zu gering, wird die Anfrage abgewiesen.*
  Zum anderen können durch Einfügen von Streufaktoren die konkreten Einzeldaten bis zur Unkenntlichkeit verändert werden mit der Nebenbedingung, daß Mittelwert und Streuung unverfälscht bleiben, sofern nicht der obige Extremfall vorliegt.

– die Verwendung von Existenzaussagen, bei denen die Bedingungen so speziell sind, daß auf einzelne Werte geschlossen werden kann.

  Beispiel 2.2 *Anfrage über alle Datensätze einer Personaldatenbank:*
  Existiert eine Person mit Namen SOSNA und Gehalt zwischen 18 und 18.5 TDM, deren Arbeitsplatz das INSTITUT FÜR INFORMATIK ist ?

  Lösung 2.2 *Abweisen solcher Anfragen, das Datenbanksystem führt die Anfrage ggf. in einer erweiterten Fassung intern aus und bewertet die Ergebnismenge nach Sicherheitsregeln. Werden die dort gestellten Bedingungen von der Anwort erfüllt, wird die Ausgangsanfrage beantwortet. Die Schwierigkeit dieses Vorgehens besteht in einer intelligenten Bewertung der Ergebnismenge.*

– Kombination der Ergebnismenge mehrerer unverfänglicher Anfragen außerhalb des Systems.

  Beispiel 2.3 *Folgende Anfragen werden unabhängig voneinander an eine Personaldatenbank unseres Instituts gestellt:*

`SELECT Personalnummer FROM Personen WHERE Vorname='Dieter'`

und

`SELECT Personalnummer FROM Personen WHERE Alter` $\geq$ `50`

Ein Blick in die Ergebismengen zeigt, daß es genau eine Person mit Vornamen `Dieter` *gibt, die älter als 49 Jahre ist. Deren Peronalnummer ist jetzt bekannt.*

Lösung 2.3 *Protokollierung von Aktionen/Zugriffen und Auswertung der „Geschichte“ bei neuen oder kombinierten Anfragen.*

- Auch die Tatsache, daß Informationen vorhanden sind, kann selbst wieder eine Information für mögliche Angreifer sein. Deshalb ist es oft auch notwendig, die Existenz von Daten/Informationen zu verbergen.

  Beispiel 2.4 (Leitungsüberwachung)
  Ein Kommunikationskanal wird von einer dritten Person permanent abgehört. Der Zuhöhrer kann bei entsprechendem Zusatzwissen allein aus der Tatsache, daß auf dem Kanal ein Informationsaustausch stattfindet, Schlüsse ziehen.

  Lösung 2.4 *Auf der Leitung wird ständig ein geeignetes „Rauschen“ übertragen. Rauschen ist in diesem Zusammenhang ein Signal, welches sich für einen Nichteingeweihten von einem Nutzsignal nicht unterscheidet, dem aber keine Bedeutung zugeordnet ist. Natürlich muß hierbei gewährleistet sein, daß der berechtigte Empfänger die Nutzdaten vom Rauschen trennen kann.*
  Ein Beobachter erhält so keine Hinweise, ob und warum Informationen übertragen werden. Er kann auch keine Zusammenhänge mit externen Ereignissen feststellen.

- Zur **Verschleierung** von Informationsübertragungen an Außenstehende kann auch ein **verdeckter Kanal** benutzt werden.

  Beispiel 2.5 (verdeckter Kanal)
  Die Information wird in unauffälligen Ereignissen versteckt.

  Dies kann z.B. das Starten eines bestimmten unverdächtigen Programmes zu einem vereinbarten Zeitpunkt sein, welches dann von anderen Eingeweihten beobachtet wird und damit ein Bit überträgt.

  Diese Idee des verdeckten Kanals wird auch in der **Steganographie** genutzt, wo Daten in Bildern, Musikstücken oder Textfragmenten verborgen werden, indem diese (an unauffälligen Stellen) gegenüber dem Original

verändert werden, so daß die Veränderung die zu versteckende Nachricht kodiert.

2.2 Sicherheit eines Datenverarbeitungssystems

Definition 2.2 *Ein System heißt* **sicher**, *wenn alle Bedrohungen ausgeschlossen werden können.*

Diese Definition ist allerdings nicht sehr realistisch, da solche Lösungen technisch nicht machbar sind (z.B. ein absoluter Schutz einer DV-Anlage gegen Feuer) und wenn sie technisch machbar sind, meist einen sehr hohen finanziellen Aufwand erfordern (z.B. Gewährleistung der Erdbebensicherheit einer Datenbank mittels weiträumiger Verteilung).
Die technischen oder praktischen Grenzen, die vollständige Sicherheitslösungen unmöglich machen, legen folgende Definition nahe:

Definition 2.3 *Ein System heißt* **(praktisch) sicher**, *wenn die „Summe" der Bedrohungen ein vorgegebenes Restrisiko nicht überschreitet.*

Viele existierende Lösungen im Bereich Datenschutz/Datensicherheit bauen auf dieser Definition auf, wobei die genannten Begriffe noch einer Präzisierung bedürfen.
Eine weitere Möglichkeit, den Begriff Sicherheit zu fassen, besteht in einer induktiven Definition.

Definition 2.4 (induktive Definition) *Ein System, welches jeweils durch einen Zustand aus einer Menge von Zuständen beschrieben wird, heißt* **sicher**, *wenn es*

1. *einen sicheren Anfangszustand gibt,*
2. *eine Menge von zulässigen Operationen definiert ist und*
3. *der bestehende Zustand dadurch entstanden ist, daß auf den Anfangszustand eine Folge von zulässigen Operationen angewendet wurde.*

Beispiel: Die Erhaltung der Konsistenz einer Datenbank bei der Ausführung von Transaktionen (C aus ACID) beruht genau auf dieser Definition.

2.3 Notwendigkeit des Schutzes von Daten

2.3.1 Analyse der Schutzwürdigkeit

Hierbei versucht man zu klären, in welchem Maße die betreffenden Daten schutzwürdig sind. Dies erfordert eine komplexe Betrachtung mit Beiträgen aus folgenden Teilgebieten:

- **betriebswirtschaftliche Faktoren**
  z.B. Geheimnisschutz, Schutz vor Verlußt (Buchhaltungsdaten, ...), wirtschaftliche und technische Folgen eines Verlustes
- **juristische Faktoren**
  z.B. Auskunftspflicht, Einhaltung von gesetzlichen Vorschriften, Archivierungsfristen

  In [4] gibt K. Pommerening folgende Auswahl an Gesetzen und Verordnungen, die insgesamt oder in Teilen den Datenschutz betreffen:

  - Bundesdatenschutzgesetz (BDSG), siehe [7]
  - Landesdatenschutzgesetz
  - Bundesstatistikgesetz
  - Landesstatistikgesetz
  - Hochschulstatistikgesetz
  - Meldegesetz
  - Bundesverpflichtungsgesetz
  - Fernmeldeanlagengesetz
  - Urheberrechtsgesetz
  - Strafgesetzbuch

  Weiter betreffen das Gebiet:

  - Teledienstdatenschutz-Gesetz (TDDSG)
- **politische Faktoren**
  z.B. Vertrauensverlust, personelle Konsequenzen
- **soziale und ökologische Faktoren**
  z.B. Folgen eines Versagens der Steuerung einer chemischen oder kerntechnischen Anlage.

- **Art und Weise der Datenhaltung als Faktor**
  Es gilt zu beachten, daß die Schutzbedürftigkeit auch von der Art und Weise der Datenhaltung abhängt. Typisches Beispiel hierfür ist das klassische Telefonbuch und seine elektronische Entsprechung auf CD, bei der eine Suche nach dem Straßennamen möglich ist und eine Nutzung dieser Suche für Werbezwecke ganz offensichtlich ist. Aus Datenschutzüberlegungen wurde die Suche nach der Adresse eines Teilnehmers bei bekannter Telefonnummer aus der CD-Version herausgenommen, während sie im klassischen Telefonbuch uneingeschränkt möglich ist ...
  Bei der Bewertung der Schutzwürdigkeit ist generell eine Unterscheidung nach zwei Bestandteilen des Bereiches Datenschutz/Datensicherheit sinnvoll:

  1. Verlust der Daten (Datensicherheit)
  2. Verlust der Vertraulichkeit (Datenschutz)

  Beispiel 2.6 *Verknüpfung von Bilddaten der Straßen und Gebäude mit Telefonbuchinformationen*

  Problem: Mißbrauch zu Werbezwecken oder Informationsquelle zur Vorbereitung krimineller Aktionen.

  Beispiel 2.7 *elektronische Bestellsysteme für Waren*

  Problem: Sammeln aller Daten und Erstellen eines Profils über die Kaufgewohnheiten des Benutzers ist möglich.

Allein die Aufzählung der Faktoren, die zu einer Schutzwürdigkeit der Daten führen, macht deutlich, daß diese Feststellung nicht allein vom Informatiker getroffen werden kann. Vielmehr ist hier eine Zusammenarbeit mit Juristen, betriebswirtschaftlich ausgebildeten Fachleuten, mit dem ingenieurtechnischen Personal und der Führung eines Unternehmens notwendig.
Ein weiteres Ziel der komplexen Untersuchung der Schutzwürdigkeit ist es, die im Falle einer Verletzung zu erwartenden *materiellen* und *ideellen* Schäden abschätzen zu können.

2.3.2 Analyse der Bedrohungen

Grundlage aller Maßnahmen im Bereich Datenschutz/Datensicherheit ist nach der Feststellung der Schutzwürdigkeit die Analyse der real existierenden Bedrohungen. Dabei sind folgende Fragen zu klären:

- Auf welchen Bereich der Einrichtung bezieht sich die Analyse ?
  - Wie ist dieser Bereich gegen andere Bereiche abgegrenzt ?

  - Welche Beziehungen (Informationsflüsse) existieren zu den anderen Bereichen ?

- Welche Bedrohungen existieren ?
  - Mit welcher Wahrscheinlichkeit treten sie auf ?
  - Welcher Schaden ist zu erwarten ?

Beispielbetrachtung für ein fiktives EDV-UNTERNEHMEN **in Leipzig:**

Bedrohung	Wahrscheinlichkeit	Kalkulierbarkeit des Eintretens	Einflußfaktoren
Erdbeben	sehr gering	nein	bauliche Maßnahmen im Rahmen der Standortwahl
Hochwasser	gering	mittelfristig	bauliche Maßnahmen im Rahmen der Standortwahl
Sturm und Hagel	möglich	kurzfristig	normale Bauanforderungen
Blitzschlag	möglich	kurzfristig	Blitzschutzanlagen, Datensicherung
Überspannungen	möglich	nein	Überspannungsschutz, Datensicherung
Kriegseinwirkungen	z.Zt. sehr gering	kurzfristig	keine / baul. Maßnahmen
Terrorangriffe	möglich	nein	bauliche Maßnahmen, Objektschutz
elektronische Angriffe	hoch	nein	elektronische Gegenmaßnahmen, Qualifizierung, Spezialisierung der Mitarbeiter, Einsatz verbesserter Software
Wirtschaftsspionage	hoch	nein	Einsatz zertifizierter Software, Verschlüsselung, Geheimnisteilung
Bedienungsfehler	hoch	nein	physikalisch-technische Maßnahmen, Kontrolle und Ausbildung der Mitarbeiter Einsatz zertifizierter Software

Diese Aufstellung kann das Problem nur anreißen, in einem konkreten Fall sind diese Aussagen durch detailierte Untersuchungen unter den dann gültigen konkreten Umständen und durch Fakten zu belegen.

Beispiel Hauptrisikofaktor MENSCH**:** Am Beispiel des Einflußfaktors Mensch sollen einige konkrete Gesichtspunkte genannt werden. Der Mensch stellt nach übereinstimmender Meinung in der Literatur einen Hauptrisikofaktor dar, der sich im Gegensatz zu technischen Risikofaktoren nur unzureichend kalkulieren oder statistisch erfassen läßt. Er kann nur durch Menschen mit ihren Erfahrungen bewertet werden. Bei der Einschätzung können folgende Gesichtspunkte eine Rolle spielen:

- Ausbildung und Qualifikation
  (Einsatzgebiet des Mitarbeiters entsprechend seiner Qualifikation wählen, Probleme der Über- und Unterqualifikation)
- Persönlichkeit (labiler Charakter, Geltungsbedürfnis, Beeinflußbarkeit)
- Lebensstil (extensiv oder im Rahmen seiner finanziellen Verhältnisse)

- Umfeld (persönlicher Lebenslauf, Bekannte und Freunde)
- Loyalität zum Arbeitgeber, bisherige Tätigkeit
- politische Einstellung und gesellschaftliche Motive

Tätigkeiten in sicherheitsrelevanten Bereichen setzen immer ein Vertrauensverhältnis voraus und führen bei beiden Seiten (Mitarbeiter/Arbeitgeber) zu Einschränkungen der persönlichen/betrieblichen Freiheiten.
So hat zum Beispiel der Mitarbeiter ggf. in gewissen Maße Einblick in seine Privatsphäre zu geben, während der Arbeitgeber dafür besondere Entschädigungen gewährt bzw. für angemessene Arbeitsbedingungen sorgt. Die Einschätzung von Menschen stellt eine der schwierigsten Aufgaben im Bereich Datenschutz und Datensicherheit dar und erfordert große Erfahrung und viel Verantwortungsbewußtsein. Insbesondere können hier Fehlbeurteilungen und Nachlässigkeiten extrem fatale Folgen für die Firma und für Betroffene haben. Nicht umsonst wurden ja die personenbezogenen Daten dem Datenschutz unterstellt.

2.3.3 Bewertung und Einschätzung des Gesamtrisikos

Aus der Analyse der einzelnen Risikofaktoren ist ein Gesamtrisiko abzuleiten (Wahrscheinlichkeit für das Eintreten eines Schadensfalles) . Das Vorgehen kann nicht global festgelegt werden, sondern hängt von der Einzelsituation ab. Möglicherweise besteht die Angabe des Gesamtrisikos in einer Aufzählung der Risiken der einzelnen Bedrohungen, in einem anderen Fall können diese vielleicht zusammengefaßt werden.

2.3.4 Entscheidung des Managements zum Restrisiko

Bei unserem Vorgehen wird unterstellt, daß es keine absolute Sicherheit gibt, damit muß die Frage nach einem tragbaren Restrisiko gestellt werden. Die Entscheidung wird *im Gesamten* von den Führungskräften und *im Detail* von den Fachleuten eines Unternehmens getroffen.
Ein Vergleich der Bedrohungsanalyse mit dem akzeptablen Restrisiko zeigt nun, in welchen Bedrohungsbereichen das tatsächliche Risiko das tragbare Risiko überschreitet. Um dieses tragbare Restrisiko zu erreichen, sind ggf. weitere Entscheidungen notwendig, um entweder das akzeptable Restrisiko zu erhöhen oder das tatsächliche Bedrohungsrisiko zu senken.
Die Entscheidungen können dabei grundsätzlicher Art sein oder Details betreffen.

Hierzu zählen Entscheidungen ...

- ... zu den grundlegenden Prinzipien.

- ... zum Gesamtkonzept.
- ... zur Realisierung.
- ... zu Varianten, Mechanismen und Alternativen.

Nach den Entscheidungen sind die Analysen zu aktualisieren.
Insgesamt handelt es sich um einen langwierigen und kostenintensiven Prozeß, zu dessen Durchführung ein Unternehmen durchaus Dienstleister in Anspruch nehmen sollte. Hierfür sprechen mehrere Gründe:

- Objektivität der Einschätzungen
- Nutzung von Fachwissen auf dem Gebiet Datenschutz/Datensicherheit
- rechtliche Fragen (Haftung, Schadensersatz)

2.4 Sicherheitspolitik

Definition 2.5 *Die* **Sicherheitspolitik** *umfaßt* **grundlegende** *Ausführungen zum Thema Datenschutz/Datensicherheit in einem Unternehmen oder in einer Einrichtung.*

Insbesondere werden durch die Sicherheitspolitik Antworten auf folgende Fragen gegeben:

- Wie sieht das Systemmodell der DV-Anlage aus ?
  (Klassifizierung des Systems)
- Welche Schutzwürdigkeiten bestehen ?
- Gegen welche Bedrohungen soll geschützt werden ?
- Welches Restrisiko ist akzeptabel?
- Welche Grundregeln werden angewendet ?
  - Welche allgemeinen (Sicherheits-) Modelle werden verwendet ?
  - Wie werden diese firmenspezifisch umgesetzt ?
- Welche Personalfragen werden von den Festlegungen zum Datenschutz und zur Datensicherheit berührt (Einstellungspolitik) ?
- Welches Restrisiko besteht weiterhin ?

Von der Politik unterschieden werden konkrete Maßnahmen zur Umsetzung der Politik. Diese werden als Mechanismen bezeichnet und beziehen sich auf die in der Einleitung (vgl. Abschnitt 1.1, Seite 7) aufgeführten Bereiche.

2.5 Rollen beteiligter Personen

Definition 2.6 *Im laufenden Betrieb eines DV-Systems sind hinsichtlich des Datenschutzes / der Datensicherheit mehrere Aufgabenbereiche zu unterscheiden, die hier* **Rollen** *genannt werden.*

Bei der Besetzung dieser Rollen mit Personen ist genau zu hinterfragen, welche Rollen im Zusammenhang mit der Realisierung der Maßnahmen zu Datenschutz / Datensicherheit besetzt werden sollen bzw. welche Rollen (aus Kostengründen) zusammengefaßt werden oder gar nicht besetzt werden. Die Klassifizierung der Personen nach ihrer Rolle führt zu einer „Gewaltenteilung“ bei der Administration und hat folgende Ziele:

- Schaffung besserer, klar erkennbarer Kontrollstrukturen
- Vermeidung von Einzelfehlern, bzw. Erkennung der Fehler und Begrenzung der Auswirkungen

Im Rahmen der allgemeinen Sicherheitspolitik lassen sich meist folgende Rollen erkennen:

- **Systemadministrator**
  - ist technische Fachkraft mit umfassenden Kenntnissen des Systems
  - Er sorgt dafür, daß das System auf dem letzten Stand der Entwicklung ist und daß die in der Sicherheitspolitik festgeschriebenen Maßnahmen (z.B. Protokollierungen) in der benötigten Qualität durchgeführt werden. Im Falle der Notwendigkeit kann er (evt. nur in Verbindung mit einer der folgenden Rollen) in die Sicherheitsmechanismen eingreifen. Deshalb ist diese Funktion eine absolute Vertrauensposition.
- **Sicherheitsbeauftragter**
  - ist IT-Sicherheitsfachkraft
  - er kennt sowohl die Sicherheitspolitik, die Möglichkeiten des Sytems zur Realisierung der Politik als auch die Schutzwürdigkeit der Daten bzw. ist in der Lage, diese einzuschätzen. Auf Grund dieser Kenntnisse legt er fallbezogen die Einstufungen von Daten oder Personen fest. Beispielsweise vergibt er Zugriffsrechte der Subjekte auf Objekte (s. Abschnitt 4, Seite 35)
- **Sicherheitsinpektor**, (engl. supervisor)
  - ist IT-Sicherheitsfachkraft
  - er kennt sowohl die Sicherheitspolitik, die Möglichkeiten des Sytems zur Realisierung der Politik als auch die Schutzwürdigkeit der Daten.

Auf der Grundlage dieses Wissens prüft er Entscheidungen des Sicherheitsbeauftragten, wertet die Protokolle aus. Das Ziel seiner Tätigkeit ist das Erkennen von Verstößen gegen die Sicherheitspolitik (möglichst schon beim Versuch). Er gibt dem Systemadministrator Hinweise zu Sicherheitsmängeln im System.

- **Anwendungsprogrammierer**
  - ist technische Fachkraft
  - erstellt neue Anwendungen unter Beachtung der Sicherheitspolitik und bringt diese in das System ein. Sein Zugriff auf Daten ist auf Testzwecke begrenzt.
- **Systemnutzer**
  - Der normale Benutzer des Systems ist an die ihm zugestandenen Privilegien gebunden. Insbesondere kann er sich selbst keine neuen Privilegien zuordnen. Seine Rechte, das System zu verändern / zu ergänzen, sind stark eingeschränkt. Die Zugriffsrechte auf die Daten werden nur entsprechend der Sicherheitspolitik bemessen.
- **Service-Techniker**
  - ist eine hochqualifizierte IT-Fachkraft
  - arbeitet am System in einem irregulären Betriebsmodus mit umfassenden Privilegien
  - ist häufig Mitarbeiter einer Fremdfirma

  Die Systemwartung bringt das informationstechnische System in jedem Falle in einen sicherheitstechnischen Ausnahmezustand, in dem viele der Sicherheitsmechanismen außer Kraft gesetzt sind. Deshalb ist für den Service-Techniker diesselbe Sicherheitsanforderung wie für einen Systemadministrator zu stellen. Wenn der Service einer Fremdfirma übertragen wird (outsourceing), ist dies bei der Sicherheitspolitik zu bedenken und ggf. durch spezielle Maßnahmen zu begleiten.[11]

Die Ausprägung dieser Rollen hängt stark vom Schutzbedürfnis der Daten und der Einschätzung der Arbeitsumgebung ab. Bestes Beispiel hierfür ist das Betriebssystem UNIX in seinen etwas älteren Varianten. Es wurde entwickelt, um in einer kooperativen Umgebung eingesetzt zu werden, in der die Nutzer Fachkenntnisse besitzen. Es sollte im wesentlichen ein Mehrbenutzerbetriebssystem

[11] Zum Beispiel wurden in einem Unternehmen mit hochsensiblen Daten vor dem Eintreffen des Technikers die Plattensysteme mit diesen Daten physisch abgekoppelt und in einen sicher verschlossenen Nebenraum verbracht, um erst nach Weggang des Technikers wieder angeschlossen zu werden.

vor versehentlichen Attacken eines Nutzers schützen. Folglich wurde nur die Rolle des Systemadministrators (root) realisiert und sein Bereich sowie wichtige Systemdaten geschützt. Der Schutz der Anwenderdaten kann vom Anwender selbst festgelegt werden.

3 Grundfunktionen eines sicheren Systems

Definition 3.1 *Unter den* **Grundfunktionen** *verstehen wir Funktionen, die ein zu schützendes System realisieren muß, um damit einen ganz bestimmte Teilbereich der Sicherheitsanforderung abzudecken und die in diesem Zusammenhang nicht weiter untergliedert wird.*

Ein Beispiel für eine Grundfunktion ist die Nutzeridentifikation. Ihre Aufgabe ist es, die Identität eines Nutzers eindeutig festzustellen.

Bevor wir auf einzelnen Funktionen sicherer Systeme eingehen, wollen wir noch zwei Begriffe definieren:

Definition 3.2 *Ein* **Objekt** *ist eine beliebige Teilmenge der Daten, die in einem Systems gespeichert sind.*

Dabei ist zu bedenken, daß auch Programme, Scripte u.ä. Daten in diesem Sinn darstellen.

Definition 3.3 *Unter einem* **Subjekt** *verstehen wir einen Benutzer oder ein ablaufendes Programm/Skript, welcher/welches die Ressourcen und Objekte des Systems verwenden will.*

Zu beachten ist der bi-valente Charakter von Programmen u.ä.: Einmal sind sie aus Sicht ihres Benutzers Objekt, zum anderen sind sie Subjekt hinsichtlich der zu bearbeitenden Daten und zu benutzenden Systemressourcen.

3.1 Zugangskontrolle

Die Zugangskontrolle stützt sich auf zwei Grundfunktionen. Einmal identifiziert der Benutzer sich gegenüber dem System z.B. durch Angabe eines LOGIN-Namens. Im zweiten Schritt beweist er, daß es sich bei ihm wirklich um die Person (das Subjekt) handelt, welche(s) zum angegebenen LOGIN-Namen gehört. Wichtigste Eigenschaft der Zugangskontrolle ist ihre Täuschungssicherheit. Da es auch hier keine absolute Sicherheit geben kann, ist zu fordern, daß der Aufwand, dem System eine falsche Identität zu beweisen, so hoch ist, daß er materiell, finanziell oder technisch als nicht realisierbar erscheint oder der zu erwartende Nutzen für den Angreifer deutlich unter seinem Aufwand liegt.

3.1.1 Identifikation

Die Identifikation dient der eindeutigen Bestimmung der Identität eines Subjektes. Dies geschieht in der Regel durch Angabe einer eindeutigen Benutzerkennung (ID).

3.1.2 Authentisierung

Unter dem Begriff **Authentisierung** wollen wir das „Beweisen“ der Identität eines Benutzers verstehen. Dies kann mittels folgender Ansätze realisiert werden:

1. durch Wissen (z.B. Passwörter , Zero-Knowledge-Protokolle)
2. durch Besitz (von Gegenständen wie Chipkarten, Schlüssel)
3. durch personenbezogene, biometrische Merkmale (Fingerabdruck, Netzhaut, Gesicht)

Bisher dominieren die beiden erstgenannten Punkte in den Anwendungen, der dritte Ansatz ist noch Gegenstand der Forschung. Da er aber prinzipielle Vorteile hinsichtlich Verlust und Fälschungssicherheit besitzt, wird seine Bedeutung sicher zunehmen. Die Authentisierung tritt insbesondere beim *login-Vorgang* in unmittelbarer Folge einer Identifikation auf, jedoch gibt es eine Reihe von Ursachen, die einen erneuten Nachweis der Identität angeraten erscheinen lassen. Zugriffe, die besondere Rechte erfordern, gehören dazu. Aber auch Tatsachen, die zu der Annahme Anlaß geben, daß evt. ein anderer Nutzer am System tätig ist, müssen entsprechend beachtet werden. Hier sei die Wiederaktivierung eines „gelockten “ Terminals genannt. Mit der Aktivierung des Lock-Mechanismus hat der Nutzer dem System mitgeteilt, daß er vorübergehend das Terminal nicht sicher kontrollieren kann. Deshalb ist die Forderung nach erneuter Authentisierung sinnvoll.

3.1.3 Paßwortwahl

Paßwort-gestützte Verfahren zählen zu den meist verbreiteten Authentisierungsmechanismen. Sie sind bei richtiger Paßwortwahl in vielen Bereichen ausreichend. Bei einem 8-stelligen Paßwort ergeben sich (bei nicht vollständiger Ausnutzung der Tastatur) etwa 80^8 Kombinationen. Die Chance, ein Paßwort durch systematisches Probieren zu finden (brute-force Angriff) , ist verschwindend gering. Wesentlich unsicherer sind die sogenannten *schwachen* Paßworte. Sie bestehen aus Namen (von Verwandten und Freunden des Inhabers) und anderen Worten der Sprache. Die Namen können oft erraten werden. Gegen solche Paßworte ist auch der Lexikon-Angriff häufig erfolgreich.
Beim Lexikon-Angriff wird unterstellt, daß der Angreifer sich das verschlüsselte Paßwort verschaffen konnte (dies war beim klassischen UNIX-Betriebssystem mit Speicherung der verschlüsselten Paßwörter in der allgemein zugänglichen Datei `/etc/passwd` leicht erreichbar) und der Verschlüsselung-Algorithmus (wie bei UNIX) bekannt ist. Der Angreifer verschlüsselt nun fortlaufend die Wörter eines Wörterbuchs, bis er eine Übereinstimmung der verschlüsselten Zeichenketten von Wort und zu beschaffendem Paßwort findet. Da die Authentisierung auch auf diesem Vergleich beruht, ist dann

der Einbruch gelungen. Zur Abwehr werden systemseitig die verschlüsselten Paßwörter dem allgemeinen Zugriff entzogen und in einem geschützten Bereich abgelegt (Shadow-Paßwortsystem).

Der Beitrag des Nutzers zur Abwehr besteht in der richtigen Wahl seines Paßwortes. Eine gute Wahl sind über Eselsbrücken merkbare Kunstworte.

Sonst war alles für die Katz ! Swa4dK!

3.2 Zugriffskontrolle, Rechteprüfung

Die Zugriffskontrolle prüft, ob ein Subjekt die Berechtigung hat, in der gewünschten Weise auf ein Objekt zuzugreifen. Hierbei sind Zeitpunkt sowie Art und Weise der Prüfung wichtig. Je nach Ziel kann vor dem Zugriff auf die Daten oder in Abhängigkeit vom Ergebnis nach dem Zugriff, aber vor Freigabe der Ergebnisse geprüft werden.

Voraussetzung für jede Rechteprüfung ist eine sichere Identifikation jedes Subjekts und jedes Objekts.

3.3 Rechteverwaltung

Hierzu zählen primär die Vergabe, der Entzug und die Veränderung von Rechten. Darüber hinaus müssen aber auch die Folgen der Weitergabe von Daten und Rechten geregelt werden, um zu verhindern, daß durch die Übertragung von Rechten ein verdeckter Kanal entsteht oder geschaffen werden kann. Bei der Weitergabe von Daten ist aus diesem Grunde sehr sorgfältig abzuwägen, welche Rechte der neue Besitzer an diesen Daten erhält.[12]

3.3.1 Prinzipien

Im allgemeinen existieren bei der Vergabe von Rechten zwei Grundprinzipien:

$\mathcal{A}$: **Prinzip der Vergabe minimaler Privilegien**

Definition 3.4
Nach dem Prinzip der Vergabe minimaler Privilegien erhält jeder Nutzer eines Systems solche minimalen Zugriffsrechte, so daß er seine Aufgaben (gerade noch) erfüllen kann.

[12]Unter UNIX impliziert beispielsweise das Leserecht für andere Nutzer die Möglichkeit der unkontrollierbaren Weitergabe.

Probleme:

- Aufgaben der Nutzer können sich ändern, so daß zusätzliche Rechte notwendig werden oder andere Rechte nicht mehr benötigt werden. In jedem dieser Fälle muß die Rechteverwaltung aktiviert werden. Es entsteht großer Administrationsaufwand.

$\mathcal{B}$: **Prinzip der Vergabe maximaler Privilegien**

Definition 3.5
Nach diesem Prinzip können mit Ausnahme von wenigen Einschränkungen alle Daten und Systemressourcen von allen Nutzern genutzt werden.

Probleme:

- Übersehen notwendiger Einschränkungen durch den Administrator.
- Unbekannte Sicherheitsprobleme können ausgenutzt werden, da es dafür zunächst keine Einschränkung gibt.

Prinzip $\mathcal{A}$ führt bei konsequenter Anwendung zu einem **abgeschlossenen** System. Dieses läßt sich durch folgenden Satz charakterisieren:

Es ist alles verboten, was nicht ausdrücklich erlaubt wird.

Vorteile:

+ Sicherheit ist leicht nachprüfbar
+ i.A. ist der Sicherheitsstandard höher

Nachteile:

- wird bei großer Anzahl von Rechten schnell unübersichtlich und langsam
- Administration wird aufwendig
- zentraler Systemverwalter für die Rechtevergabe notwendig

Prinzip $\mathcal{B}$ liefert ein **offenes** System. Hier gilt:

Es ist alles erlaubt, was nicht ausdrücklich verboten wird.

Vorteile:

+ Vergabe und Kontrolle der Rechte ist weniger aufwendig

Nachteile:

- Sicherheit ist schlechter nachprüfbar

- Ausnutzen von unbekannten Sicherheitslücken möglich, deshalb ständiges Beobachten des Systems und Suche nach neuen Sicherheitsproblemen notwendig
  (Administrator gefordert)

3.3.2 Modelle der Rechteverwaltung

Die genannten Prinzipien können in mehr oder weniger reiner Form durch verschiedene Modelle der Rechteverwaltung realisiert werden. Diese Modelle sind Gegenstand des nächsten Abschnitts der Vorlesung. Die Modelle können in zwei Gruppen eingeteilt werden:

1. Modelle mit individueller Zuordnung der Rechte
   (engl.: discretionary security models)

   Auf Grund von Nutzer- und Objektidentifikation wird zwischen jedem Subjekt und jedem Objekt festgelegt, welche Rechte das Subjekt am Objekt hat.

2. Modelle mit regelbasierter / erzwungener Zuordnung der Rechte
   (engl. mandatory security models)

   Subjekte und Objekte unterliegen Klasseneinteilungen. Zwischen den Klassen bestehen Beziehungen, aus denen nach einem Regelwerk die Rechte für die Klassenelemente vom System abgeleitet werden.

3.4 Beweissicherung

Die Beweissicherung umfaßt insbesondere die Protokollierung der Ausübung bzw. des Versuchs der Ausübung von Rechten. Aus praktischen Gründen spielt dabei das Granulat des Protokolls eine wichtige Rolle:

- Auswertungsprobleme - falls das Granulat zu fein gewählt wurde.
- Nichterkennen von sicherheitsrelevanten, interessanten Zugriffen oder Zugriffsversuchen, falls das Granulat des Protokolls zu grob gewählt wurde.

Zu den Aufgaben der Beweissicherung zählt die Bereitstellung von Mechanismen zur Auswertung der Protokollendaten, um im Fall einer Rechteverletzung, Aktionen und Reaktionen der Betroffenen nachvollziehen zu können. Davon können aber auch Rückschlüsse auf Systemfehler und ggf. die Einleitung von Vorsorgemaßnahmen abhängig sein.
Man unterscheidet zwei Arten der Auswertung und Speicherung von Protokolldaten:

- **Accounting:** grundsätzliches Speichern aller Vorgänge.
  Damit kann ein Beitrag sowohl zur Datensicherheit geleistet werden (Datenmanipulationen nachvollziehbar und ggf. an Hand des Protokolls korrigierbar - roll back) als auch zum Datenschutz (Nachweis der Informationssammlung über mehrere Zugriffe hinweg).
- **Auditing:** zielgerichte Suche nach Sicherheitsverstößen bzw. entsprechenden Versuchen.

Wesentliches Merkmal der Beweissicherung sind die eigene Sicherheit und die eigene Integrität. Nur dadurch ist ihre Beweiskraft gegeben. Deshalb ist eine vom zu sichernden System unabhängige Funktion der Beweissicherung zu realisieren, die auch im Falle von Systemfehlern, Attacken noch zuverlässig arbeitet. Auf Grund ihrer dokumentierenden Funktion sind die Protokolle auch Ziel von vorsätzlichen Angriffen, um Spuren der Attacken auf andere Daten zu vernichten, und bedürfen besonderen Schutzes gegen unbefugte Manipulation und Vernichtung.[13]

Eine Möglichkeit zur (vom Zielsystem) unabhängigen Beweissicherung ist der Einsatz eines **Log-Servers**. Dieser verfügt lediglich über eine Schnittstelle (z.B. ein serieller Eingang) zur Entgegennahme der Protokolldaten vom Zielsystem. Ansonsten ist er völlig unabhängig und ggf. baulich vor unbefugten Zugriff geschützt. Der Server prüft selbständig seine freien Ressourcen (wie z.B. Plattenspeicherplatz) und signalisiert akkustisch kritische Zustandsänderungen. Die Protokolldaten werden mit Zeit und kryptographischer Prüfsumme (Hashwert) gespeichert und ggf. ausgewertet.
Da dieser Rechner nicht im Netzwerk eingebunden ist, können die gespeicherten Daten nur physikalisch (große Magnetfelder) oder vor Ort (an der Konsole) manipuliert werden. Leider können sie auch zur Kontrolle nur vor Ort gelesen werden.

Eine andere Möglichkeit wäre die Benutzung eines nur einmal beschreibaren Speichermediums.

3.5 Wiederaufbereitung von Ressourcen

Alle Betriebsmittel, deren Benutzung zwischen verschiedenen Subjekten geteilt wird, müssen nach ihrer Verwendung aufbereitet werden, d.h. von evt. dort noch vorhandenen Daten befreit werden. Dadurch soll

- ein unerlaubter Informationsfluß zwischen Subjekten verhindert

und

[13] Beispiel aus aktuellem Anlaß: Beim „Hacken“ der PC mit UNIX-artigen Betriebssystemen zur Vorbereitung von Massenanfragen an Web-Server werden (fast) alle Protokolldateien manipuliert, so daß die Tatsache, daß der Rechner nicht mehr vertrauenswürdig war, verschleiert blieb.

- die Integrität der Daten erhalten werden.

Diesem Ziel dienen u.a. folgende Maßnahmen:

- vollständiges Löschen von Speicherbereichen (Wipeing) bei Start und Ende der Nutzung
- Neuinitialisierung der Betriebsmittel vor neuem Gebrauch.
  Benutze Betriebsmittel und Geräte sollen sich vor Beginn und nach Ende der Nutzung in einem wohldefinierten Zustand befinden.
- Schließen von Dateien und Zurücksetzen von Geräten bei abnormalem Programmende
- Mehrfaches systematisches Überschreiben der Informationen auf magnetischen Datenträgern mit Nullen, Einsen und zufälligen Bitmustern (Löschen zerstört nur die Verzeichniseinträge, läßt die Daten unverändert, einfaches Überschreiben der Daten erlaubt durch Analyse der Feinstruktur der Magnetschicht Datenrekonstruktion)

3.6 Wahrung der Integrität

Hierunter fallen alle Maßnahmen, die die Korrektheit und Konsistenz von Daten sichern. In Datenbanksystemen existieren Mechanismen (Primär- und Fremdschlüsseldefinitionen, Trigger) zu dieser Grundfunktion. In anderen Bereichen werden solche Maßnahmen erst entwickelt. Durch die zunehmende Verbreitung des e-Commerce ist derzeit diese Fragestellung für den Datenaustausch im Internet von großer Bedeutung.

3.7 Fehlerüberbrückung

Möglichkeiten, die Auswirkungen bei Fehlverhalten eines Systems oder des Verlustes an Funktionalität einzuschränken.

1. Fehlererkennung - ist die notwendige Voraussetzung der Fehlerüberbrückung.
2. Fehlerüberbrückung durch Abbruch (geordneter Abbruch zur Begrenzung der Auswirkung) oder Fehlerbehebung (Redundanz z.B. durch fehlerkorrigierende Codes, Selbsttests, unabhängige Paralellsysteme[14])

Diskussionspunkte in diesem Zusammenhang:

Welche Fehler sollen überbrückt werden, welche Daten-, Funktions- und Zeitverluste können akzeptiert werden.

[14] werden z.B. in Flugzeugen eingesetzt

3.8 Garantie der Funktionalität

Die zu sichernde Funktionalität wird auch bei Störungen oder unter störenden Einflüssen aufrechterhalten.
Dazu kann auch die Einhaltung von Zeitbedingungen gehören (Prozeßsteuerung) im Fehlerfall oder unter fehlerhafter Last. Hier bestehen Beziehungen zum vorigen Punkt. Hierfür einige Beispiele:

- Sicherung des Betriebs einer Anlage über eine unterbrechungsfreie Stromversorgung (USV) zur Überbrückung von Ausfällen der elektrischen Netzversorgung
- Freihaltung von wichtigen Systemressourcen für Notfälle (z.B. Prozessnummern für den Superuser durch das Betriebssystem)
- Abarbeitung der Prozesse nach Priorität

3.9 Grundfunktionen bei der Datenkommunikation

Unter dem Stichwort *Übertragungssicherung* werden mehrere Einzelaspekte zusammengefaßt, die sowohl unter dem Gesichtspunkt Datenschutz als auch Datensicherheit zu sehen sind. Einige Aspekte der Sicherheit der Kommunikation treten auch in schon besprochenen Grundfunktionen auf, sie werden hier ggf. auf die neuen Bedürfnisse ausgerichtet.

3.9.1 Authentisierung des Senders und des Empfängers

Sender und Empfänger eines Datenstroms müssen sich beide eindeutig gegenseitig identifizieren. Dies ist i.A. eine stärkere Forderung als die in der Grundfunktion Identifizierung festgelegte. Algorithmen hierzu werden in meiner Vorlesung „Kryptographische Protokolle“ vorgestellt.

3.9.2 Vertraulichkeit der Daten

Hier ist der Begriff Daten in umfassender Bedeutung zu verstehen. Die Geheimhaltung betrifft die eigentlichen Daten und die Adressierungen. Verschlüsselung ist ein Bestandteil zur Lösung des Problems. Desweiteren existieren Protokolle, die Angaben zu Absendern und Adressaten schützen.
Auch die Tatsache, daß Daten existieren bzw. übertragen werden, ist ggf. schutzwürdig (Vertraulichkeit der Verbindungsdaten). Mit entsprechendem Hintergrundwissen ist es möglich, allein aus der Kenntnis der Tatsache, daß eine Datenübertragung stattgefunden hat, Informationen zu gewinnen (*Verkehrsanalyse*). Lösun-

gen basieren auf Verschlüsselung. Damit wird im Idealfall erreicht, daß sich die zu übertragenden, jetzt verschlüsselten Daten statistisch nicht von digitalen Zufallszahlen unterscheiden. Auf dem Übertragungskanal werden nun permanent Folgen von Zufallszahlen übertragen, in die bei Bedarf die verschlüsselte Nachricht eingeordnet wird. Das Protokoll muß nun im Detail so ausgelegt sein, daß der Empfänger diese Nachricht wieder aus dem Datenstrom extrahieren kann.
Andererseits ist das Speichern von Verbindungsdaten notwendig, wenn z.B. bei der Nutzung kostenpflichtiger Dienste Einzelabrechnung bzw. Einzelnachweis verlangt wird (z.B. ISDN- Telefonanlagen).

3.9.3 Integrität der übertragenen Daten

Die relevanten Daten müssen für den Empfänger eindeutig zu erkennen und ggf. überprüfbar sein und gegen Veränderung geschützt sein (z.B. durch digitale Signaturen).

3.9.4 Anerkennung von Daten

Ursprung und Empfang von Daten darf nicht abstreitbar sein. Dies ist z.B. für jeden rechtsverbindlichen elektronischen Dokumentenaustausch Voraussetzung. Es sind drei Teilprobleme erkennbar:

1. Identifikation und Authentisierung des Urhebers eines Datenstroms (Data Origin Authentication). Im Netzwerk wird die Urheberschaft eindeutig festgestellt, so daß sie später nicht geleugnet werden kann.
2. Der Empfänger kann nachweisen, daß der zu einem Datenstrom ihm genannte Sender auch tatsächlich der Sender ist.
3. Der Sender eines Datenstroms kann beweisen, daß der Empfänger die Daten auch tatsächlich erhalten hat.

Die Punkte 2 und 3 ergeben den ISO-Begriff *Non-repudiation*.
Negativbeispiele zu dieser Thematik liefert das derzeit benutzte Verfahren zur Übertragung von elektronischer Post (e-mail).
Protokolle zur Lösung dieser Teilproleme beruhen beispielsweise auf der Einschaltung eines von allen Beteiligten als vertrauenswürdig eingeschätzten Kommunikationszentrums, über das der Nachrichtenaustausch erfolgt und dessen Aussagen in einem Beweisverfahren als „wahr“ akzeptiert werden (Notarfunktion).

4 Modelle

4.1 Matrix-Modelle

4.1.1 Matrix-Modell nach Harrison, Ruzzo und Ullmann

Historische Entwicklung:

- 1971 von Lansgram für Betriebsysteme eingeführt
- 1997 durch Graham erweitert
- 1976 formale Beschreibung durch Harrison

Bestandteile des Modells:

1. Subjekt: Benutzer bzw. ein aktiver Prozess
2. Objekt: passive Dinge, wobei $\mathcal{O} \supset \mathcal{S}$ gilt
3. Matrix der Rechte $A(\mathcal{S}_i, \mathcal{O}_j)$: A enthält eine Aufzählung von Rechten, die $\mathcal{S}_i$ gegenüber $\mathcal{O}_j$ hat, mit folgenden Bedingungen:
   - zeitabhängig und abhängig vom Inhalt (Stichwörter, Schutzvermerke)
   - kontextabhängig, d.h. Zugriff auf die Daten darf z.B. nur von sicheren Terminals erfolgen
   - abhängig von der Vorgeschichte der Zugriffe

Operationen auf der Matrix:

- Eintragen eines Rechtes r in $A(\mathcal{S}_i, \mathcal{O}_j)$
- Austragen eines Rechtes r aus $A(\mathcal{S}_i, \mathcal{O}_j)$
- Erzeugen eines neuen Subjekts s, d.h. $\mathcal{S} = \mathcal{S} \cup \{s\}$
  (Ggf. müssen hierbei Default-Rechte in $A(\mathcal{S}_i, \mathcal{O}_j)$ gesetzt werden.)
- Erzeugen eines neuen Objekts o, d.h. $\mathcal{O} = \mathcal{O} \cup \{o\}$
  (Ggf. müssen hierbei Default-Rechte in $A(\mathcal{S}_i, \mathcal{O}_j)$ gesetzt werden.)
- Entfernen eines Subjekts, Objekts und aller zugehörigen Matrixeinträge
  (Beachte: Objekte könnten auch als Subjekte eingetragen sein !)

- Prüfung[15] von Zugriffen, z.B. `if` $\bigwedge_{\forall i,j}(r_i \in A(x_i, x_j))$ `then` $\underbrace{\{\phi_1, \phi_2, \ldots\}}_{\text{Folge von Operationen}}$

Forderungen zur Rechtevergabe:

- Rolle des Besitzers: Nur er hat das Privileg, die Rechte seiner Objekte zu vergeben.
- Die Rolle des Besitzers kann nicht weitergegeben oder übertragen werden. Hierdurch wird die Sicherheit des Systems garantiert.
- Ein Besitzer kann seine Rechte nicht selbst vergrößern.

Abschwächung hinsichtlich der Weitergabe von Rechten:
Eine Abschwächung dieser Forderungen hinsichtlich der Weitergabe von Rechten ist denkbar: *Der Benutzer darf Rechte, die er selbst besitzt, auch weitergeben.*

Dabei tauchen folgende neue Fragestellungen auf:

- Gibt der Besitzer die Rechte ansich oder nur eine Kopie weiter ?
- Welche Regelungen gibt es hinsichtlich eines zusätzlichen „Weitergabe"-Rechtes ?

Effizente Verwaltung der Matrix $A(\mathcal{S}_i, \mathcal{O}_j)$:

- schwach besetze Matrizen können als Liste gespeichert werden
- zeilen- oder spaltenweise Speicherung je nach Zugriffscharakteristik

Eigenschaften des Modells:

- sehr mächtig und flexibel, aber mit zunehmender Größe schnell unübersichtlich
- keine internen Mechanismen zur Kontrolle der Konsistenz der Matrix, da es keine allgemeinen Regeln gibt
- bietet Angriffspunkte für *Trojanische Pferde*

[15] Die Struktur der Matrix impliziert bei komplexen Kommandos eine dynamische Auswertung der Bedigungen. Bei einfachen Kommandos ist jedoch auch eine statische Auswertung möglich.

4.1.2 Take-Grant-Modell

Historische Entwicklung:

- 1976 als Erweiterung der Matrixmodelle vorgestellt

Grundidee des Modells:

- Subjekte und Objekte sind die Knoten eines Graphen
- Kanten des Graphen repräsentieren die Rechte

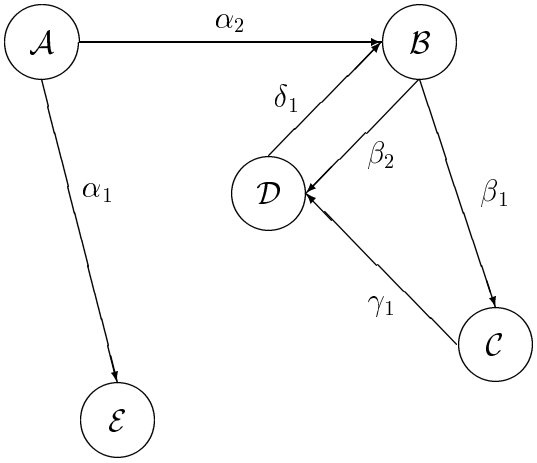


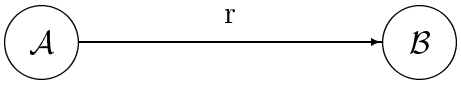
Abbildung 2: Darstellung von Rechten als Graph

- $\mathcal{A}$ hat das Recht α_1 an $\mathcal{E}$ und das Recht α_2 an $\mathcal{B}$
- $\mathcal{B}$ hat das Recht β_1 an $\mathcal{C}$ und das Recht β_2 an $\mathcal{D}$
- $\mathcal{C}$ hat das Recht γ_1 an $\mathcal{D}$
- $\mathcal{D}$ hat das Recht δ_1 an $\mathcal{B}$

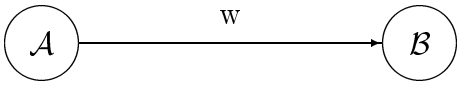
	$\mathcal{A}$	$\mathcal{B}$	$\mathcal{C}$	$\mathcal{D}$	$\mathcal{E}$
$\mathcal{A}$		α_2			α_1
$\mathcal{B}$			β_1	β_2	
$\mathcal{C}$				γ_1	
$\mathcal{D}$		δ_1			
$\mathcal{E}$					

Abbildung 3: Adjazenzmatrix des Graphen

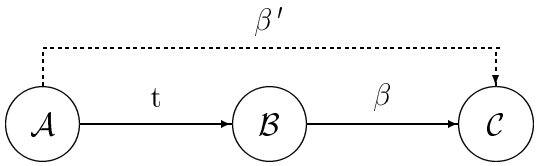
- Speicherung der Rechte in einer Adjazenzmatrix A_{ij}, wobei $a_{ij} \subseteq \{r, w, t, g\}$. Das Subjekt $\mathcal{S}_i$ hat dann diese Rechte am Objekt $\mathcal{O}_j$.
- Die Rechte $\{r, w, t, g\}$ sind wie folgt festgelegt:
  - *Leserecht:* $\mathcal{A}$ darf Inhalt von $\mathcal{B}$ lesen



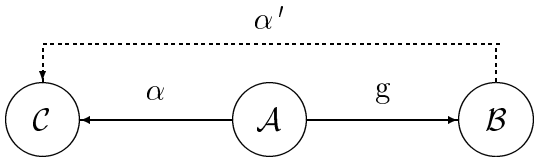
  - *Schreibrecht:* $\mathcal{A}$ darf in $\mathcal{B}$ schreiben



  - *Take-Recht:* $\mathcal{A}$ darf Recht β von $\mathcal{B}$ übernehmen



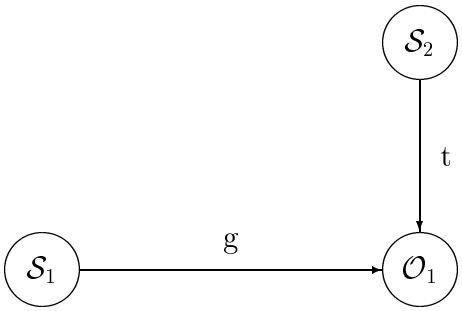
  - *Grant-Recht:* $\mathcal{A}$ darf Recht α an $\mathcal{B}$ weitergeben



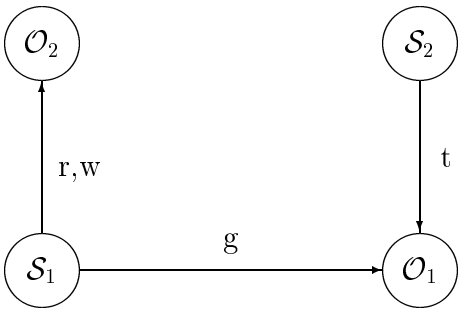
Eigenschaften des Modells:

- sonstige Nachteile des Matrixmodells
- `take` und `grant` wirken global auf alle Rechte und erlauben damit keinen differenzierten Zugriff (zu grob)
- keine Kontrolle über Ausbreitung von Zugriffsrechten

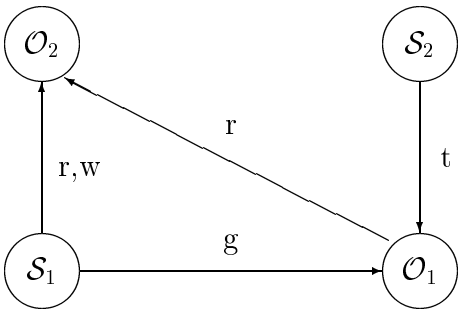
Kritische Bemerkung: Der Verbleib von Rechten kann bei der Vergabe nicht eindeutig gesichert werden (unbeabsichtigte Weitergabe).



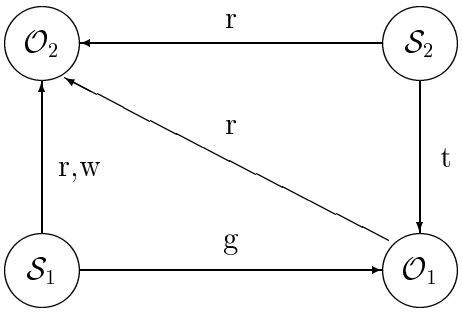
Ausgangssituation



$\mathcal{S}_1$ erzeugt $\mathcal{O}_2$ mit r,w-Rechten



$\mathcal{S}_1$ gibt r-Recht an $\mathcal{O}_1$ weiter



$\mathcal{S}_2$ übernimmt r-Recht an $\mathcal{O}_2$
(von $\mathcal{S}_1$ nicht beabsichtigt)

4.2 Regelbasierte Modelle

Diese Modelle werden oft auch unter dem Begriff *mandatory access control* (MAC) zusammengefasst. Die grundlegende Idee ist ein systemweites Regelwerk, welches den Zugriff von Subjekten auf Objekte kontrolliert.

Jeder Versuch wird gegen die Regeln abgeprüft und der Zugriff erlaubt, falls ...

1. eine Regel existiert, die den Zugriff explizit erlaubt (abgeschlossenes System).
2. es **keine** Regel gibt, die den Zugriff verbietet (offenes System).

Administration des Systems heißt also in diesem Zusammenhang das Verwalten und Aufstellen der Regeln.

4.2.1 Schutzklassen-Modell

Es gibt hier neben den Subjekten und Objekten noch ein vollständig geordnetes System von Schutzstufen.

Beispiel 4.1 (Dokumentenschutzstufen)
offen $\prec$ *nur für den Dienstgebrauch* $\prec$ *vertraulich* $\prec$ *streng vertraulich* $\prec$ *geheim* $\prec$ *streng geheim*

Die Subjekte und Objekte werden hinsichtlich dieser Schutzstufen klassifiziert:

- **Objekte:** Schutzstufe ist die Schutzwürdigkeit.
- **Subjekte:** Schutzstufe ist die Ermächtigung/Vertrauen, die/das ein Subjekt im System genießt.

Hauptziel: Schutz der Information vor dem „Abfließen“ in weniger vertrauenswürdige Bereiche.

Lösung:

- Subjekt $\mathcal{S}$ darf Objekt $\mathcal{O}$ lesen, wenn seine Ermächtigung mindestens so hoch ist, wie die Schutzwürdigkeit des Objektes.
- Subjekt $\mathcal{S}$ darf in ein Objekt $\mathcal{O}$ schreiben bzw. es erzeugen, wenn dessen Schutzwürdigkeit mindestens so hoch ist, wie die Ermächtigung des Subjekts.
- Subjekt $\mathcal{S}$ darf nur solche neuen Subjekte erzeugen, deren Ermächtigung nicht größer als die eigene ist (Hierarchieerhaltung).

Beispiel 4.2 (Problematik) *Ein Geheimnisträger liest das offene Telefonbuch und macht sich einen Auszug daraus. Nach der Schreibregel ist dieser Auszug mindestens als „geheim“ einzustufen.*

Ausweg: Ein möglicher Ausweg wäre eine inhaltliche Prüfung mit Einzelfallentscheidung. Dieser Ansatz verlässt allerdings schon die regelbasierten Systeme, da ein solches Vorgehen nicht mehr durch allgemeine Regeln beschrieben werden kann.

Prinzip des notwendigen Wissens: Dieses Prinzip (auch mit `need-to-know` Strategie bezeichnet) wird in *orthogonalen Regelsystemen* eingesetzt. Dabei wird die „gesamte“ Welt in disjunkte Klassen $B = \{b_1, b_2, \ldots\}$ aufgeteilt. Zu jedem Subjekt wird ein Zuständigkeitsbereich erklärt, der die Klassen enthält, zu denen das Subjekt Zugriff haben sollte. Jedem Objekt wird ein Arbeitsbereich zugeordnet, der ggf. aus mehreren Klassen besteht.

Ziel: Verhinderung der Informationsausbreitung aus ursprünglichem Bereich.

Regeln:

- Subjekt $\mathcal{S}$ darf Objekt $\mathcal{O}$ lesen, wenn $B_\mathcal{S} \supseteq B_\mathcal{O}$ gilt, d.h. $\mathcal{S}$ muß für alle Bereiche zuständig sein, denen $\mathcal{O}$ zugeordnet ist.
- Subjekt $\mathcal{S}$ darf $\mathcal{O}$ schreiben bzw. erzeugen, falls $B_\mathcal{S} \subseteq B_\mathcal{O}$ zutrifft.
- Subjekt $\mathcal{S}_{\texttt{alt}}$ darf nur neue Subjekte $\mathcal{S}_{\texttt{neu}}$ mit $B_{\mathcal{S}_{\texttt{neu}}} \subseteq B_{\mathcal{S}_{\texttt{alt}}}$ erzeugen.

4.2.2 Bell-LaPadulla-Modell

Historische Entwicklung:

- als Kombination von Schutzklassen und Prinzip des notwendigen Wissens 1976 vorgestellt

Ziel: Abfluß der Information in weniger geschützte Bereiche verhindern

4.2.3 Clark-Wilson-Modell

Historische Entwicklung:

- 1987 im Bereich Datenbanksicherheit entwickelt

Ziel: Erhalt der Integrität von Daten

Idee: induktive Herangehensweise, d.h.

1. Ausgangszustand des Systems ist sicher
2. nur sichere Zugriffe sind erlaubt
3. System ist auch danach sicher

Aufbau: 2 Typen von Prozeduren sind vorgesehen:

1. Integritätsprüfungsprozeduren (IVP)
2. erlaubte Transaktionen (TP)

Regeln des Clark-Wilson-Modells:

(E1) Innerhalb des Systems ist zu gewährleisten, daß nur die in (C2) definierten und um System gespeicherten Relationen zur Anwendung kommen.

(E2) Im System muß eine Liste gespeichert sein, aus der hervorgeht, welches Subjekt welche TP auf welche Objekte anwenden darf. Nur hiermit im Einklang stehende Aktionen dürfen ausgeführt werden.

(E3) Jedes Subjekt, das eine TP ausführen möchte, muß zuvor identifiziert und authentisiert sein.

(E4) Nur derjenige, der die Funktion der Zertifizierung übernimmt, darf die Zugriffslisten (speziell im Hinblick auf TP's) ändern.

(C1) Die IVP's müssen sicher feststellen können, ob alle Objekte in einem gültigen Zustand sind.

(C2) Der Sicherheitsbeauftragte legt einen Satz von Relationen fest, die beschreiben, welche TP's auf welche Objekte zugreifen dürfen. Die TP's sind dahingehend zu zertifizieren, daß sie die Integrität der Objekte, auf die sie zugreifen dürfen, erhalten.

(C3) Die Liste aus (E2) muß zertifiziert sein.

(C4) Es muß ein Objekt für die fortlaufende Protokollierung aller Transaktionen existieren. Die TP's müssen dahingehend zertifiziert sein, daß sie alle Aktionen dort so aufzeichnen, daß sie anschließend wieder rückgängig gemacht, d.h. die Objekte in den vorherigen Zustand versetzt werden können.

(C5) Können Objekte, die im System nicht von der Integritätspolitik erfaßt werden, als Eingabedaten für TP's verwendet werden, so muß gesichert (Zertifizierung !) sein, daß die betreffende TP nur zulässige Verarbeitungen ausführt oder die Objekte ggf. zurückweist.

5 Normen, Standards und Zertifikate

In diesem Abschnitt soll das Herangehen an die Probleme einer Standardisierung diskutiert werden. Außer den besprochenen Vorschlägen existieren weitere. Auch ist das Gebiet mit dem Fortschreiten der Technologie einer starken Weiterentwicklung unterworfen. Mit der Auswahl ist keine Wertung verbunden.

5.1 Das amerikanische Orange Book

1985 wurden im Orange Book vier Funktionalitätsklassen A bis D mit Unterklassen beschrieben:

$$D \prec C1 \prec C2 \prec B1 \prec B2 \prec B3 \prec A1.$$

Sie erhalten eine hierarchische Ordnung, indem eine weiter rechts stehende Klasse die Anforderungen der links von ihr stehenden Klassen enthält. Die Details zeigt folgende Übersicht:

- Klasse D: In dieser Klasse landen automatisch alle Produkte, die sich für keine andere Klasse qualifizieren konnten.
- Klassen C: Genau die sicherheitsrelevanten Funktionen des informationsverarbeitenden Systems bilden die *Trusted Computing Base* (TCB), die Gegenstand der Sicherheitsuntersuchungen ist.
  Individuelle Rechtevergabe (DAC) als Basis des Schutzes.
  - Klasse C1: Kooperative Nutzer mit gleichem Grad an Schutzwürdigkeit der Daten
  - Klasse C2: Feineres Granulat der Zugriffskontrolle, login-Prozedur, Protokollierung sicherheitsrelevanter Ereignisse, Isolation der genutzten Ressourcen von anderen Nutzern
- Klassen B: Zusätzlich regelbasierter Zugriffsschutz , Einführung eines *Referenzmonitors*
  - Klasse B1 (*Labeled Security Protection*): informelle Darstellung des Sicherheitsmodells, Daten einstufbar, exakte Einstufung exportierter Informationen
  - Klasse B2 (*Structured Protection*): Die TCB basiert auf klar definiertem und dokumentiertem formalen Modell der Sicherheitspolitik und besitzt eine wohl definierte Schnittstelle. Das TCB-Design und die Implementierung sind Gegenstand von Prüfungen.
  - Klasse B3 (*Security Domains*): Die TCB muß die Referenzmonitoreigenschaften erfüllen und übersichtlich (klein) sein, so daß sie selbst

analysiert und getestet werden kann. Sicherheitsadministrator wird unterstützt, sicherheitsrelevante Ereignisse werden vom Protokollmechanismus signalisiert, Recovery-Proceduren werden gefordert.

- Klasse A (A1): Funktional wie B3. Formale Techniken der Spezifikation und Verifikation beim Entwurf des Systems gefordert.

Bemerkungen: Einige wichtige Bereiche wie Kommunikation über Netze und auch Vefügbarkeitsforderungen bei Prozeßsteuerung werden nicht erwähnt, die Sicherheit in vernetzten Systemen war in Erscheinungsjahr 1985 noch nicht derartig praxisrelavant wie heute. Bei den Forderungen wurden solche nach der Funktionalität, zu Konzepten, zur Korrektheit der Implementierung gemeinsam in die Klassendefinition aufgenommen. Damit sind einige sinnvolle Kombinationen von Funktionalität und Qualität nicht möglich.

5.2 Die deutschen Funktionalitätsklassen

Bei der Entwicklung der deutschen Funktionalitätsklassen wurden die funktionellen Anforderungen von den sicherheitspolitischen Ansätzen zu ihrer Realisierung getrennt. Desweiteren wurden Anforderungen zur Verfügbarkeit bzw. Ausfallsicherheit, die insbesondere in der Prozeßrechentechnik eine wichtige Rolle spielen, ergänzt. Weiterhin wurden Funktionalitätsklassen geschaffen, die sich mit der Sicherheit der Datenübertragung in Netzwerken befassen. Damit ergibt sich für das Gesamtsystem der Klassen kein vollständiger hierarchischer Aufbau, einige Anforderungen sind naturgemäß nicht mit anderen Anforderungen vergleichbar. Andererseits ergeben sich auch Überlappungen/Berührungen.
Insgesamt wurden zehn Funktionalitätsklassen definiert, von denen die Klassen F1 bis F5 Anforderungen an das Betriebssystem festschreiben. Diese Klassen sind hierarchisch geordnet und können mit den Klassen des Orange Book wie folgt verglichen werden:

ITS	Orange Book
F1	C1
F2	C2
F3	B1
F4	B2
F5	B3/A1

Dabei sind die deutschen Klassen nicht schwächer als die vergleichbaren des Orange Book, d.h. erfüllt ein Produkt die Forderungen einer deutschen Funktionalitätsklasse, so auch die der entsprechenden Klasse des Orange Book.

Die Klasse F6 befaßt sich mit Integritätsforderungen, wie sie typischerweise in Datenbanksystemen auftreten, aber auch im Bereich der Betriebsysteme eine Rolle spielen. In der Klasse F7 werden Anforderungen hinsichtlich der *Fehlerüberbrückung* für Hardwarekomponenten und *Gewährleistung der Funktionalität* beschrieben.
Fragen der *Vernetzung von Systemen* und der *Datenübertragung* werden in den Klassen F8 bis F10 behandelt.
Eine detaillierte Beschreibung der Funktionalitätsklassen findet sich in [3], deshalb werden hier nur in Stichworten die betroffenen Grundfunktionen genannt.

F1: Identifikation und Authentisierung
Rechteverwaltung
Rechteprüfung

F2: Wie F1, aber detaillierter
Beweissicherung
Wiederaufbereitung

F3: neu: Attribute als Grundlage regelbasierter Zugriffsrechte

F4: detaillierter,
neu: vertrauenswürdiger Pfad für Identifzierung und Authentisierung
Rollen bei Rechteverwaltung

F5:

F6: Fragen der Integritätssicherung, Typkonzept

F7: Verfügbarkeit
Fehlerüberbrückung
Gewährleistung der Funktionalität

F8: Datenübertragung in Netzwerken - Integrität

F9: Datenübertragung in Netzwerken - Vertraulichkeit

F10: Datenübertragung in Netzwerken - Zusammenfassung

Beispiel: Einordnung von UNIX-artigen Betriebssystemen nicht schematisch möglich, es liegt zwischen F1 und F2.

5.3 Der Evaluierungs- und Zertifizierungsprozeß in Deutschland

5.3.1 Komponenten einer Bewertung

Definition 5.1 Mechanismus: *Unter einem Mechanismus versteht man die Verfahren, Algorithmen, Festlegungen usw., mit denen eine Grundfunktion oder eine Gruppe von Grundfunktionen eines informationstechnischen Systems realisiert ist.*

Von Mechanismus ist seine Implementierung / Realisierung klar zu unterscheiden. Folglich gibt es auch bei der Bewertung zwei Gesichtspunkte: Die Bewertung des Mechanismus, seiner Schwächen einerseits (*Stärke*) und die Bewertung der der Implementierung bzw. andersgearteten technischen Umsetzung andererseits (*Qualität der Implementierung bzw. des Herstellungsvorgangs*).

Bewertung der Stärke

Definition 5.2 Die Stärke eines Mechanismus *besteht in der Resistenz gegen Manipulations- / Täuschungsversuche. Maßstab der Bewertung sind die zur Manipulation nötigen Kenntnisse (+ Verbreitungsgrad), der zeitliche und finanzielle Aufwand, die Verfügbarkeit der benötigten Hilfsmittel.*

Damit wird die Beurteilung der Stärke nur verbal möglich und vom subjektiven Kenntnisstand des Beurteilenden abhängig. Selbstverständlich ist die Einschätzung auch zeitlich veränderlich - in Abhängigkeit von Entwicklung und Verfügbarbeit von Hard- und Software.
Die deutschen Bewertung hat eine sechsstufige Skala, die nicht von der Funktionalität abhängt.

- **ungeeignet:**
  Der Mechanismus erfüllt die Anforderungen nicht.
- **schwach:**
  Abwehr unbeabsichtigter Verstöße.
- **mittelstark:** Schutz bei absichtlichen Verstößen, mit mittelgroßem Aufwand und normalen Systemkenntnissen brechbar.
- **stark:** guter Schutz bei absichtlichen Verstößen, mit großem Aufwand oder mit aufwendigen Hilfsmitteln brechbar. Organisatorische Maßnahmen, mit denen die Stärke des Mechanismus gesichert wird, müssen recht einfach geartet und wenig fehleranfällig sein. Ggf. müssen Methoden zur Erkennung und Vermeidung von Fehlern implementiert sein.

- **sehr stark:** sehr guter Schutz bei absichtlichen Verstößen, mit sehr großem Aufwand oder mit sehr aufwendigen Hilfsmitteln brechbar. Organisatorische Maßnahmen, mit denen die Stärke des Mechanismus gesichert wird, müssen relativ einfach geartet und wenig fehleranfällig sein. Mögliche Fehlerquellen ... müssen weitgehend vom System überwacht werden.

- **zur Zeit nicht überwindbar:** nicht überwindbarer Schutz vor absichtlichen Verstößen. Als organisatorische Maßnahmen höchstens solche zulässig, die praktisch vollständig gegen Fehler abgesichert sind.

Die Bewertung einer Gruppe von Einzelmechanismen kann generell nicht besser als die schlechteste Einzelbewertung sein, es sei denn, daß Schwächen eines Mechanismus ausdrücklich durch andere Mechanismen kompensiert werden.

Die Stufen des Orange Book enthalten auch Forderungen an die Stärke, deshalb ist folgende Gegenüberstellung möglich:

Orange Book	Dt. Kriterien
D	ungeeignet
C1 / C2	mittelstark
B1 / B2	stark
B3 / A1	sehr stark

Verbundene Metriken: Bisher wurden drei Kriterien zur Beurteilung diskutiert: Funktionalität, Stärke des Mechanismus und Korrektheit der Implementierung. Es ergibt sich ein dreidimensionaler Bewertungsraum, der schwer zu übersehen ist. Desweiteren machen auch nicht alle Kombinationen einen Sinn (es ist sinnlos, bei einen starken Mechanismus die Korrektheit der Implementierung nur an einigen Beispielen zu testen).
Der diametral entgegegengesetzte Weg ist die Verbindung der drei Kriterien zu einer Klasseneinteilung, wie er im Orange Book gegangen wurde. Es macht durchaus Sinn, eine „niedere“ Funktionalitätsklasse wie F3 mit starken Mechanismen, die korrekt implementiert sind, zu realisieren. Dies motiviert eine Kopplung von Stärke und Korrektheit zu einer Qualität, die in 8 Q-Stufen ausgedrückt wird.

Stufe	Mechanismus	Korrektheit
Q0	unwirksam/max. schwach	unzureichend
Q1	mittelstark *)	getestet
Q2	mittelstark	methodisch getestet
Q3	stark *)	methodisch getestet, teilanalysiert
Q4	stark	informell analysiert
Q5	sehr stark *)	semiformal analysiert
Q6	sehr stark	formal analysiert
Q7	nicht überwindbar *)	formal verifiziert

*) Ausnahmen möglich

Zur Abwertung in Stufe Q0 reicht es aus, wenn eines der beiden Merkmale, wie in der Tabelle angegeben, eingestuft wird; bei den anderen Stufen müssen beide Merkmale die Einstufung erfüllen.

5.3.2 Evaluierungsprozess

Die Grundlagen werden in folgenden Dokumenten beschrieben:

- *IT-Sicherheitskriterien*
- *IT-Evaluationshandbuch*
- *IT-Sicherheitshandbuch*

Aus naheliegenden Gründen müssen diese Dokumente aktuell gehalten werden bzw. ersetzt / ergänzt werden. Herausgeber und Ansprechpartner ist das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Definition 5.3 Evaluierung *ist die Prüfung eines Systems oder einer Komponente hinsichtlich seiner Sicherheitseigenschaften auf der Basis von Funktionalitätsmerkmalen und angestrebter Qualitätsstufe.*

Definition 5.4 Zertifizierung *beinhaltet das Veröffentlichen eines Prüfberichts und eines Prüfzeugnisses.*

Die Zertifizierung erfolgt derzeit durch das BSI.

Die Prüfung selbst ist ein mehrstufiger, ggf. Monate in Anspruch nehmender Vorgang, bei der die antragstellende Firma und die prüfende Einrichtung kooperativ zusammenarbeiten.

- **Vorbereitungsphase**

  - Vorgespräche, Klärung der Funktionalität, angestrebte Q-Stufe, benötigte Dokumente
  - Antragstellung
  - Personal- und Ressourcenplanung, Schulung, Pilotstudien ..., Terminpläne
  - Vertragsabschluß (Schutz der Firmeninterna des Herstellers, Zeitplan, Kosten)

- **Dokumenten-Prüfung**
  Prüfung der vom Hersteller vorgelegten Dokumentation auf Vollständigkeit und Widerspruchsfreiheit.
- **System-Tests**
  Prüfung, ob das vorgelegte Produkt mit der Dokumentation übereinstimmt, die Schärfe der Prüfung entspricht der Q-Stufe.
- **Bewertungsphase**
  Auswertung der Prüfungsergebnisse
- **Abschluß der Evaluierung**
  Erstellen eines *internen* Evaluationsberichts, der alle Ergebnisse der Prüfung zusammenfaßt und mit konkreten Verweisen auf Produkteigenschaften und Produktinterna begründet. Dieser Bericht kann wegen der enthaltenen Details nicht veröffentlicht werden (Schutz des Herstellers vor Mißbrauch seines Wissens und seiner Technologie).

In allen Phasen außer dem Abschluß können geringfügige, durch die Prüfung offenbar gewordene Mängel durch den Hersteller beseitigt / nachgebessert werden.

5.3.3 Ergebnisdarstellung

Auf der Grundlage des o.g. Berichts erfolgt die Zertifizierung. Dazu wird zunächst der Bericht durch Personen, die nicht an der Evaluierung beteiligt waren, intensiv geprüft, Einzelergebnisse ggf. verifiziert. Führt dies nicht zur Ablehnung des Berichts, wird das Zertifikat ausgestellt. Es besteht aus einem Zeugnis über die erreichten F- und Q-Stufen und einem offenen Bericht. Dieser beschreibt die Sicherheitseigenschaften, Auflagen, Risiken. Interessenten können dieses Zertifikat beim Hersteller oder dem BSI abfordern, welches eine Liste der zertifizierten Produkte führt.

Das Zertifikat wird grundsätzlich für ein konkretes Produkt erteilt, verliert also bei Veränderungen des Produkts oder seiner Erstellungstechnologie (z.B. Compilerwechsel) seine Gültigkeit. Bei der Erweiterung eines Zertifikats kann ggf. der

Prüfvorgang auf geänderte Bestandteile und ihre Einpassung in das Restsystem eingeschränkt werden.

5.3.4 Kombination elvaluierter Produkte

Grundsätzlich bedarf die Kombination einer Nachbewertung. Wenn jede der Komponenten bereits eine Bewertung in der angestrebten Gesamtstufe hat, ist zu sichern, daß die Anforderungen und ihre Aufteilung auf die zu kombinierenden Produkte genau beschrieben werden und durch die Kombination der Produkte auch tatsächlich vollständig abgedeckt werden, daß die Wirkung der Teilkomponenten durch die Kombination nicht beeinträchtigt wird. Dies muß bei der Bewertung der Einzelprodukte nicht Gegenstand der Evaluation gewesen sein. Weiterhin ist die ausreichende Abgrenzung der sicherheitsrelevanten Bestandteile von den nicht evaluierten Systemkomponenten auch für die Produktkombination zu prüfen.

5.3.5 Beispiele

- Bewertung der login-Prozedur in UNIX-Betriebssystemen mit Passwortablage in der Datei */etc/passwd*, Vergleich zwischen den Bewertungen von 1990 und 2000.

Literatur

[1] Adam, Uwe: *Einführung in die Datensicherheit*,
Vogel Buchverlag, 1995

[2] Castano, Silvana; Fugini, Mariagrazia; Martella, Giancarlo;
Samarati, Pierangela: *Database security*, Addison-Wesley, 1994

Der Erfolg im Wettbewerb um den Kunden und das öffentliche Vertrauen in Regierungsbehörden hängt oft von der Sicherheit der Informationen ab, die in den Datenbanken dieser Institutionen gespeichert sind. Sicherheitslücken können hier zu erheblichen Schäden führen. Dieses Buch behandelt eine Vielzahl an Sicherheitsproblemen von Datenbanksystemen und zeigt, wie derzeit eingesetzte oder zukünftige Datenbanken gestaltet werden sollten, um Sicherheit, Integrität und Vertrauenswürdigkeit zu gewährleisten. Bestandteile des Buches sind u.A.: *Vergleich und Betrachtung bezüglich der Datenbanksicherheit von Modellen, Systemen, Architekturen und Standards*, *Ausführungen zum Design von sicheren Datenbanksystemen*, *Betrachtung von verfügbaren Sicherheitsmechanismen und Vergleich der Schutzfunktionen von Betriebssystemen, DBMS und Datensicherheitssoftware*, *momentane Trends im Bereich der Datenbanksicherheit und Datenbankkontrolle anhand von objektorientierten bzw. statistischen Datenbanken*

Das Buch ist nicht nur für Datenbankadministratoren und Entwickler geeignet, sondern kann auch für IT-Manager und Sicherheitsbeauftragte in Unternehmen nützliche Hinweise geben.

[3] Heinrich, Kersten: *Einführung in die Computersicherheit*,
Serie: Sicherheit in der Informationstechnik,
R. Oldenbourg-Verlag, 1991

Hacker, Computermißbrauch, Viren und die Folgen fehlender Sicherheitsvorkehrungen beunruhigen die Öffentlichkeit zunehmend. Dieses Buch führt praxixorientiert in die grundlegenden Konzepte und Ideen des Fachgebiets Computersicherheit ein. Der Autor, Mitarbeiter des Bundesamtes für Sicherheit in der Informationstechnik, vergleicht internationale Sicherheitskriterien. Dabei berücksichtigt er wesentliche Bereiche wie *Sicherheitsprobleme und deren Lösungen*, *Bedrohungs- und Risikoanalyse*, *Sicherheitspolitiken*, *Grundfunktionen, Mechanismen und Bewertungen sicherer Systeme*, *Verfahren und Methoden des Software-Engineerings*. Listen evaluierter Produkte und ein umfangreiches Glossar runden das Buch ab.

[4] Pommerening, Klaus: *Datenschutz und Datensicherheit*,
BI Wissenschaftsverlag Mannheim/Wien/Zürich, 1991

Dieses Buch zeigt, welche Probleme beim Betrieb sicherer Rechner- und Kommunikationssysteme zu bewältigen sind. Diskutiert werden die Anforderungen des Datenschutzes, organisatorische Maßnahmen und der aktuelle Stand der Forschung. Hierbei liegt ein besonderes Gewicht auf der Informationssicherheit in offenen Systemen und ihrer Verwirklichung mit Hilfe von kryptographischen Protokollen. dem Informatiker wird gezeigt, wie sich aus den praktischen Sicherheitsproblemen Ansätze für die Forschung ergeben. Der Praktiker erhält einen Überblick über Sicherheitslücken, konkrete Handlungsanleitungen, Checklisten und eine Darstellung des Standes der Technik und der Wissenschaft.

[5] Schneier, Bruce: *Angewandte Kryptographie*,
Addison-Wesley Bonn, 1996

Dieses hervorragende Buch wird oft auch als Standardwerk zur Kryptographie bezeichnet. Es bietet einen umfassenden Einblick in die moderne Kryptographie. Das Buch beschreibt nicht nur zahlreiche kryptographische Algorithmen, sondern gibt auch praktische Hinweise zur Implementierung kryptographischer Software und zeigt, wie Sie damit Sicherheitsprobleme lösen.

Weitere Informationen zur Kryptographie bieten die Newsgroups `sci.crypt` und `sci.crypt.research`.

[6] Waltraud, Gerhardt: *Zugriffskontrolle bei Datenbanken*,
Serie: SICHERHEIT IN DER INFORMATIONSTECHNIK,
R. Oldenbourg-Verlag, 1993

[7] *Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990*,
Beck-Texte im Deutschen Taschenbuch Verlag (dtv)

[8] *Gesetz zur digitalen Signatur (SigG) vom 22. Juli 1997*,
Beck-Texte im Deutschen Taschenbuch Verlag (dtv)

[9] *Teledienstdatenschutzgesetz (TDDSG) vom 22. Juli 1997*,
Beck-Texte im Deutschen Taschenbuch Verlag (dtv)

Verweise im WWW und UseNET

[A] Computer Emergency Response Team: `http://www.cert.org`

[B] deutschsprachige Newsgroup zur Computersicherheit: `de.comp.security`

Index

Notizen