IT-Sicherheit

Teil 2 Duale Sicherheit

Rüdiger Dierstein, S.M.

TECHNISCHE UNIVERSITÄT MÜNCHEN

WS 2003/04

Funktionseinheit *(functional unit)*

ISO/IEC 2382–1

01.01.40 – **functional unit** – An entity of hardware or software, or both, capable of accomplishing a specified purpose.

nach DIN 44300

Ein nach **Aufgabe** oder **Wirkung abgrenzbares** Gebilde**.**

Funktionseinheit *(Fts.)*

Anmerkungen

Funktionseinheit sagt nichts aus über Natur, Bauweise oder Art der Abgrenzung des verarbeitenden Systems.

Ein ***System von Funktionseinheiten*** kann in einem gegebenen Zusammenhang wieder als eine Funktionseinheit aufgefasst werden.

DIN 44300 definierte zusätzlich die ***Baueinheit*** als „ein nach Aufbau oder Zusammensetzung abgrenzbares ***materielles*** Gebilde“.

Folgerung

Definiere genau, welche Elemente zu einem gegebenen Zeitpunkt als zu **einer Funktionseinheit** gehörig **betrachtet** werden und welche nicht!

Fortsetzung

Rechner, Rechensystem, Datenverarbeitungssystem
computer system, data processing system

ISO/IEC 2382–1

01.01.20 – **data processing system** – **computer system** – **computing system** – One or more computers, * peripheral equipment, and software that perform data processing

01.03.03 – **computer** – A functional unit that can perform substantial computations, including numerous arithmetic operations and logic operations without human intervention. –

NOTES – 1 A computer may consist of a stand-alone unit or several interconnected units. –
2 In English, in information processing, the term computer usually refers to a digital computer

nach DIN 44300

Eine **Funktionseinheit* zur Verarbeitung und Aufbewahrung** von Daten*

Rechner, Rechensystem, Datenverarbeitungssystem (Fts.)

Anmerkungen

- Verarbeitung nach DIN 44300 umfasst die Durchführung mathematischer, umformender, übertragender und speichernder Operationen.
- Informationsverarbeitung sollte auch die ***korrelierenden Operationen*** enthalten **–** und damit ***jede Art der Nutzung*** umfassen.
- Inder ISO/IEC bleibt offen, was unter „***substantial computations***“ einzuordnen ist und was nicht.
- Beachte, dass in ISO/IEC die Begriffe *Rechner* und *Rechnersystem* unterschieden werden

System der Informationstechnik
IT-System (it-system)

Aus ISO/IEC und DIN abgeleitet

Jedes **Gebilde**, das **Daten verarbeiten** kann und in gegebenem Kontext als **Gesamtheit** (Funktionseinheit) betrachtet wird

Verarbeiten heißt nach DIN

aufnehmen	➡	erfassen, erheben
aufbewahren	➡	speichern
weitergeben	➡	übertragen, übermitteln
umformen	➡	transformieren, operativ verknüpfen

aber auch allgemein

nutzen	➡	einschließlich der Nutzung von Daten ***außerhalb*** des Systems (vgl. BDSG)

Nutzen enthält insbesondere das

korrelieren	➡	Verknüpfen ohne Veränderung
interpretieren	➡	Insbesondere im Sinne von Bedeutung zuweisen oder zuordnen

Fortsetzung ↳

Systeme der Informationstechnik*)

- **Menschen**
- **andere Lebewesen**
- **Computer**
  - Mainframes
  - Arbeitsplatzsysteme, PCs
  - Prozessrechner, Realzeitsysteme
  - **…**
- **Rechnerkomponenten oder Subsysteme**
  - Hard- und Software-Komponenten
  - Betriebssysteme
  - Datenbanken, Anwendungssysteme
  - **…**
- **IT-Komplexe**
  - Rechenzentren
  - Rechnernetze
  - Kommunikationsnetze
  - **…**
- **Teile der Gesellschaft**
  als informationsverarbeitende Subsysteme aus Menschen **und** Maschinen

*) Vergleiche hierzu auch den englischen Begriff ***Target of Evaluation (TOE)*** bei der Bewertung der IT-Sicherheit

System der Informationstechnik
IT-System (Fts.)

Vorbemerkungen

Definitionen und Erläuterungen zur Sicherheit hier vor allem bezogen auf

IT-Systeme (engl. ***it-systems***)

und deren Komponenten. Vorrangig abgeleitet aus **ISO/IEC 22382–8** und **DIN 44 300** *(*Ausgabe November 1988)

Beachte:
Die Systeme der Kommunikationstechnik sind in dieser Definition ***IT-System*** enthalten.

Synonym gebrauchte Begriffe
- Systeme der Informationstechnik
- informationstechnische Systeme
- Datenverarbeitungssysteme

weniger empfehlenswert
- informationsverarbeitende Systeme
- Informationsverarbeitungssysteme

schlecht
- Informationssysteme

Definition

Ein IT-System ist eine **Menge von Elementen**, d.h. von

Gegenständen	(Subjekten und Objekten),
Relationen	zwischen Gegenständen,
Aktionen	{ ausgelöst von Gegenständen ausgeübt auf Gegenstände

die in einer

bestimmten Umgebung (Kontext) als Gesamtheit (Funktionseinheit)

betrachtet werden.

Elemente

Gegenstände (engl.: *items*)

- sind entweder an einer **Aktion beteiligt** oder sind
- **Elemente einer Relation.**

Relationen

Relationen sind **Beziehungen zwischen Gegenständen**. Sie erzeugen

Untermengen oder **Unterstrukturen** in einem IT-System.

Aktionen

Aktionen sind **Funktionen** oder **Prozesse**, die ein System ausführen kann (= die in einem System ablaufen können).

Gegenstände in Aktionen

An Aktionen sind Gegenstände beteiligt als

Subjekte	**aktive Gegenstände**, Akteure oder die Auslöser von Aktionen
Objekte	**passive Gegenstände**, auf die Aktionen ausgeübt werden

Die Eigenschaft eines Gegenstandes, **Subjekt** oder **Objekt** zu sein, kann sich in der Zeit

dynamisch ändern.

Beispiele:

① Programm → Unterprogramm 1
↓
Unterprogramm 1 → Unterprogramm 2

② Benutzer → Login-Prozedur → Benutzer

gleichbedeutend mit

Benutzer ↔ Login-Prozedur

Aktionen

Aktionen sind Funktionen oder Prozesse, die ein System ausführen kann (= die in einem System ablaufen können).

Interne Aktionen

an denen nur Gegenstände des Systems selbst beteiligt sind

Externe Aktionen

ausgelöst von einem Subjekt außerhalb des Systems (Umgebung) auf einen Gegenstand im System
➡ **Eingabeaktion**

oder von einem Subjekt im System auf einen Gegenstand außerhalb
➡ **Ausgabeaktion**

Anmerkung

Externe Aktionen arbeiten stets über
Schnittstellen
des Systems.

Funktionseinheit – Betrachtungseinheit

Ein IT-System muss immer im **Zusammenwirken mit seiner Umgebung** gesehen werden.

Folgerung

Definiere genau, welche Elemente zu einem gegebenen Zeitpunkt als zu **einer Funktionseinheit, also zum IT-System,** gehörig **betrachtet** werden und welche nicht!

Geschlossenes System

Idealisierende Annahme: System *ohne Zusammenhang* mit der Umgebung

Schnittstellen und Zusammenhang

Schnittstelle *(interface)*

Gedachter oder tatsächlicher Übergang an der Grenze zwischen zwei gleichartigen Einheiten wie Funktionseinheiten*, Baueinheiten* oder Programmbausteinen*, mit den vereinbarten Regeln für die Übergabe von Daten oder Signalen *(DIN 44300)*.

Externe Schnittstelle

Schnittstelle zwischen dem System und seiner Umgebung

Zusammenhang

die **Menge der externen Schnittstellen** eines Systems

Fortsetzung ↳

Systemsicherheit und Umgebung

Änderung des Zusammenhangs

Änderung der Anzahl oder der Eigenschaften der Schnittstellen (Kanäle)

⬇

Änderung der Möglichkeiten für die Nutzung des Systems

⬇

Änderung des Systemverhaltens

Fortsetzung ↳

Systemsicherheit und Umgebung

(Fts.)

Zwei Möglichkeiten für verbesserte Systemsicherheit

1. *Änderung des* **Systemverhaltens** *oder*
2. *Änderung der* **Schnittstellen**

① Änderung des Systemverhaltens

Ändere die Funktionsweise (Funktionalität) des Systems so, dass nicht-ordnungsmäßige Anforderungen als solche erkannt und entweder nicht ausgeführt oder korrigiert werden.

➧ **wünschenswert**

② Änderung des Zusammenhangs

Ändere den Zusammenhang des Systems mit seiner Umgebung – also Art oder Menge der externen Schnittstellen – so, dass nicht-ordnungsmäßige Anforderungen nicht mehr gestellt oder ins System gelangen können.

➧ **Praxis der „Käseglocke"**

Systemsicherheit und Umgebung

(Fts.)

Anmerkung zu ①

In der Praxis überall dort nicht oder nur bedingt möglich, wo Systeme ***„unzugänglich"*** sind

- fehlende Dokumentation
- Patente oder Urheberrechte
- Firmenpolitik
- Vertraulichkeit, Geheimhaltung
- Problematik der „Nicht-Open Source"
- Komplexität der Systeme ...

Anmerkung zu ②

➔Meistgebrauchte Form der Fehlerbehandlung➔

- Problematik des Unterlaufens oder Umgehens der Schnittstelle zwischen Käseglocke und System
- Verletzlichkeit der Nahtstellen Schutzschild ↔ System
- *Sonderform*: „Anpassung der Anforderungen"

Das Problem der Vorbesetzung

Sicherheit ***(Safety, Security)***

ist als Begriff längst weit verbreitet und vorbesetzt.

Folgen

verschiedene Bedeutungen
in verschiedenen Anwendungsgebieten

Missverständnisse
in fachübergreifenden Diskussionen

⬇

Notwendige Voraussetzung

Vereinbare eindeutig
Bedeutungsumfang und **Bedeutungsinhalt**
des Begriffs Sicherheit als
Grundlage jedes Verständnisses.

Fortsetzung ↳

OECD / Document GD(92)190*)

IT Security

The objective of security in information systems is the protection of the interests of those relying on information systems from harm resulting from failures of availability, confidentiality, and integrity.

Anmerkung

- ***Protection of the interests*** kann sowohl als Beherrschbarkeit als auch als Verlässlichkeit verstanden werden.
- ***Failures of availability, confidentiality, and integrity*** ist dann aber eine zu enge Auslegung von Sicherheit.

*) **OECD** Organization for Economic Cooperation and Development, Paris

Begriffe zu IT-Sicherheit (aus VDE)

2.1 Schaden

Schaden ist ein Nachteil durch Verletzung von Rechtsgütern auf Grund eines bestimmten technischen Vorganges oder Zustandes.

2.2 Risiko

Das Risiko, das mit einem bestimmten technischen Vorgang oder Zustand verbunden ist, wird zusammenfassend durch eine Wahrscheinlichkeitsaussage beschrieben, die die zu erwartende Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und das beim Ereigniseintritt zu erwartende Schadensausmaß berücksichtigt.

2.3 Grenzrisiko

Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes. Im allgemeinen lässt sich das Grenzrisiko nicht quantitativ erfassen.

2.4 Gefahr

Gefahr ist eine Sachlage, bei der das Risiko größer als das Grenzrisiko ist.

IT-Sicherheit (VDE 31000 (1987))

2.5 Sicherheit

Sicherheit ist eine Sachlage, bei der das Risiko nicht größer als das Grenzrisiko ist.

IT-Sicherheit (nach ???)

IT-Sicherheit *(it-security)*

ist eine dem Individuum und der Gesellschaft bekannte und verständliche Sachlage, bei der das ***Risiko***, das mit einem informationstechnischen Vorgang oder Zustand verbunden ist, das ***Grenzrisiko nicht überschreitet***, das jedes Individuum für sich hieraus, früher oder später, erfahren könnte: eine Beeinträchtigung oder Verlust von Geist, Körper, Seele, Freiheit, Lebensraum, Hab und Gut.

Anmerkungen

Die in der IT auftretenden Risiken sind sowohl

- Folgeschäden der **unbefugten Nutzung** von Daten und Funktionen, verursacht durch (menschliche) Fahrlässigkeit oder Absicht, oder
- Schäden, die aus **konstruktiven oder materiellen Fehlern** erwachsen.

Datensicherheit
(data security)

DIN 44300 (Fassung 11/1988)

Sachlage, bei der **Daten*** unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung oder Missbrauch bewahrt sind,

und zwar unter Berücksichtigung verarbeitungsfremder Risiken wie auch im Verlauf auftrags- und ordnungsgemäßer Erbringung einer Datenverarbeitungsleistung*. Daten dürfen also

- weder bei datenverarbeitenden Prozessen* oder auftragsbedingten Vor- und Nacharbeiten
- noch in Funktionseinheiten* zur Abwicklung auftragsbedingter Arbeiten
- noch durch das Handeln von an auftragsbedingten Arbeiten beteiligten Personen

beeinträchtigt werden.

Anmerkung:
Beeinträchtigung von Daten umfasst u.a. Verlust, Zerstörung, Verfälschung. Zum Begriff Sicherheit siehe DIN VDE 31 000 Teil 2.

Fortsetzung ↯

IT-Sicherheit
(it-security)

Nach **DIN 44300**

Sachlage, bei der ***IT-Systeme oder deren Komponenten*** unmittelbar oder mittelbar so weit wie möglich vor Beeinträchtigung oder Missbrauch bewahrt sind.

Sicherheit ISO/IEC 2382–8

08.01.01 – Computersicherheit, IT-Sicherheit (*computer security), COMPUSEC*

Schutz von Daten und ***Betriebsmitteln*** vor **versehentlichen** oder **arglistigen** Handlungen, **gewöhnlich** durch das Ergreifen geeigneter **Maßnahmen**.

Anmerkung:
Handlungen dieser Art können sein: nicht autorisierte Änderung und Zerstörung, unberechtigter Zugriff, unberechtigte Offenlegung oder Aneignung.

Nationale Anmerkung
Der Begriff „Sicherheit" ist im Deutschen abweichend definiert, siehe z. B. DIN VDE 31000-2.

Fortsetzung ↳

Sicherheit ISO/IEC 2382–8 (Fts.)

08.01.02 – administrative oder **prozedurale Sicherheit** (administrative *security, procedural security)*

Administrative ***Maßnahmen,*** die der Computersicherheit dienen,

Anmerkung:
Maßnahmen dieser Art können sein: Vorkehrungen für den Normalbetrieb und für die Zurechenbarkeit, für die Ermittlung eines Bruchs der Sicherheit und für die Ausweitung von Mitschnitten.

08.01.03 – Kommunikationssicherheit (*communications security, (COMSEC)*

Auf die Datenübermittlung angewandte Computersicherheit.

08.01.04 – Datensicherheit *(data security)*

Auf Daten angewandte Computersicherheit

Datensicherung
(data security measures)

DIN 44300

Maßnahmen und Einrichtungen, die Datensicherheit* herbeiführen oder aufrechterhalten.

Anmerkung: Beeinträchtigung von Daten umfasst u.a. Verlust, Zerstörung, Verfälschung.
Zum Begriff Sicherheit siehe DIN VDE 31 000 Teil 2.

➔ Wird in **ISO/IEC 2382–8** nicht aufgeführt

Datenschutz
(*privacy protection*)

DIN 44300 (1988)

Sachlage, bei der die **schutzwürdigen Belange Betroffener** vor Beeinträchtigung, die von der Verarbeitung der Daten* ausgeht, bewahrt sind.

Betroffene können natürliche oder juristische Personen oder Personenvereinigungen sein, aber nur insoweit, als Daten über sie verarbeitet werden oder durch Verarbeitung von Daten auf ihre Identität geschlossen werden kann.

Anmerkung: Die rechtliche Seite des Datenschutzes wird durch Gesetz, Rechtsverordnung oder Rechtsprechung geregelt. Es ist zu unterscheiden zwischen Datenschutz und Maßnahmen, die ihn herbeiführen.

Zum Begriff Schutz siehe DIN VDE 31 000 Teil 2.

Fortsetzung

Schutz
(*privacy protection*)

DIN VDE 31000 (1987)

2.7 Schutz

Schutz ist die Verringerung des Risikos durch Maßnahmen, die entweder die Eintrittshäufigkeit oder das Ausmaß des Schadens oder beide einschränken.

Datenschutz
(*data protection*)

08.06.02 – Datenschutz
(data protection)

Durchführung administrativer, technischer oder organisatorischer Maßnahmen, um Daten vor unberechtigtem Zugriff zu schützen.

Anmerkung: Überarbeitet übernommen aus ISO/IEC 2382–01.07.01 – 1993.

Nationale Anmerkung:
Benennung in 1.2.12 von E DIN 44300-I: 1995-03: *Datenschutz* nicht konzeptgleich

Datenschutz
(*privacy protection*)

08.06.08 – Schutz der Privatsphäre (privacy protection)

Maßnahmen zum Schutz der Privatsphäre.

Anmerkung: Diese Maßnahmen schlie8en Datenschutz und Einschränkungen bezüglich Sammeln, Kombinieren und Verarbeiten von personenbezogenen Daten ein.

Nationale Anmerkung:
Benennung in 1.2.12 von E DIN 44300-I : 1995-03: Datenschutz nicht konzeptgleich

Die deutsche Definition von **Datenschutz** nach BDSG §1 entspricht weitestgehend dem englischen Begriff **privacy** (**ohne** Zusatz)!

Datenschutz

Novellierung des BDSG (Arbeitsfassung zum Änderungsgesetz vom 23. Mai 2001)*)

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) … … … (5)

*) Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes, Artikel 1 (Neufassung des Bundesdatenschutzgesetzes – BDSG) vom Dezember 1990

Datenschutz

GDD 1983*)

eine **Menge von Anforderungen**, die die Zulässigkeit der Zugriffe auf Daten und die Ausführbarkeit der Informationsgewinnung aus Daten festlegen

***Anmerkung*:**

Diese Definition geht auf Diskussionen des Arbeitskreises „Datensicherheit" der GDD zurück (vor 1983).

Sie stellt einen Bezug her zwischen **Schutz/-Sicherheit** und **Ordnungsmäßigkeit.**

Fortsetzung ↳

*) GDD ***G****esellschaft für* ***D****atenschutz und* ***D****atensicherung,*
Bonn

1/95

Bezug zur Ordnungsmäßigkeit (Fts.)

Menge von Anforderungen aus

- Gesetzen
- Verordnungen
- organisatorischen Regelungen
- technischen Vorschriften
- Funktionsbeschreibungen
- Entwurfsspezifikationen
- technischen Anleitungen
- Unternehmensinteressen
- Konventionen und Traditionen
- Standesregeln, Ehrenkodizes
- Bräuchen, Gewohnheiten, Vereinbarungen
- … …

Hinweis

Datenschutzgesetze
(Europa ➔ Bund ➔ Länder)
sind nur eine
Untermenge der Anforderungen.

Leistungssteigerung – Preisverfall ca. 1960 – 2000

Der Faktor 10^6–10^{10}

Rechengeschwindigkeit

1965 ≈ 1000 FLOPS (Gleitkommaoperationen/s)

2000 ≈ 1000×10^9 FLOPS = 1 TFLOPS

Speicherkapazität

1960 einige 10^3 Byte (KByte)

2000 10^9–10^{12} Byte (GByte – Tbyte)

Raumbedarf (Miniaturisierung)

1960 1 Schaltfunktion ≈ 250 cm^3 = ¼ Liter (Röhrenbaustein der Zuse Z22R)

2000 ≥10^8 Schaltfunktionen (ein Chip) ≈ 250 mm^3

Preisverfall

1963 300.000,-- DM je 1 Mbyte

2000 0,02 DM • •

Fortsetzung

Leistungssteigerung – Preisverfall (Fts.) Beispiel für den Faktor 10^6

- **2 KByte** (2×10^3 Byte)
  - 1 Schreibmaschinen***seite***
- **1 MByte** (1×10^6 Byte)
  - 1 Ordner à 500 Seiten
  - 1 Buch à 200–300 Seiten
- **1 GByte** (1×10^9 Byte)
  - 1.000 Ordner
  - 500 Bücher
  - ½ – 1 Mio Schreibmaschinenseiten
  - 500–1.000 Disketten
  - 1–2 t Papier

Sicherheit bei individueller Datenverarbeitung

- Individualisierte Informationstechnik, d.h. Datenverarbeitung und Kommunikation mit dezentralen und vernetzten Systemen, bringt eine Vielzahl
  - **neuer Möglichkeiten**, aber auch
  - **neuer Bedrohungen** mit sich.
- Sie sind auch Fachleuten, Informatikern wie Juristen, **erst in Ansätzen bekannt.**
- Sicherheit ist nur erreichbar, wenn Maßnahmen, Regeln und Verhaltensweisen auf **allen** Ebenen, d.h.
  - personell,
  - technisch,
  - organisatorisch

  und nicht zuletzt
  - juristisch

  den **neuen Gegebenheiten angepaßt** werden.

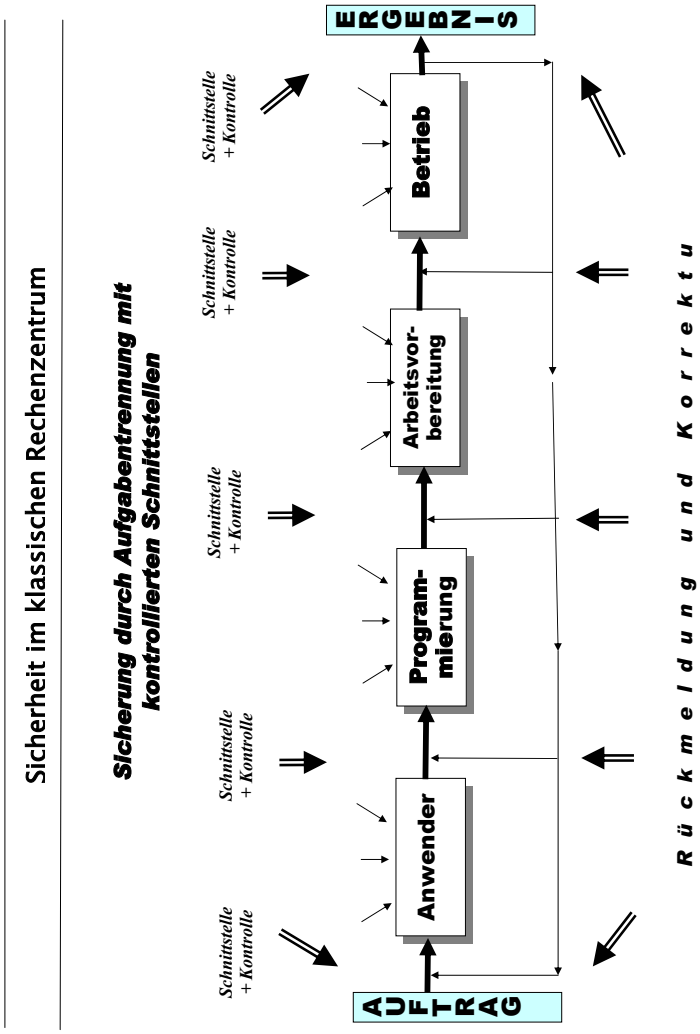
Sicherheitslücken der IDV

- **physische Gefährdung**
  - Entfernung (Diebstahl) des Gesamtsystems
  - mechanische Beeinträchtigung
  - keine zusätzliche „klassische“ Sicherung (gegen Feuer, Wasser, Einbruch, Sabotage, …)
- **unzulängliche (keine) Zugriffskontrolle**
  - (Zutritt, Zugang, Zugriff)
- **unzulängliche Benutzerverwaltung**
  - Identifizierung und Authentisierung
  - Rechtevergabe
  - Rechteverwaltung
  - Rechtekontrolle
- **unzulängliche Funktionstrennung**
  (Anwender = Programmierer = Systemverwalter = Arbeitsvorbereiter =Operateur = Revisor = RZ-Leiter = Datenschutzbeauftragter = **…**)
- **keine Kontrolle der Abläufe**
  keine Kontrolle (oder Automatisierung) der Datensicherung (→ Backup → Protokollierung → Wiederanlauf)

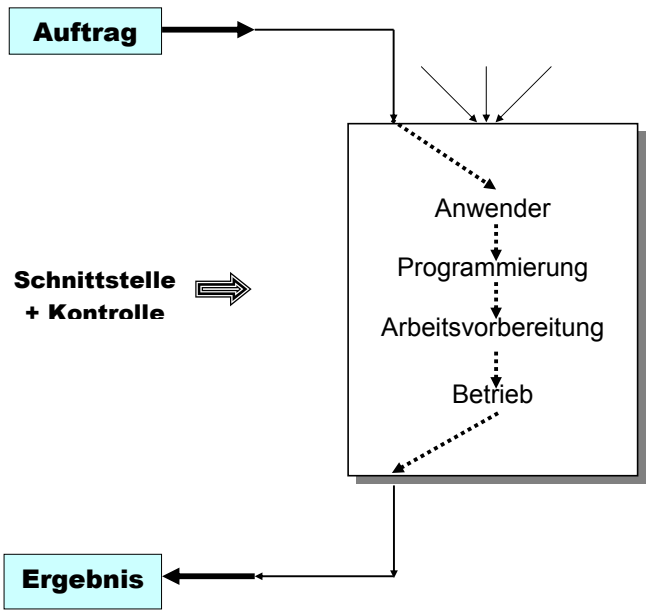
Fortsetzung

Sicherheitslücken der IDV – (Fts.)

- **keine Trennung**
  Anwendungen ⇔ System
- **keine Datenträgerkontrolle**
- **unzulängliche Dateiverwaltung**
  - (Änderungsprotokoll, Zugriffe, Historie)
- **(fast) keine Protokollierung**
- **(fast) keine Fehlerbehandlung**
  - (Fehlerkorrektur und -kompensation)



Mangelnde Aufgabentrennung



Motive wachsenden Interesses

- **Zunehmende Durchdringung** *(Ubiquität)*
  kein (technischer) Bereich ohne „Computer“
  - in allen Wissenschaften
  - in der gesamten Verwaltung
  - im Beruf
  - im Privatleben
- **Wachsende Komplexität**
  - komplexere Geräte und Programme
  - Netze (Hard- und Software), Internet
  - neuartige Verfahren und Systeme (künstliche Intelligenz, lernende Systeme, neuronale Netze)
- **Abhängigkeit und Bedrohung**
  Zusammenhänge und Schwachstellen auch für Spezialisten kaum noch durchschaubar
  - Verhalten der Systeme undurchschaubar
  -
  - neue Bedrohungen (Viren, …)
  - undurchschaubare Entscheidungen
- **neues Bewusstsein**
  - Verbreitung persönlicher Systeme (PC)
  - dezentrale und vernetzte DV
  - öffentliche Diskussion (oft emotional!)
  - staatliche Maßnahmen (Gesetzgebung), staatliche Institutionen national (BSI, DSB) und international (EU, NIST, NSA)

Fortsetzung

Motive wachsenden Interesses (Fts.)

- **Offene Rechtslage**
  - eigenes Informationsrecht oder nicht?
  - informationelle Selbstbestimmung vs. Sicherheit (vgl. GG Art.10 Abs.1 vs. Abs.2, Volkszählungsurteil (BVerfG 1983),
  - Kryptokontroverse)
  - unzureichendes BDSG 1991 und 2000
  - Ansätze im 2. WiKG (Änderung StGB)
  - Urheberrecht in der EU
  - Produkthaftung
  - CyberCrime Problematik
- **Keine allgemeingültigen Konzepte**
  - Entwicklung der Evaluationskriterien
  - Probleme des praktischen Nutzens der Common Criteria (CC)
- **Unsichere Systeme**
  - UNIX, MS-DOS, Windows, Linux(?) ...
- **Zu wenig Forschung**
- **Sprach- und Verständnisprobleme**
  - zwischen Juristen, Informatikern, Politikern
  - formale Beschreibung vs. Formulierung in natürlicher Sprache
  - formale Definition vs. Legaldefinition

Grundsatz

IT-Systeme müssen **verlässlich** sein.

IT-Systeme müssen **beherschbar** sein.

Zwei komplementäre Sichten

Verlässlichkeit

Sicherheit ***der*** Systeme – die technische Sicht

Sachlage, bei der weder die **Systeme** noch die mit ihnen verarbeiteten Daten (Informationen) noch die Datenverarbeitung (Funktionen und Prozesse) in ihrem Bestand, ihrer Nutzung oder ihrer Verfügbarkeit unzulässig beeinträchtigt werden.

Beherrschbarkeit

Sicherheit ***vor dem*** System **–** die Sicht der Betroffenen

Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden.

Duale Sicherheit in Netzen

Datenverarbeitung und Kommunikation in Netzen müssen (mindestens) genau so **verlässlich und beherrschbar** sein, als wenn sie ohne Hilfe eines Netzes abliefen.

Zusatzforderung

Vorgänge, die in Netzen oder über Netze initiiert ablaufen, dürfen die an den Netzen angeschlossenen **IT-Systeme nicht** (unzulässig) **beeinträchtigen,**

- weder deren Funktion
- noch die in ihnen vorhandenen Daten.

Sicheres IT-System (im Sinne dualer Sicherheit)

- System der Informationstechnik, das den drei Grundbedrohungen der **Verlässlichkeit**, denen ein IT-System ausgesetzt sein kann,
  - unbefugter Informationsgewinn
  - unbefugte Modifikation von Daten.
  - unbefugte Beeinträchtigung der Verfügbarkeit

  in ausreichender Weise widersteht und
- **beherrschbar** ist in dem Sinne, dass es die von seiner ordnungsgemäßen Funktion Betroffenen nicht mehr als zulässig in ihren Rechten und Handlungsmöglichkeiten beeinträchtigt.

Beachte:

Unbefugte Modifikation ist generell eine Grundbedrohung. In den Anforderungen kann aber sinnvoll nur die Sicherung gegen ***unbemerkte, unbefugte Modifikation*** verlangt werden.

Forderung

Duale Sicherheit, d.h.

Sicherheit des Systems
+
Sicherheit der Betroffenen

insbesondere dort, wo maschinelle Systeme schon vorhandene menschliche Tätigkeiten übernehmen oder ersetzen.

Das gilt insbesondere für die **Informationsverarbeitung**.

⬇

Problem

Sicherheit wird in der Informationstechnik weniger als anderswo beachtet!

Rolle des Menschen

Beachte:

Menschen können
IT-Systeme[*)] oder **Betroffene**
sein.

Diese Aussage ist **reflexiv**, das heißt

⬇

Ein und derselbe Mensch kann in ein und dem selben Vorgang, sowohl **System(teil)** als auch **Betroffener** sein.

[*)] Genauer: IT-Systeme oder Teil von IT-Systemen oder Komponenten solcher Systeme

Sicherheit der Systeme – Verlässlichkeit –

Ein IT-System ist sicher in technischer Sicht,

➡ wenn seine Funktionsweise den **vorgegebenen Anforderungen genügt.**

Das heißt in anderen Worten:

Ein IT-System ist technisch sicher, wenn der Benutzer sich auf die

Ordnungsmäßigkeit und Verfügbarkeit der Funktionen des Systems und der

verlassen kann, die mit Hilfe dieser Funktionen gewonnen wurden.

➡ **Verlässlichkeit von IT-Systemen**

Fortsetzung ↳

Sicherheit realer Systeme – Verlässlichkeit –

Sicherheit für reale Systeme impliziert, dass der Benutzer sich auf die

> Korrektheit und Verfügbarkeit der Funktionen des Systems und der Ergebnisse
>
> **hinreichend verlassen kann,**
>
> auch wenn Teile des Systems nicht oder **nicht immer ordnungsmäßig arbeiten.**

➡ **Verlässlichkeit *realer* IT-Systeme**

Fortsetzung ↳

Anforderungen an die Verlässlichkeit

Vertraulichkeit *(confidentiality)*

- keine unbefugte **Einsichtnahme** von Daten
- kein unbefugtes Erschließen von Informationen oder Interpretieren von Daten

Integrität*) (*integrity*)

- keine unbefugte, **unbemerkte Veränderung** oder Beeinträchtigung
  - der Daten
  - der Funktionen
- **Konsistenz** der Daten und Funktionen

Verfügbarkeit (*availability*)

- Prozesse (Aktionen) im IT-System müssen zum vorgegebenen **Zeitpunkt** ausführbar sein.
- Prozesse (Aktionen) im IT-System müssen im vorgegebenen **Zeitrahmen** ablaufen.

*) auch Unversehrtheit

Die Grundbedrohungen der Verlässlichkeit

- **unbefugte Kenntnisnahme**
- **unbefugte Änderung**
- **unbefugte Beeinträchtigung der Verfügbarkeit**

Voraussetzung

Befugte Nutzung

Es ist **definiert und bekannt**, was das IT-System tun soll und was nicht (► Vollständigkeit des Anforderungskatalogs)

Beachte:

Grundbedrohung ist *jede* unbefugte Änderung, die bemerkte ebenso wie die unbemerkte.

Verfügbarkeit vs. Zuverlässigkeit

In der Zuverlässigkeitstheorie wird zwischen beide Begriffen unterschieden.

Verfügbarkeit *(availability)*

- ist die Wahrscheinlichkeit, ein System (genauer: eine Funktionseinheit oder Betrachtungseinheit), zu einem bestimmten Zeitpunkt in einem funktionsfähigen Zustand vorzufinden.

Zuverlässigkeit *(reliability)*[*)]

- ist die Fähigkeit einer Funktionseinheit (Betrachtungseinheit), den vereinbarten Anforderungen während einer bestimmten Zeitdauer zu genügen.

*) **Unterscheide** stets zwischen:
Verlässlichkeit *(trustworthyness)* als übergreifendem Begriff in der dualen Sicherhit und
Zuverlässigkeit *(reliability)* technischen Teilaspekt sicherer Systeme

Sicherheit *vor dem* System Beherrschbarkeit – die Sicht der Betroffenen –

Ein IT-System ist sicher aus der Sicht der Betroffenen,wenn seine Funktionsweise nicht nur **verlässlich** ist, sondern darüber hinaus zwei weitere Anforderungen erfüllt:

Zurechenbarkeit *(accountability)*

- ► wenn von jeder Aktion (Vorgang, Prozeß) während ihres Ablaufs oder danach feststellbar ist, welcher Instanz sie zuzuordnen ist;

Revisionsfähigkeit oder **Rechtsverbindlichkeit** *(legal liability)*

- ► wenn Aktionen, die mit ihnen erzeugten Daten und die Zuordnung zwischen beiden Dritten gegenüber beweiskräftig nachgewiesen werden können.

Das gleiche gilt nicht nur für die Aktionen selbst, sondern auch für deren Ergebnisse oder Auswirkungen.

➡ **Beherrschbarkeit von IT-Systemen**

Anforderungen an die Beherrschbarkeit

Zurechenbarkeit *(accountability)*

- ► aller Aktionen (Vorgänge) und Daten (Ergebnisse) zu bestimmten Subjekten (Instanzen, insbesondere Personen), die sie ausgelöst (verursacht) und damit letztlich **zu verantworten** haben

Revisionsfähigkeit oder Rechtsverbindlichkeit *(legal liability)*

- ► aller Vorgänge und Veranlassungen – und der mit ihnen gewonnenen Ergebnisse,– insbesondere im Sinne der **Beweisbarkeit** (Nachweisbarkeit) gegenüber Dritten*)

In Netzen heißt dies insbesondere

- ► Sender/Empfänger sind **authentisch** und
- ► können **nachweisbar** bestimmten, ebenfalls authentischen Nachrichten **zugeordnet** werden (→ *Datenschutzproblem der Anonymität*).
- ► Vorgänge im Netz sind **unbestreitbar** *(→ **non-repudiation).***

*) Einige Autoren verwenden die kürzere Bezeichnung **Verbindlichkeit** (engl. ***(liability)***, geben aber damit dem Nachweis gegenüber Dritten zu geringes Gewicht.

Semantische Dimensionen

Vertraulichkeit
Integrität
Verfügbarkeit
Zurechenbarkeit
Revisionsfähigkeit*)

sind fünf **Fundamentalkomponenten der Sicherheit**, die den Grundbedrohungen gegenüberstehen In diesem Sinne sind sie im Hinblick auf Verlässlichkeit und Beherrschbarkeit von IT-Systemen als

semantische Dimensionen

für die Bedeutung des Begriffs Sicherheit

konstitutiv.

Hinweis: In der Literatur werden die Bezeichnungen

- ► **Semantische Dimensionen** (engl. ***dimensions***)
- ► **Fundamentalkomponenten**
- ► **Ziele** (engl. ***objektives***)
- ► **Facetten** (engl. ***facets***)

oft ***synonym*** gebraucht.

*) (oder **Rechtsverbindlichkeit**)

Der semantische Raum

Die Bedeutung des Begriffs Sicherheit

Vertraulichkeit, Integrität und Verfügbarkeit Zurechenbarkeit und Revisionsfähigkeit spannen als Fundamentalkomponenten (oder semantische Dimensionen) den semantischen Raum des Begriffs auf, sind aber voneinander nicht unabhängig.

Sie können als Komponenten der Sicherheit

verschieden gewichtet

werden:

- ► von System zu System,
- ► von Anwendung zu Anwendung,

abhängig von den (aktuellen) Anforderungen an die Systemsicherheit.

Grundsatz

In jedes **Sicherheitskonzept** und jede **Evaluation** (Audit) sind **alle** semantischen Dimensionen einzubeziehen. Wird eine vernachlässigt, muss dies explizit begründet werden.

Semantische Dimensionen dualer Sicherheit (Fts.)

Das bedeutet

- **Vertraulichkeit, Integrität und Verfügbarkeit**
  von Geräten, Daten, Programmen und Personen schaffen und erhalten;
- **Zurechenbarkeit**
  aller Vorgänge und Ergebnisse zu definierten Veranlassern gewährleisten und deren
- **Revisionsfähigkeit (Rechtsverbindlichkeit)**, d.h. Nachvollziehbarkeit und Beweisbarkeit gegen über Dritten, sicherstellen

trotz

- Dezentralisierung
- Individualisierung
- Vernetzung
- Intensivierung
- Komplexität
- technischer Weiterentwicklung
- ...

Sicherheit der Gesellschaft

IT-Systeme und Informationstechnik müssen **verlässlich, gesellschaftlich verträglich** und **verfassungskonform** sein.

Ziele

① **Informationelle Selbstbestimmung** BVerfG1983)

② **Gewährleistung des Rollenspiels**

③ **Erhalt der verfassungsgemäßen Struktur der Gesellschaft**

IT-Sicherheit im Unternehmen

Ansatz ①

Jedes Wirtschaftsunternehmen, jede Behörde, jede Verwaltung oder irgendeine andere Gruppierung ist **Teil der Gesellschaft** und damit auch

ein IT-System

Ansatz ②

Jedes Wirtschaftsunternehmen, jede Behörde, jede Verwaltung oder irgendeine andere Gruppierung **enthält informationsverarbeitende Subsysteme aus Menschen und Maschinen** und ist damit selbst – in dieser Hinsicht –

ein IT-System.

IT-Sicherheit im Unternehmen

Grundlage

- **Information**

ist heute die vierte, **mindestens gleichgewichtige Grundvoraussetzung** neben den drei klassischen Komponenten

- **Kapital**
- **Arbeitskraft**
- **Boden (Rohstoffe).**

für eine leistungsfähige Wirtschaft.

Folgerung:

Bereitstellung und Nutzung von Information muss im Unternehmen mit (mindestens) der gleichen Umsicht geplant und betrieben werden wie die der klassischen Komponenten.

IT-Sicherheit im Unternehmen (Fts.)

Das bedeutet für die Informationsverarbeitung:

- **Verträglichkeit mit den Unternehmenszielen**
- **Konsistenz der Organisation**
- **Primat der Unternehmensführung**

Informationstechnik
(IT-Systeme und **IT-Verfahren)**
darf im Unternehmen
keine Eigendynamik
entwickeln (→ *Beherrschbarkeit*).

Duale Sicherheit als Unternehmensstrategie

Grundsatz

Leistungsfähigkeit und Sicherheit
der Informationstechnik*) sind
gleichrangige Forderungen.

Ziel

Primat der Unternehmensziele

Verlässlichkeit + Beherrschbarkeit
der **Informationstechnik** und der **Informationen** (→ Daten) nach Maßgabe der Anforderungen des Unternehmens

*) Genauer: aller Einrichtungen und aller Vorgänge im Zusammenhang mit Informationsverarbeitung (Datenverarbeitung) und Kommunikation – Personen und deren Handlungen eingeschlossen

Duale Sicherheit als Unternehmensstrategie (Fts.)

Forderung

Ordnungsgemäßer Umgang mit **Information*) und Informationstechnik in allen Teilen des Unternehmens**

Folgerung

Gewährleiste sichere, d.h. verlässliche und beherrschbare Informationsverarbeitung durch planvolles Vorgehen im Sinne der vorgegebenen Anforderungen (insb. der Unternehmensziele) auf allen Ebenen:

- physisch
- personell
- organisatorisch
- informationstechnisch.

*) D.h. nicht nur mit den **Zeichen** gemäß DIN 44300, sondern insbesondere auch mit deren ***Interpretation***, d.h. mit den **Daten**

Duale Sicherheit als Unternehmensstrategie (Fts.)

– Schlusskette –

Informationsverarbeitung
lebensnotwendig
für das Unternehmen.

↓

Informationsverarbeitung
so leistungsfähig wie möglich.

↓

Informationsverarbeitung
so sicher wie nötig.

↓

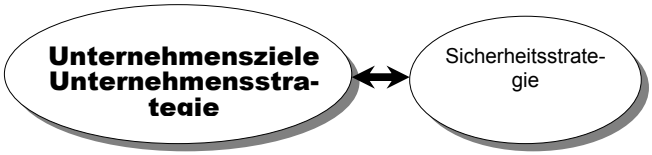
Sicherheit ist
zuerst Vorstandssache,
dann Aufgabe der Linie!

Duale Sicherheit als Unternehmensstrategie (Fts.)

– Unternehmensgrundsatz –

Sicherheit der Informationsverarbeitung
muss integriert werden,
nicht aufgezwungen **(→ Akzeptanz)!**

Wechselwirkung



Falsche Behauptung

„Sicherheit beeinträchtigt Leistungsfähigkeit“

Duale Sicherheit als Unternehmensstrategie (Fts.)

Aufgabe der IT im Unternehmen

Vertraulichkeit, Integrität und Verfügbarkeit
von Geräten, Daten, Programmen und Personen als wesentlichen Bestandteil des Unternehmens aufbauen und erhalten.

Zurechenbarkeit und Rechtsverbindlichkeit
der Vorgänge, Veranlassungen und Ergebnisse – wo immer gefordert – sicherstellen.

Aufgabe der Führung

Planen und Durchsetzen
einer sicheren Informationsverarbeitung
im gesamten Unternehmen

Folgerungen

- Einführen und Durchsetzen dieses Leitsatzes als **Prinzip für das ganze Unternehmen …**
- **…** und eines darauf aufbauenden **unternehmensweiten Sicherheitskonzepts**
- Schaffen der materiellen und immateriellen Voraussetzungen
- Überzeugen der Mitarbeiter in Führung und Linie → **Akzeptanz**
- Einleiten und Durchsetzen aller Planungen, Änderungen, Beschaffungen und Kontrollen
  - personell
  - technisch
  - organisatorisch

Aufgabe der Linie

Gewährleisten
einer sicheren Informationsverarbeitung
im gesamten Unternehmen

Folgerungen

- bestmögliche Annäherung an die Anforderungen, insbesondere des Sicherheitskonzepts
- Kompensation der Auswirkungen nicht-ordnungsmäßiger Komponenten

Analyse

Untersuchung und Bewertung von Bedrohungen und Schwachstellen

Konzeption

Erarbeitung der Komponenten eines Sicherheitskonzepts

Installation

Einführung der Maßnahmen und Verfahren

Betrieb

Durchführung der Maßnahmen und Verfahren

ergänzt durch

Kontrolle und Revision

Überwachung und Nachprüfung aller Vorgänge und Objekte

Bedrohungen

- **Fehler**
  in Systemen und Komponenten (Hardware, Software, Organisation)
- **Infrastruktur**
- **menschliche Unzulänglichkeit**
- **Manipulation**
  vorsätzliche Änderung (→ Missbrauch, Sabotage, **…**)

dazu, vor allem bei **„*interessierten*“ *Benutzern***

Spieltrieb
Neugier

und zunehmend bei ***Insidern***

Frust
Rache

Ziele der Bedrohungen

- **Rechnerhardware jeder Art**
  - vor allem Personal Computer, Arbeitsplatzsysteme, **…**
- **Kommunikationssysteme**
  - Netze, Übertragungsstrecken
  - Knoten- und Vermittlungssysteme,
  - Server und zentrale Systeme
  - Verteiler, …
- **Software aller Art**
  - Systemprogramme,
  - Anwendungssysteme,
  - Fremdsoftware, …
- **Datenbestände**
  - Stamm- und Bewegungsdaten,
  - Bibliotheken,
  - Archive und Sicherungskopien, …
- **Infrastruktur**
  - Gebäude und Räume
  - Ver- und Entsorgungseinrichtungen, …
  - Verkehrsflächen
- **Personen**
  - eigenes **und** fremdes Personal
  - Hilfs- und Katastrophendienste
  - Besucher, …

Motive aktiver Bedrohungen (Manipulationen)

- Wirtschaftsspionage allgemein
- Konkurrenzspionage
- Sabotage

Gegenstände von Manipulationen

- **Entwicklung**
  - Dokumentationen (Chemie, Pharmazie, …)
  - Designunterlagen (Kfz, …)
  - Konstruktionsunterlagen, …
- **Vertrieb, Verwaltung**
  - Kunden- und Lieferantendaten
  - Finanz-, Vertriebs-, Lieferantendaten, …
- **Produktion**
  - Steuerparameter
  - Produktionsdaten, …

Ziel von Manipulationen

Wettbewerbsvorteile

in, am Rande und außerhalb der Legalität

Strategie physisch/infrastrukturell

Vorgehensweise

- Planung, Errichtung, Betrieb und Kontrolle des Aufbaus und des Zusammenwirkens aller **physischen Bestandteile** der IT-Systeme
  - Gebäude und Infrastruktur (Ein- und Ausgänge, Zufahrten, …)
  - Versorgungs- und Entsorgungseinrichtungen
  - Verkehrs- und Übertragungswege
  - Installationen für Informationsverarbeitung und Kommunikation
- Planung, Einführung, Betrieb und Kontrolle aller **Abläufe** der Informationsverarbeitung und Kommunikation

unter dem gemeinsamen Prinzip

Leistungsfähigkeit + Sicherheit

Strategie personell

Prinzipien

- letztlich auf Kenntnis über Personen fußend (Nutzen klassischer Hilfsmittel der Psychologie)
- Risiken schlecht abschätzbar
- trotzdem unverzichtbar

Folgerungen

- sorgfältige Wahl der Personen (→ *„Wer soll, wer darf was wie tun?“)*
- niemals „Generalvollmachten“, Berechtigungen nach dem Minimalprinzip *(„need to know“)*
- Überwachung und Kontrolle von Personen (→ ***immer problematisch!***)
- letztlich Frage des Vertrauens in Personen

↓

Verhaltens- / Ehren-Codex
des Unternehmens (*code of honor*)

↓

Vorbild der Führungskräfte

Strategie organisatorisch

Information Controlling

Prinzip

- Festlegung (Planung)
- Bekanntmachung des Umgangs
- Kontrolle

aller IT-Systeme und **IT-Vorgänge**
des Unternehmens und ihrer Nutzung

Strategie informationstechnisch

Prinzip

Einsatz sicherer, also

verlässlicher und **beherrschbarer**

IT-Systeme in allen Teilen des Unternehmens

↓

Zentrale Frage der IT-Sicherheit

Wann sind IT-Systeme sicher?