IT-Sicherheit und ihre Besonderheiten – Duale Sicherheit –

Rüdiger Dierstein, S.M.
Weichselbaum 13, 82234 Oberpfaffenhofen

1. Sicherheit in der Informationstechnik

1.1 Merkwürdige Missstände[1]

Was ist ein „Sicheres System der Informationstechnik"? Die Antwort auf diese Frage fällt ganz verschieden aus, je nachdem, wen man nach der Bedeutung dieses Begriffes fragt. Es gibt dafür bisher keine hinreichend allgemeingültige, geschweige denn verbindliche Erläuterung oder gar Definition. Viele Ungereimtheiten, viele – meist unnötige – Diskussionen werden einfach dadurch verursacht, dass jedermann die Begriffe *Sicherheit*, *System* oder *Information* in der für seine Aufgaben bestgeeigneten Weise auslegt und interpretiert.

Die Fragen beginnen bereits beim Begriff *System*. Soll der Begriff *System der Informationstechnik* eingeschränkt werden auf das allgemeine Verständnis von Rechen- oder DV-System (englisch: *computer* oder *computer system*), was auch immer mit „allgemeinem Verständnis" gemeint ist? Soll die Software in den Bedeutungsumfang mit einbezogen werden? Wenn ja, ist dann auch alles, was zum organisatorischen Umfeld eines Rechners gehört, Bestandteil des Begriffs System? Ist es möglich – und sinnvoll – Rechensysteme zu untersuchen und dabei die Tatsache außer acht zu lassen, dass diese Systeme über die Ein- und Ausgabe aufs Engste mit Menschen verbunden sind? Ist es denkbar und möglich, die Sicherheit eines umfassenden Rechnernetzes zu untersuchen und zu bewerten und dabei die selben Kriterien anzuwenden wie bei der Analyse der Sicherheit eines einfachen Computers oder eines Programmbausteins? Fragen über Fragen!

Nicht viel anders sieht es aus mit der Bedeutung des Begriffs *Sicherheit*. Noch 1972, also vor rund 30 Jahren, konnte die IBM verbindlich definieren: [2]

Security Prevention of access to or use of data or programs without authorization

Immerhin war IBM damals der größte und einflußreichste Hersteller von Datenverarbeitungssystemen.

Auch wenn man dieser sehr eng gefaßten Definition einräumt, dass sie nur für einen bestimmten Teilbereich der Datenverarbeitung habe gelten sollen, so bleibt sie doch weit hinter dem zurück, was man schon zu jener Zeit vom Bedeutungsumfang und Bedeutungsinhalt des Begriffs Sicherheit hätte fordern müssen.

Das Hinterherhinken scheint für alles, was in der Informationstechnik auch nur entfernt mit Sicherheit zu tun hat, geradezu kennzeichnend zu sein. Genauer gesagt: es scheint kennzeichnend zu sein für die Informations- und Kommunikationstechnik, seit deren Leistungsfähigkeit durch programmierbare Automaten (Computer) in einer Weise gesteigert *und* verändert wurde, wie es vor 50 Jahren auch nicht annähernd vorhersagbar war. Warum aber klafft gerade in der Informationstechnik zwischen Leistungsfähigkeit und Sicherheit eine so große Lücke, größer als in jedem anderen Bereich der Technik?

Dem, der sich mit Informationstechnik beschäftigt, fällt noch ein weiterer Missstand auf. Man schlage irgend ein Glossar über Begriffe auf, die mit Systemen der Informationstechnik und deren Sicherheit zusammenhängen, und man stößt auf den größtmöglichen Wirrwarr. Nimmt man gar Glossare in verschiedenen Sprachen zur Hand, so ist die Verwirrung vollständig.

Um nur ein Beispiel zu nennen: Das englische *security* heißt auf deutsch Sicherheit, das englische *safety* aber ebenso. Wie muss dann umgekehrt der deutsche Begriff *Sicherheit* ins Englische übersetzt werden? Kein englischer Fachmann wird müde, auf den unverzichtbaren Unterschied zwischen den beiden englischen Begriffen hinzuweisen, für die es im Deutschen nur ***ein*** Wort gibt.

Es ist durchaus sinnvoll, darüber nachzudenken, weshalb Menschen auf dem für sie so wichtigen Gebiet der Informationstechnik und Kommunikation mit der Frage der Sicherheit so nachlässig umgehen, weitaus nachlässiger als in allen anderen Bereichen, in denen der Mensch sich auf die Technik, ihre Produkte und deren korrekte Funktion verlässt.

1.2 Das Umfeld

Die Ausgangssituation in der Informations- und Kommunikationstechnik ist bekannt: Es gibt in den entwickelten Industriestaaten der Welt heute keinen Wirtschaftszweig mehr, kein Forschungsgebiet, keine Verwaltung, keine Behörde oder irgendeine andere Organisationseinheit, die sich nicht bis in ihre letzten Verästelungen hinein moderner Informationstechnik bedient. Automatisierte Verarbeitung und Weitergabe von Daten ist zum Werkzeug geworden, ohne das unsere Gesellschaft, die Wirtschaft, Forschung oder Verwaltung die Leistungen nicht mehr erbringen können, die wir von ihnen erwarten und auf deren An-

[1] überarbeitete und ergänzte Fassung des Beitrags [Dst97]
[2] *IBM Data Processing Glossary* GC20-1699-4, File No. S360/S370-20, Fifth Edition, December 1972

nehmlichkeiten wir inzwischen nicht mehr verzichten wollen.

Mehr noch: auch außerhalb des Berufslebens dringen Computer und informationstechnische Werkzeuge der Kommunikation weiter und weiter vor. Es gibt fast keinen Lebensbereich mehr, und sei es der entlegenste Winkel unseres Privatlebens, in den nicht die automatisierte Informationsverarbeitung, diese alles verändernde Kombination aus Elektronik und Programmierung, gestaltend Einzug gehalten hätte.

Es ist mehr als berechtigt, danach zu fragen, wie dieses neue Werkzeug *Informationstechnik* unser aller Umgang mit Informationen beeinflußt und verändert. Dabei werde unter dem Begriff Informationstechnik alles zusammengefaßt, was an Technik der Datenverarbeitung und Kommunikation inzwischen zu einem vielfältig vernetzten Ganzen zusammengewachsen ist, das Aufbewahren und das Wiederfinden von Daten eingeschlossen. Die Vertrauenswürdigkeit moderner Informationstechnik steht hier zur Debatte und damit deren Sicherheit.

Insbesondere interessiert die Antwort auf die darin enthaltene Frage, ob wir uns auf Daten, die von Maschinen bearbeitet und weitergegeben werden, in gleicher Weise *verlassen* können wie bei Menschen. Für unsere Gesellschaft ist diese Antwort lebenswichtig. Sie hat seit Jahrhunderten Verfahren, Regeln, Organisationsformen, Vorgehensweisen und Techniken für den Umgang mit Daten – sei es auf Papier, sei es bei mündlicher Kommunikation – entwickelt, um bei deren Verarbeitung korrekte, reproduzierbare und vertrauenswürdige Ergebnisse zu erhalten und diese gezielt, rechtzeitig, unverfälscht und unbehelligt weitergeben zu können.

Sobald von Sicherheit *moderner* Informationstechnik die Rede ist, wird dies allzu gern als eine Frage gesehen, die *allein* von der Seite der Technik her zu beantworten ist. Solch eine eingeengte Betrachtungsweise lässt eine Grundtatsache außer acht: dass nämlich Daten und Information etwas sind, über das es wenig Sinn hat nachzudenken, *ohne* den Menschen mit einzubeziehen. Wenn hier nach Besonderheiten des Begriffs Sicherheit gefragt wird, dann hat diese Frage im Zusammenhang mit der Informationstechnik – mindestens – drei Facetten, nämlich die drei Fragen

- nach der Technik,
- nach dem Menschen und schließlich
- nach den Problemen, die aus dem Zusammenwirken beider entstehen.

1.3 Die technischen und wirtschaftlichen Randbedingungen

Die Ursachen für das Eindringen der Informationstechnik in alle Lebensbereiche sind bekannt. Man braucht nur die wichtigsten Meßgrößen der Rechentechnik von einst und jetzt einander gegenüber zu stellen, um auf einen Blick zu erkennen, in welch ungeheurem Maß sich allein die technischen und wirtschaftlichen Gegebenheiten in den letzten 30-35 Jahren verändert haben.

In knapp einer Generation wuchsen Rechengeschwindigkeit und Speicherkapazität um den Faktor 10^6–10^{10} und mehr. In ähnlichem Maße wie die Leistung stieg, nahm der Platz ab, den Hard- und Software benötigten – und gleichzeitig fielen die Preise dafür um Größenordnungen.

Der Faktor 10^6–10^{10}

Rechengeschwindigkeit

1965	≈ 1.000 FLOPS[3]
2000	≈ 1.000×10^9 FLOPS = 1 TFLOPS

Speicherkapazität

1960	einige 10^3 Byte (KByte)
2000	10^9–10^{12} Byte (GByte – Tbyte)

Miniaturisierung

1960	1 Schaltfunktion (Röhrenbaustein der Zuse Z22R) ≈ 250 cm^3 = ¼ ℓ
2000	≥10^8 Schaltfunktionen (ein Chip) ≈ 250 mm^3

Preisverfall

1963	300.000,-- DM je 1 Mbyte
2000	0,02 DM " "

Leistungsanstieg und Preisverfall ca. 1960 – 2000

Allein aus den nackten Zahlen der Tabelle lassen sich bereits Folgen dieser Entwicklung für die Sicherheit des Werkzeugs moderne Informationstechnik ablesen. Man bedenke: 1 GByte sind 1 Mrd. Zeichen. Wer eine Festplatte mit 1 GByte in seine Verfügungsgewalt bringt, macht sich zum Herrn über den Inhalt von rund 1000 Aktenordnern à 500 Schreibmaschinenseiten à 2000 Zeichen. Das kann der Datenbestand eines ganzen Forschungsinstituts oder des Archivs eines mittelgroßen Betriebes sein. Der Raumbedarf für diesen Datenberg schrumpft von mehr als 70 m^3 Papier auf rund 250 cm^3 = ¼ℓ zusammen. Eintausend Aktenordner komprimiert auf die Größe einer – mit Verlaub – Käseschachtel!

Bis zur Jahrtausendwende waren Speicher*chips* mit 2 Gbit = 256 MByte, also mit 256.000.000 Zeichen auf dem Markt. Vier dieser Chips haben die gleiche Kapazität wie die Festplatte mit 1 GByte, sind aber wesentlich schneller als diese und benötigen nur mehr einen Bruchteil des bisherigen Volumens.

Was für die Speicherkapazität gilt, kann mutatis mutandis auf das ganze Rechensystem übertragen werden. Wer vor 30, 40 Jahren einen „Computer" mit auch nur annehmbarer Leistung beiseite schaffen wollte, hätte sich einen Lastwagen mittlerer Größe besorgen müssen, um das schwere Möbel samt notwendigem Zubehör abtransportieren zu können – von der

[3] FLOPS = **Fl**oating point **o**perations **p**er **s**ec (Gleitkommaoperationen/s)

Schwierigkeit, dieses Unterfangen unbemerkt auszuführen einmal ganz abgesehen. Wer heute einen PC oder ein Arbeitsplatzsystem – wohlgemerkt mit deutlich größerer Leistung als der Computer damals – stiehlt, hat kaum noch Transportprobleme, und wer einen Laptop „mitlaufen" lassen möchte, verbirgt ihn einfach in seiner Aktentasche.

Beide Beispiele, Diebstahl von Speichern oder ganzen Rechnern, wurden inzwischen wiederholt erfolgreich praktiziert. Sie geben eine erste, einleuchtende Antwort auf die Frage nach den Besonderheiten der Sicherheit moderner Informationstechnik. Nur bleibt diese Antwort zu sehr an der Oberfläche und reicht bei weitem nicht aus. Sie muss vertieft und vor allem wesentlich allgemeiner gegeben werden.

2. Besonderheiten in den Definitionen der Grundbegriffe der Informationstechnik – das Kontextproblem

Die Besonderheiten und damit die Probleme beginnen bereits bei den für die Informationstechnik und IT-Sicherheit grundlegenden Begriffen *Zeichen* und *Datum*. Diese Begriffe werden oft genug gar nicht definiert oder mit wechselnder Bedeutung gebraucht – wobei der Leser dann raten darf, welche Bedeutung von Fall zu Fall gemeint ist, – oder aber ihre Bedeutung wird in jeder Veröffentlichung anders festgelegt, eine Vorgehensweise, die das Verständnis auch nicht sonderlich erleichtert.

Diese Unsauberkeit ist um so befremdlicher, als – zumindest im Deutschen – in der DIN 44300 (**D**eutsches **I**nstitut für **N**ormung) für die grundlegenden und viele darauf aufbauende Begriffe aus der Informations- und Kommunikationstechnik seit über 30 Jahren Standarddefinitionen angeboten werden. (Die im Folgenden nach der Fassung vom November 1988 zitierten Definitionen sind gegenüber der vorhergehenden Ausgabe von 1972 in allen wesentlichen Teilen unverändert geblieben.)

Nicht alle dieser Begriffserklärungen sind Definitionen im strengen Sinn; denn zum gegenwärtigen Zeitpunkt scheint für einige Begriffe, die hier benötigt werden, eine strenge Form der Definition noch nicht möglich zu sein.

Die Erklärungen der DIN bieten aber Festlegungen an, die sowohl umfassend als auch genau genug sind, um als Basis für weitere Diskussionen zum Thema Sicherheit zu dienen. Sie schaffen ferner einen Begriffsrahmen, in dem eine Verständigung und damit eine sinnvolle Diskussion möglich ist, und sei es zunächst auch nur im Rahmen dieser Veröffentlichung.

Hinzu kommt eine weitere, im Zusammenhang mit der Frage nach den Besonderheiten der Sicherheit in der Informationstechnik besonders schätzenswerte Eigenschaft der DIN-Definitionen. Interpretiert man sie wörtlich und schränkt sie nicht vorschnell auf rein technische Gegebenheiten ein – was auch nirgendwo in der DIN verlangt wird – so lassen sich aus ihnen bereits Antworten auf das Kernproblem dieses Beitrags herleiten, nämlich Antworten auf die Frage: „Wieso ist Sicherheit in der Informationstechnik in bestimmten Punkten etwas Besonderes, etwas Anderes als in anderen Bereichen der Technik?"

2.1 Zeichen – das Problem der uumittelbaren Wahrnehmung

Physikalische Grundlage aller Datenverarbeitung und aller Kommunikation sind **Zeichen**, d.h. wahrnehmbare und erkennbare physikalische Gebilde irgendwelcher Art. Sie müssen nur endlich und unterscheidbar sein, damit sie erkannt werden können. **Wer** die Zeichen wahrnimmt, ob eine Maschine oder ein Mensch oder beide, darüber wird in der Definition nichts festgelegt. DIN 44 300 definiert in folgender Weise:

Begriff	Definition (DIN 44 300)
Zeichen *character*	Ein Element (als Typ) aus einer zur Darstellung von Information vereinbarten endlichen Menge von Objekten (**Zeichenvorrat**, *character set*), auch jedes Abbild (als Exemplar) eines solchen Elements.
Nachricht *message*	Gebilde aus Zeichen* oder kontinuierliche Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Information darstellen und die zum Zwecke der Weitergabe als zusammengehörig angesehen und deshalb als Einheit betrachtet werden.
Daten *data*	Gebilde aus Zeichen* oder kontinuierliche Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Information darstellen, vorrangig zum Zwecke der Verarbeitung und als deren Ergebnis Anmerkung: Verarbeitung umfaßt die Durchführung mathematischer, umformender, übertragender und speichernder Operationen. Der wesentliche Unterschied zwischen Daten und Nachricht* liegt in ihrer Zweckbestimmung.

Ebenso wenig wird in den Definitionen irgend etwas darüber ausgesagt, **wie** Zeichen wahrgenommen werden, mit welchen der fünf Sinne: ob durch sehen, hören, fühlen, riechen, schmecken bleibt völlig offen.

Genau an dieser Stelle steckt aber bereits das erste Kernproblem der Sicherheit moderner Informationstechnik.

> Maschinelle, digitale Systeme der Informationstechnik arbeiten fast ausschließlich mit **magnetischen** oder **elektromagnetischen Zeichen**. Physikalische Darstellungen dieser Art sind aber für den Menschen **ohne technische Hilfsmittel nicht wahrnehmbar**.

Um zu erkennen, was in einem Digitalrechner oder auf digitalen Übertragungsstrecken an Zeichen aufgenommen, aufbewahrt, verarbeitet und weitergegeben wird, ist der Mensch immer auf Werkzeuge, auf Hard- oder Software angewiesen, mit deren Hilfe die magnetischen und elektromagnetischen internen Darstellungen in Zeichen umgesetzt werden, die für ihn direkt wahrnehmbar sind. In der digitalen Datenverarbeitung und Kommunikation gibt es damit durchweg, von wenigen Ausnahmen abgesehen, **keine Möglichkeit der *unmittelbaren* Wahrnehmung.**

Lediglich im schmalen Frequenzband von 0,4µm – 0,8µm kann der Mensch elektromagnetische Zeichen als optische Zeichen *unmittelbar* wahrnehmen, in einigen Bereichen >1µm auch Infrarotwellen als Wärme empfinden.

Wie vertrauenswürdig die Abläufe und deren Ergebnisse in einem Rechen- oder Kommunikationssystem sind, hängt danach entscheidend mit ab von der Vertrauenswürdigkeit der Umsetzungen und der für diese Umsetzungen benötigten Hard- und Software im Rechner.

Diese Abhängigkeit hat schwerwiegende Folgen, und zwar nicht nur, wenn es sich um rechtsverbindliche Vorgänge im Geschäftsalltag handelt, sondern grundsätzlich. Denn aus der Unmöglichkeit für den Menschen, Zeichen in modernen Systemen der Informations- und Kommunikationstechnik *unmittelbar* wahrzunehmen, folgt notwendig:

> Wo immer moderne Informationstechnik als Werkzeug benutzt wird, gibt es **keine direkte Inaugenscheinnahme**. Damit entfällt für alle rechtsverbindlichen Vorgänge die Möglichkeit des
>
> **Augenscheinbeweises**.

Der Augenscheinbeweis muss durch andere, völlig neue Techniken ersetzt werden. Diese Techniken müssen mindestens ebenso vertrauenswürdig sein wie die unmittelbare Wahrnehmung.

Ohne allzu weit ins Einzelne zu gehen, mache man sich klar, dass dieses Ersetzen durch neue Techniken weit mehr ist als lediglich das Auswechseln eines bisher manuell vollzogenen Vorgangs gegen sein elektronisches Gegenstück. So genügt es beispielsweise nicht, die klassische persönliche Unterschrift durch ein elektronisches Analogon zu ersetzen. Klassisches „Unterschreiben" ist sehr viel mehr als nur das Erzeugen des Namenszuges. Es umfaßt, je nach Wichtigkeit des Vorgangs, der durch die Unterschrift rechtswirksam werden soll, eine Vielzahl technischer und organisatorischer Zusätze und Randbedingungen, die erst in ihrem Zusammenwirken das Maß der Vertrauenswürdigkeit einer Unterschrift ausmachen. Dazu gehört z.B. die Art des Papiers, der Vollzug der Unterschrift im Beisein von Zeugen, die Bestätigung durch eine Amtsperson (Notar), das Verbot von Korrekturen oder Löschungen, usf. (vgl. dazu insbesondere [prov94]).

Nahezu alle diese Vorkehrungen und Randbedingungen, die den ***Kontext*** einer Unterschrift ausmachen, gehören im klassischen Rechtsverkehr zu den unmittelbar wahrnehmbaren Vorgängen oder Daten (Ergebnissen). Man denke als Beispiel nur an die notarielle Bestätigung der Authentizität einer Person durch die Formel „Ist dem Notariat persönlich bekannt." Solche und viele weitere verwandte Randbedingungen müssen im elektronischen Rechtsverkehr durch andere, neue Techniken und Organisationsformen ersetzt werden, wenn die Möglichkeit der unmittelbaren Inaugenscheinnahme entfällt.

2.2 Daten und Information – das Problem der Interpretation

Der Begriff *Information* wird in der DIN 44300 nicht definiert, sondern nur in einer Anmerkung erläutert.[4] Im Sinne einer umgangssprachlichen Festlegung wird in der Norm vereinbart:

Information	Kenntnisse über Sachverhalte und Vorgänge

Die DIN 44300 enthält deshalb auch keine Definitionen für zusammengesetzte oder abgeleitete Begriffe wie *Informationsverarbeitung* oder *Informationsverarbeitungssystem*.

Untersuchungen darüber, was Information ist, wie sie entsteht, wie sie wirkt, wie man sie messen, wie man sie beschreiben kann, gibt es zu Hunderten. DIN 44300 tat gut daran, das Für und Wider nicht aufzugreifen und sich mit einer „plausiblen" Umschreibung zu begnügen. Diese Umschreibung ist offensichtlich ein Zirkelschluß; denn *Information* wird hier durch den Begriff *Kenntnisse* erklärt, und der wiederum hängt in der Luft. Die Norm verlässt sich hier auf ein natürlichsprachliches Verständnis des Definiens. Gibt man sich aber mit dieser Ungenauigkeit zufrieden, so lassen sich aus allen folgenden Festlegungen und Erklärungen der Norm weitreichende Schlüsse ziehen.

Das Erstaunliche ist, dass *Information* in der Norm nur noch zweimal benutzt wird, nämlich bei den Definitionen der Begriffe *Zeichen* und *Daten,* dann nicht mehr. Wer die DIN von dieser Warte aus der Unsau-

[4] Das Zeichen * nach einem Wort in den Definitionen gibt bei DIN an, dass dieser Begriff an anderer Stelle der Norm erklärt wird.

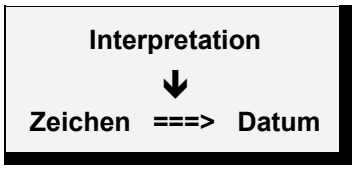
berkeit bezichtigt, der möge sich in deutschen – und in internationalen! – Veröffentlichungen der letzten 40, 50 Jahre umsehen. In ein und demselben Schriftstück wird wahllos zwischen *Datum* (engl. *data*) und *Information* hin- und hergesprungen.

Was die DIN-Definition für **Daten**[5] auszeichnet, ist, dass sie so eng wie möglich an den entscheidenden Zusammenhang zwischen **Zeichen** und vereinbarter oder unterstellter **Bedeutung** anknüpft, durch den überhaupt erst eine Beziehung zwischen Daten und Information zustande kommt. Der Hinweis auf diese entscheidende, Daten kennzeichnende Eigenschaft fehlt in anderen Definitionen fast überall. Aus der DIN-Definition folgt direkt:

> Zeichen werden erst dadurch zu **Daten** und damit zu Informationsträgern, dass ihnen eine **Bedeutung zugeordnet** wird, d.h. dass sie **interpretiert werden.**

Ganz bewusst wird in der DIN nichts darüber ausgesagt

- **wer** den Zeichen die Bedeutung unterlegt (Mensch oder Maschine),
- **wie** das geschieht (in Maschinen durch Programme, in Menschen auch anders),
- **woher** die Bedeutung „genommen" wird.



Interpretation und IT-Sicherheit

In diesen Fragen nach der Art der Interpretation, der Zuordnung von Bedeutung zu Zeichen, steckt wiederum eine Besonderheit und damit ein weiteres Kernproblem der Sicherheit in der Informationstechnik.

Interpretation in maschinellen datenverarbeitenden Systemen geschieht immer durch Programme, sei es durch Hard-, sei es durch Software. Die Folge für die Vertrauenswürdigkeit der Verarbeitung und der Kommunikation mit maschinellen Systemen liegt auf der Hand: Die Interpretation der Maschine ist nur durchschaubar, solange die interpretierenden **Programme nachvollziehbar oder durchschaubar** sind. Also ist auch das, was die Maschine an Ergebnissen, was sie an Daten erzeugt, nur solange durchschaubar und damit vertrauenswürdig, solange es die dafür eingesetzte Hard- und Software ist.

Selbstverständlich kann auch im Menschen Interpretation programmiert geschehen. In aller Regel geht sie aber wesentlich darüber hinaus. Welche Bedeutungen der Mensch Zeichen unterlegt, welche Information er damit aus ihnen gewinnt oder gewinnen kann, hängt von seinem Wissen, von seinem Können, seiner Erfahrung, seiner Intuition, seinem Gefühl, vom gesamten momentanen Umfeld der Interpretation ab, kurz: vom gesamten **Kontext**, in dem der Mensch Zeichen aufnimmt, verarbeitet und weitergibt.

Für die Kommunikation zwischen zwei oder mehreren Partnern heißt das, dass sowohl dem Sender als auch dem Empfänger die Abmachungen – also der Kontext – bekannt sein müssen, nach denen die gesendeten oder empfangenen Zeichen zu interpretieren sind, wenn denn beim Empfänger genau die Information ankommen (lies: erzeugt werden) soll, die vom Sender gemeint war.

Ein Beispiel: Das akustische Zeichen ***[i:gl]***, über eine Telefonleitung von den USA nach Deutschland oder umgekehrt übertragen, wird nur dann bei Sender und Empfänger mit der gleichen Information *Adler* verbunden, wenn beide zuvor vereinbart oder unterstellt hatten, dass der Interpretation des Gesprochenen resp. des Gehörten die Sprache *Englisch* zugrunde gelegt werden soll.

Vor diesem Hintergrund ist es unsinnig anzunehmen, eine bloße Erhöhung der Übertragungsgeschwindigkeit, d.h. der Menge der übertragenen Zeichen, müsse zwangsläufig die Kommunikation verbessern. Dieses Eindrucks kann man sich zuweilen in Diskussionen über Multimediasysteme nicht erwehren. Ein Mehr an Zeichen oder Bits kann die Kommunikation nur dann verbessern, wenn gleichzeitig geeignete Werkzeuge bereitstehen, mit denen dieses Mehr quantitativ und qualitativ auch interpretiert werden kann. Dazu gehören als erstes verbesserte Werkzeuge für das Auffinden, Sortieren und Sichten und für das Weiterverarbeiten der übertragenen Zeichen.

2.3 Das Kontextproblem

Die Tatsache, dass erst die Interpretation aus Zeichen Daten macht und damit Information schafft, wirft ein Schlaglicht auf ein Problem vertrauenswürdiger Informations- und Kommunikationstechnik, das immer noch viel zu wenig beachtet wird. Dieses Problem tritt vor allem dort auf, wo moderne Werkzeuge der Informationstechnik wie z.B. Computer bisher noch nicht oder kaum benutzt worden sind und erst jetzt mit Macht althergebrachte Kommunikations- und Verarbeitungsformen flächendeckend beiseite schieben. Beispiele: Arztpraxen, Kanzleien, Kleinbetriebe und viele andere mehr.

Wo der Mensch Vorgänge der Kommunikation oder der Informationsverarbeitung an Maschinen übergibt, die er bisher allein oder mit Hilfe manueller Werkzeuge bewältigt hat, überträgt er nicht nur Teile der Verarbeitung einem Werkzeug, sondern er überlässt dem Automaten (Computer) **die Interpretation** dessen, was er an Zeichen für die Informationsverarbeitung aufnimmt, speichert, verarbeitet oder weitergibt.

Wenn Information durch Interpretation von Zeichen gewonnen wird, dann hängt die Antwort auf die Fra-

[5] *Verarbeitung* enthält – auch nach DIN – die *Weitergabe*. Der Begriff *Nachricht* ist deshalb in der Definition von *Datum* enthalten und letztlich redundant.

ge, welche Information aus einer Zeichenkette entnommen wird, entscheidend davon ab, in welchem **Kontext** die Zeichenkette interpretiert wird, das heißt, wer das tut, wann, wo, mit welchen Kenntnissen, zu welchem Zweck, unter welchen Voraussetzungen, etc. Das führt folgerichtig zu einer einfachen, jedoch für die Sicherheit der Informationstechnik, d.h. für deren Verlässlichkeit und Beherrschbarkeit wesentlichen Schlußkette:

- Ein programmierbarer Automat (Computer) interpretiert nach anderen Regeln als ein Mensch. Was ihm in Hard- oder Software nicht als Programm vorgegeben ist, nachgerüstet oder über Programme geändert werden kann, kann von einem Automaten nicht für die Interpretation und damit nicht für die Gewinnung, Bereitstellung und Weitergabe von Information herangezogen werden.
- Auch der Mensch interpretiert mit Hilfe angeborener oder erlernter Algorithmen (Programme), aber nicht ausschließlich. Wichtigen Teilen seiner Interpretation und damit seiner Art und Weise, Information zu gewinnen, liegen „Mechanismen" offenbar ganz anderer Art zugrunde. Auch wenn die Funktionsweisen dieser andersartigen Interpretationsweisen wie z.B. Intuition, Assoziation, Gefühle, Stimmungen, … bis heute nur in Ansätzen bekannt sind, wissen wir doch aus Erfahrung, insbesondere aus der Kommunikation mit anderen Menschen, dass es solche anderen Interpretationsweisen gibt und beziehen sie in unser Verhalten gegenüber unserer Umgebung ständig mit ein.
- Mit wachsender Komplexität und Flexibilität der in Automaten ablaufenden Programme, insbesondere bei adaptierenden und lernenden Algorithmen, wird die Interpretation und damit die Arbeitsweise technischer informationsverarbeitender Systeme immer weniger durchschaubar. Damit wächst zwangsläufig die Abhängigkeit des Menschen und damit der Gesellschaft von der vertrauenswürdigen, korrekten Arbeitsweise dieser Systeme.

2.4 Umsetzbarkeit von Kontexten

Bei dem Kontextproblem, das hier in der Beziehung Mensch ⇔ Maschine sichtbar wird, geht es um viel mehr als nur um den korrekten und reibungslosen Ablauf von Prozessen in maschinellen Systemen.

Wenn nach den Kontexten gefragt wird, in denen Datenverarbeitung und Kommunikation ablaufen, dann spielen Einflußgrößen wie Zweck, Notwendigkeit, Zulässigkeit, Verträglichkeit mit Bisherigem, Plausibilität und vieles Andere mehr eine entscheidende Rolle. Diese Art von Kontexten ist Automaten – wenigstens bis heute und wohl auch in absehbarer Zukunft – so gut wie nicht zugänglich. Wichtiger noch, solche Kontexte sind auch mit menschlicher Nachhilfe kaum oder gar nicht sinnvoll in Algorithmen und Programme umsetzbar.

Sicherheit von IT-Systemen muss deshalb auch die Frage beantworten, ob denn eine Aufgabe, die in irgendeinem Teilbereich der Gesellschaft (Unternehmen, Behörde, Bank, Arztpraxis, …) einem technischen System zur Ausführung übertragen werden soll, von diesem tatsächlich so gelöst werden **kann**, dass nicht nur die technischen Anforderungen an die Ausführung erfüllt werden, sondern dass auch den Anforderungen der Betroffenen Genüge getan wird und das heißt, dass die Belange der Betroffenen nicht unzulässig beeinträchtigt werden (vgl. dazu Abschnitt *Duale Sicherheit – die Beziehung Mensch ⇔ Maschine).*

Überall dort, wo subjektive, intuitive Komponenten des Kontextes in der Kommunikation eine wesentliche Rolle spielen, insbesondere Komponenten, deren Wirkmechanismen wir bis heute nicht oder nur unvollkommen kennen, muss dem Übergang Mensch→ Maschine ernstlich misstraut werden. Das bloße *„Mehr und schneller"* – das übrigens schon für die Erörterung der bloßen *technischen* Sicherheit von IT-Systemen nicht mehr genügt – ist als alleinige Begründung beim Übergang Mensch→Maschine völlig unzureichend. Denn wo Teile einer Datenverarbeitung oder einer Kommunikation, die bisher von Menschen ausgeführt wurden oder zwischen Menschen abliefen, einem maschinellen System übertragen werden sollen, muss sich nach dem bisher Gesagten unvermeidlich der Kontext und damit auch die Information ändern.

Wenn aber Datenverarbeitung und Kommunikation ganz oder teilweise vom Menschen auf automatisierte Systeme der Informationstechnik übertragen werden, dann können die Jahrhunderte lang zwischen Menschen eingeübten und bewährten Regeln für den Umgang mit Informationen nur noch sehr bedingt gültig bleiben.

In anderen Worten: an die Stelle althergebrachter und bewährter Ordnungen für den Umgang mit Daten und Informationen müssen in der modernen Informations- und Kommunikationstechnik neue Ordnungen treten, die die einschneidenden technischen und strukturellen Veränderungen berücksichtigen und auch unter völlig veränderten technischen und organisatorischen Randbedingungen sichere, das heißt verlässliche und beherrschbare Datenverarbeitung und Kommunikation gewährleisten.

Die anhaltende Diskussion um die Nutzung von Chipkarten in der medizinischen Versorgung liefert genügend Beispiele für die Fehleinschätzung, nach der Maschinen (Automaten) ohne weiteres informationstechnische Aufgaben übernehmen können, die bisher der Mensch ausgeführt hat.

Ein Beispiel: Nach gängiger Ansicht ist das Verhältnis Arzt⇔Patient hochgradig von subjektiven Faktoren bestimmt. Stichwort: *psychosomatische Wechselwirkungen*. Wenn diese Ansicht richtig ist, dann kann eine Chipkarte zwar in vielen Fällen hilfreich sein (z.B. für die Anamnese). Sie kann aber nicht den persönlichen Kontakt zum Arzt ersetzen, schon gar nicht

aufgrund ihrer vorgeblichen „Objektivität". Dieser Begriff ist im Zusammenhang mit dem, was zuvor über Kontext und Interpretation gesagt wurde, für die Beschreibung des Verhältnisses Arzt ⇔ Patient nachgerade eine contradictio in adjecto. Man bedenke nur, dass die Information zwischen Arzt und Patient durch Kommunikation zwischen *beiden* und durch Interpretation *beider* entsteht.

Die Quintessenz dieses ganzen Abschnitts lässt sich danach eher in einer Frage als in einer Aussage zusammenfassen:

Leitfrage

Welche Aufgaben dürfen ganz oder teilweise einem maschinellen System der Informationstechnik übertragen werden, ohne dass dabei aufgrund **fehlender, unzulässig veränderter oder nicht in einem Automaten darstellbarer Kontexte** Interpretationen und damit Ergebnisse der Datenverarbeitung entscheidend und zum Nachteil der Betroffenen verändert werden?

3. Informationsverarbeitende Systeme – IT-Systeme – Systeme der Informationstechnik

Im vorhergehenden Abschnitt wurden Besonderheiten des Begriffs Sicherheit aufgezeigt, die berücksichtigt werden müssen, sobald man ihn mit der Informationstechnik in Verbindung bringt. Dazu genügte es zunächst, einige Grundbegriffe der Informationstechnik genauer daraufhin anzusehen, wie ihre Definitionen sich auf die Bedeutung des Begriffs Sicherheit auswirken. Spätestens beim Problem des Kontextes zeigte die Herleitung, dass das Zusammenwirken von Mensch und Maschine bei solchen Überlegungen eine besondere Rolle spielt.

Ehe auf diesen Zusammenhang im Abschnitt *Duale Sicherheit* ausführlicher eingegangen wird, soll der für alles Folgende zentrale Begriff *IT-System* präziser gefaßt werden.

3.1 Definitionen und Erläuterungen

Eine sinnvolle, auch für die zum Teil schon angesprochenen Probleme der Sicherheit in der Informationstechnik brauchbare Definition des Begriffes ***IT-System*** muss zwei Extreme zu vermeiden suchen:

- Der Begriff IT-System darf keinesfalls vorschnell eingeschränkt werden auf technische, maschinelle Systeme oder Hilfsmittel. Ebensowenig darf er eingeengt werden auf im Sinne der Umgangssprache „komplette" Systeme, weder im Sinne von *abgeschlossen* noch im Sinne von *vollständig*. Unter wohlbestimmten, stets festzulegenden Voraussetzungen muss er Komponenten oder Teilfunktionen von Systemen ebenso umfassen wie ganze Systemkomplexe (Netze, Verbünde jeder Art u.a.m.).
- Der Begriff IT-System soll aber auch nicht zu weit gefaßt werden. Es dürfen in den Bedeutungsumfang des Begriffes nicht zu viele Aspekte hineingepackt, die Grenzen des Bedeutungsfeldes nicht zu unscharf gefaßt werden. Der Begriff würde sonst zu umfassend und zu ungenau und ließe von vornherein Raum für fast beliebige Missverständnisse

Der Grundgedanke der folgenden Definitionen ist, bestimmte, auch zusammengesetzte Gebilde als eine Einheit zu betrachten, sei es, weil sie von Haus aus als Einheit gegeben *sind*, sei es, weil sie für den Zweck der Betrachtung als ein funktionelles oder strukturelles Ganzes angesehen werden *können*.

Begriff	Definition (DIN 44 300)
Funktionseinheit *functional unit*	Ein nach Aufgabe oder Wirkung abgrenzbares Gebilde.. *Anmerkung*: Ein System von Funktionseinheiten kann in einem gegebenen Zusammenhang wieder als eine Funktionseinheit aufgefaßt werden. Der Funktionseinheit können eine oder mehrere Baueinheiten* oder Programmbausteine* oder beides entsprechen.
Rechensystem, Datenverarbeitungssystem *computer system, data processing system*	Eine Funktionseinheit* zur Verarbeitung und Aufbewahrung von Daten*. Verarbeitung umfaßt die Durchführung mathematischer, umformender, übertragender und speichernder Operationen.

In der DIN-Definition des Datenverarbeitungssystems (DV-Systems) war – und ist – die bereits angedeutete Gefahr versteckt, den Begriff ***DV-System*** zu früh auf die bloße Bedeutung von Rechner (Compu-

ter) mit oder ohne Software einzuschränken. Die Vergangenheit hat gezeigt, dass man landauf, landab dieser Gefahr oft genug erlegen ist. Wo von DV-System die Rede ist, wird fast immer nur an Computer gedacht. Das wird spätestens dann fatal, wenn es nicht mehr nur um die Sicherheit einzelner, in sorgfältig abgeschotteter Umgebung installierter Rechenanlagen geht (Rechenzentrum), sondern um Tausende, fast völlig frei zugängliche „Personal Computer (PC)", die über Netze zu kaum noch überschaubaren komplexen Systemen miteinander verbunden sind, und zwar zu Komplexen, in denen die einst weitestgehend getrennten Gebiete **Datenverarbeitung** und **Kommunikation** ineinander übergehen und völlig miteinander verschmelzen.

Zum anderen ist in der DIN-Definition auf den ersten Blick nicht erkennbar, welche Rolle der Mensch darin spielt, sei es als informationsverarbeitendes Ganzes, sei es als Teil einer Mensch-Maschine-Kombination. Es genügt aber eine geringfügige Verallgemeinerung der DIN-Definition, um dem Mangel einer zu engen Bedeutung des Begriffs IT-System zu begegnen.

Begriff	Definition (DIN 44 300 entsprechend)
System der Informationstechnik, IT-System *it-system*	Eine Funktionseinheit* zur Aufnahme, Verarbeitung, Aufbewahrung und Nutzung von Daten*.

3.2 Beispiele für IT-Systeme

Offensichtlich reichen die Beispiele, auf die die Definition der DIN ebenso wie die hier weiter gefaßte Definition des IT-Systems angewendet werden können, erheblich über das hinaus, was man gemeinhin unter Daten- oder Informationsverarbeitungssystem zu verstehen gewohnt ist. Nimmt man den Inhalt einer der beiden Definitionen ganz einfach wörtlich, dann mag das nächstliegende Beispiel für solch ein System auf den ersten Blick überraschen, es liegt aber auf der Hand: Das bekannteste, weitest verbreitete Gebilde, das als funktionelle Einheit mit Daten so umgehen kann, wie es diese Definition des IT-Systems aussagt, ist **der Mensch.**[6]

Denn wenn es überhaupt Tätigkeiten gibt, die den Menschen in besonderer Weise auszeichnen, sei es wegen der Art, in der er sie ausführt, sei es wegen ihrer Bedeutung für seine Existenz, so sind es diejenigen Tätigkeiten, die in irgendeiner Weise mit der Aufnahme, Verarbeitung, Aufbewahrung, Weitergabe oder sonstigen Nutzung von Daten oder Informationen zu tun haben. Der Mensch ist in diesem Sinne ***das*** informationsverarbeitende System per se.

Den Menschen in solcher Weise als „informationstechnisches System" zu sehen, mag manch einen auf den ersten Blick befremden. Wo aber von IT-Sicherheit die Rede ist, tut man gut daran, den Menschen von Anfang an in die Überlegungen mit einzubeziehen. Tut man es nicht, ist man schon im Ansatz der Gefahr erlegen, die ganze Betrachtung der IT-Sicherheit auf eine rein technische und damit, was die Auswirkungen der Informationsverarbeitung angeht, völlig einseitige Sicht einzuschränken.

Menschen

andere Lebewesen

Computer
- Mainframes
- Arbeitsplatzsysteme, PCs
- Prozessrechner

Subsysteme und Komponenten
- Bausteine und Programme
- Betriebssysteme
- Anwendungssysteme
- Netzkomponenten

IT-Komplexe
- Rechenzentren
- Rechnernetze
- Kommunikationsnetze

Teile der Gesellschaft (Unternehmen)
- als informationsverarbeitende Subsysteme aus Menschen *und* Maschinen

Beispiele für IT-Systeme

Eigentlich sollte es selbstverständlich sein, dass das Thema Sicherheit in der Informationstechnik nicht behandelt werden kann, ohne den Menschen als *mit entscheidende* Komponente mit einzubeziehen. Dass es dennoch immer wieder getan wird, steht auf einem anderen Blatt! Wenn von *Informations*technik die Rede ist, dann ist der Mensch davon unmittelbar betroffen, weil „Information" ohne Beteiligung des Menschen in diesem Zusammenhang eine leere Worthülse ist.

Entscheidende Komponente heißt hier, dass der Mensch als Sender, als Empfänger, als Nutzer, als Transformator, als Korrelator, kurz als eine, in ihrer Funktion variable Komponente eines zusammengesetzten IT-Systems, aber auch als eigene Funktionseinheit, also selbst als IT-System auftreten kann und auftritt.

[6] Selbstverständlich gibt es Informationsverarbeitung in der Biosphäre auch außerhalb des Menschen. Das wird mit dieser Aussage nicht angezweifelt. Es geht in diesem Beitrag jedoch vor allem – im Zusammenhang mit der Informationsverarbeitung durch und für Menschen – um den Unterschied zwischen Mensch und Maschine und um die Wechselwirkung zwischen diesen beiden.

Selbstverständlich fallen unter die Definition des IT-Systems alle Arten von *Rechnern und deren Komponenten*, alle Hardware, Software und deren Kombinationen, alle Arten von digitalen oder analogen Rechengeräten, von Programmen, Softwaresystemen, ebenso auch alle informationsverarbeitenden Komponenten beliebiger anderer Systeme, solange sie in einer gegebenen Umgebung oder in einem bestimmten Kontext als Funktionseinheit aufgefaßt werden oder werden können.

Nach der Definition kann aber auch jeder größere, kompliziertere Komplex von Elementen als IT-System bezeichnet werden, sofern er als eine Einheit betrachtet wird. Jedes *Rechenzentrum* ist ein typisches Beispiel für solch eine komplexere Funktionseinheit. Als IT-System aufgefaßt, umfaßt es nicht nur die gesamte Hard- und Software, sondern auch die organisatorischen Strukturen, alle Personen, die in irgendeiner Weise mit dem Rechenzentrum in Beziehung stehen, und zwar nicht nur während des regulären Betriebs, sondern ebenso auch in allen Sondersituationen (Wartung, Fehler, Wiederanlauf, Test, Vorführung, Katastrophe, …), schließlich auch die gesamte Infrastruktur. die Gebäude, die Ver- und Entsorgung, Klimaanlagen, nicht zu vergessen alle Sicherheitsvorkehrungen, Not- und Backupsysteme, usw.

Jede Behörde, jede Verwaltungseinheit, jedes Unternehmen ist als *Funktionseinheit*, also als ein nach Aufgabe und Funktion abgrenzbares Gebilde betrachtet, solch ein komplexes IT-System. Genauer: jede solche Funktionseinheit enthält als Substruktur ein oder mehrere Systeme der Informationstechnik, die als Komponenten sowohl Menschen als auch nicht-menschliche Bestandteile enthalten. Für zusammengesetzte Systeme wie Rechnerverbünde, Rechnernetze oder Kommunikationsnetze gilt Entsprechendes.

Alles, was in einem IT-System nicht-menschlicher Bestandteil ist, werde im Folgenden kurz unter dem Begriff **maschinell** subsumiert, also auch die Akte, das Papier, auf dem geschrieben wird, die Schreibmaschine, das Telefon, kurz alles, was irgendwie als Hilfsmittel oder Werkzeug für Datenverarbeitung und Kommunikation benutzt wird oder benutzt werden kann.

4. Duale Sicherheit – die Beziehung Mensch ⇔Maschine

Mit den Aussagen im vorhergehenden Abschnitt tritt an die Stelle einer rein technischen Betrachtung eine wesentlich umfassendere Sichtweise, die den Menschen grundsätzlich in die Überlegungen zum Problem IT-Sicherheit mit einbezieht.

Schon für die Sicherheit einfacherer, überschaubarer Systeme wie z.B. für den simplen, einzelnen PC ist die Unterscheidung ob mit oder ohne Mensch entscheidend. Es sind zwei völlig verschiedene Dinge, ob unter dem Gesichtspunkt der Sicherheit lediglich der PC selbst, der *maschinelle Anteil* des Systems, betrachtet wird, oder ob man den Menschen als Systemkomponente, als Teil der Funktionseinheit in die Betrachtungen einschließt.

Ohne den Menschen endet die Betrachtung in einer rein technischen Auslegung des Begriffs IT-Sicherheit. Wird der Mensch mit einbezogen, führt die Betrachtung zu einer ***dualen Sicht*** des Begriffs Sicherheit. Diese Sicht beschränkt sich nicht auf die bloße ordnungsmäßige Funktion und Verlässlichkeit des Werkzeugs Informationstechnik, sondern bezieht als wesentlichen Bestandteil die Auswirkungen seiner Nutzung mit ein, und zwar die Auswirkungen sowohl auf die einzelnen Benutzer als auch auf das gesamte Umfeld.

4.1 Mehrseitige Sicherheit

Dass Sicherheit in der Informationstechnik von mehreren Seiten aus betrachtet werden muss und nicht vorschnell auf die eine, enge Sicht technischer Verlässlichkeit eingeschränkt werden darf, wird schon seit längerer Zeit von verschiedenen Autoren direkt oder indirekt gefordert (vgl. dazu u.a. [Cha85], [Dst90], [Cdn93]).

In [RPM96] weisen *Rannenberg, Pfitzmann* und *Müller* eindringlich darauf hin, dass die Begriffe *Benutzer* oder *Betroffener* auf keinen Fall zu eng ausgelegt werden dürfen. Insbesondere dürfen sie nicht auf den „Anwender" im engeren Sinn eingeschränkt werden. Denn IT-Sicherheit wird nicht nur von diesen gefordert, sondern genau so berechtigt und genau so notwendig auch von Systembetreibern, von Herstellern, von Juristen, kurz: von einer Vielzahl anderer Personen und Institutionen, die von der Verlässlichkeit und Beherrschbarkeit der Informationsverarbeitungs- und Kommunikationssysteme in vielfältig betroffen oder abhängig sind.

In [RPM96] wird für diesen weitergehenden Ansatz der Begriff **mehrseitige Sicherheit** eingeführt und damit klar gemacht, dass IT-Sicherheit stets von mehreren Seiten, d.h. aus der Sicht verschiedener Gruppen von Betroffenen oder Interessenten beleuchtet werden muss. Die Ziele und damit die Anforderungen der verschiedenen Interessentengruppen werden nur in wenigen Fällen konvergieren oder gar gleich sein. In vielen Fällen können – und werden sie auch – sich durchaus widersprechen.

Als Voraussetzung jedes Sicherheitskonzepts müssen deshalb im Sinne dieser mehrseitigen Sicherheit die verschiedenartigen Anforderungen und Interessen gegeneinander abgewogen und ein für alle Betroffenen tragbarer Kompromiss gefunden werden. Wie weit dies möglich ist und wie weit solche Kompromisse von allen Betroffenen getragen werden können, wird sich oft nur unter den Randbedingungen des Einzelfalles entscheiden lassen.

4.2 Duale Sicherheit – die komplementären Sichten

Der Ansatz einer mehrseitigen Betrachtungsweise wird im Folgenden zu der Forderung verallgemeinert, in den Bedeutungsumfang des Begriffs Sicherheit grundsätzlich **zwei einander ergänzende Sichten** aufzunehmen, die **Verlässlichkeit** und die **Beherrschbarkeit** der Systeme**.** Erst gemeinsam beschreiben diese beiden Sichten den vollständigen Bedeutungsinhalt des Begriffes IT-Sicherheit. Sie sind in diesem Sinne **komplementäre Sichten** des einen Begriffs Sicherheit**.**

Um den Begriff in dieser umfassenderen Bedeutung von anderen Definitionen der Vergangenheit zu unterscheiden, die zu sehr auf bloße *technische* Sicherheit ausgerichtet waren, soll sie fortan **duale IT-Sicherheit** genannt werden. Ihre Definition lehnt sich engst - möglich an die Definitionen der DIN 44300 an.

Begriff	Definition (entsprechend DIN 44 300)
Duale Sicherheit *dual security*	Sachlage, bei der die Verlässlichkeit* und die Beherrschbarkeit* der Systeme, der mit ihnen verarbeiteten Daten (Informationen) und der für die Nutzung der Systeme benötigten Funktionen und Prozesse gewährleistet sind.
Verlässlichkeit *oder* **Sicherheit der Systeme**	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 *oder* **Sicherheit der Betroffenen, Sicherheit vor dem System**	Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden

Die Überlegungen, die zu dieser umfassenderen Definition des Begriffs IT-Sicherheit führen, sind letztlich sehr einfach. Informationstechnik ist für den Menschen ein Werkzeug, das wie jedes andere Werkzeug geschaffen und genutzt wird, um

- bisher Unmögliches zu bewältigen
  ⇨ ***Funktionalität,***
- bisher Mögliches funktionell zu verbessern
  ⇨ Qualität,
- bisher Mögliches zu vereinfachen
  ⇨ ***Effizienz, Wirtschaftlichkeit.***

Für das Werkzeug Informationstechnik sind diese Ziele nur erreichbar, wenn IT-Systeme in zweierlei Weise sicher sind:

- IT-Systeme müssen verlässlich sein und
- IT-Systeme müssen beherrschbar sein, d.h. sie dürfen ihre Benutzer (oder die von ihrer Funktion Betroffenen) weder direkt noch indirekt beeinträchtigen.

Diese beiden komplementären Forderungen nach Verlässlichkeit und Beherrschbarkeit gelten im Prinzip für *jeden* Bereich, in dem der Mensch nichtmenschliche Hilfsmittel oder Werkzeuge zur Lösung von Aufgaben einsetzt, sei es in der Verkehrstechnik, der Energietechnik, in irgendeinem Bereich der Wirtschaft, der Verwaltung, in der Medizin oder wo auch immer.

Die Forderung nach dualer Sicherheit, d.h. nach **Sicherheit des Systems + Sicherheit vor dem System**[7] gilt insbesondere dort, wo maschinelle Systeme schon vorhandene menschliche Tätigkeiten übernehmen oder ersetzen.

Sie gilt wegen der engen Verbindung zwischen Mensch und Information (*vgl.* Abschnitt *Grundbegriffe*) für die Informationstechnik in ganz besonderem Maß. Gerade dort wird sie aber am wenigsten beachtet. Das ist befremdlich! Einige Gründe für diese offensichtliche Ungereimtheit werden im Abschnitt *Erworbene Sorglosigkeit* noch näher erörtert.

4.2.1 Die technische Sicht: Verlässlichkeit – Sicherheit der Systeme

Ein System der Informationstechnik ist **verlässlich,** d.h. sicher aus technischer Sicht, wenn seine Funktionsweise den vorgegebenen Anforderungen genügt. Das heißt in anderen Worten:

> Die Betroffenen müssen sich auf die **Korrektheit und Verfügbarkeit** der Funktionen des Systems und der Ergebnisse verlassen können, die mit Hilfe dieser Funktionen gewonnen wurden.

Betroffene können Benutzer sein, im Sinne mehrseitiger Sicherheit aber auch Betreiber, Hersteller etc. Diese Definition setzt stillschweigend voraus, dass technische Sicherheit erreichbar ist, wenn alle Komponenten eines IT-Systems immer korrekt und ordnungsgemäß funktionieren, dass sie also weder fehlerhaft arbeiten noch ausfallen.

Sicherheit realer IT-Systeme

Für **reale** IT-Systeme, so wie sie in der Praxis vorkommen, wird diese Annahme so gut wie nie vollständig erfüllt sein. Wird der Mensch als Systemkomponente in die Betrachtung der Sicherheit mit einbezogen, so ist die Voraussetzung eines ordnungsmäßigen, d.h. stets den Anforderungen gemäß funktionierenden Systems vollends unrealistisch. Es ist deshalb sinnvoll, die Forderung an die Realität anzupassen und leicht abgewandelt zu verlangen:

[7] *Sicherheit **vor** dem System* ist hier gleichbedeutend mit *Sicherheit der Betroffenen*. Die Begriffe sollen synonym gebraucht werden.

- Ein reales IT-System kann aus der Sicht der Technik als sicher bezeichnet werden, wenn die Betroffenen sich auf die Korrektheit und Verfügbarkeit der Funktionen des Systems und der Ergebnisse auch dann hinreichend verlassen können, wenn Teile des Systems nicht oder nicht immer ordnungsmäßig arbeiten.

Komponenten der Verlässlichkeit

Für die Verlässlichkeit, die technische Sicht der Sicherheit von IT-Systemen, können aus dieser Forderung drei grundlegende Eigenschaften sicherer IT-Systeme abgeleitet werden.

Vertraulichkeit (confidentiality)

- keine unbefugte Einsichtnahme von Daten
- kein unbefugtes Erschließen von Informationen
- kein unbefugtes Interpretieren von Daten
- kein unbefugtes Einsehen und Erschließen von Kontexten (z.B. Protokolldaten)
- keine unbefugte Weiterverwendung, **…**

Integrität (integrity)

- keine unbefugte, unbemerkte Änderung der Daten oder Funktionen des Systems (insb. Sicherung gegen und Nachweis von Manipulationen)
- Sicherung der Authentizität
- Korrektheit der Ein- und Ausgangsdaten (externe Konsistenz)
- Korrektheit der Verarbeitung (interne Konsistenz), **…**

Verfügbarkeit (availability)

- Funktionsbereitschaft des Systems zum geforderten Zeitpunkt
- Ablauf der Prozesse im vorgegebenen Zeitrahmen
- Sicherung durch Redundanz der Daten und der Verarbeitung, Ausweichverfahren, Möglichkeiten der Restauration und des Wiederanlaufs
- Sicherung gegen *denial of service*
- Verklemmungsfreiheit, **…**

Man beachte, dass die Erläuterungen dieser drei Komponenten sich auf die drei Grundbedrohungen[8] der technischen Sicherheit (Verlässlichkeit) von IT-Systemen beziehen, wie sie z.B. in den deutschen Kriterien aufgeführt werden [BSI89], nämlich die

- unbefugte Kenntnisnahme
- unbefugte Änderung
- unbefugte Beeinträchtigung der Verfügbarkeit.

Dabei wird mit dem Wort *„unbefugt"* immer vorausgesetzt, dass für das betrachtete System bekannt ist, was ***befugt*** bedeutet, d.h., dass für dieses IT-System definiert ist, was tun soll und was nicht (→ Vollständigkeit des Anforderungskatalogs).

[8] ***Grund****bedrohung* ist *jede* unbefugte Änderung, die bemerkte ebenso wie die unbemerkte.

4.2.2 Die Sicht der Betroffenen: Sicherheit vor dem System – Beherrschbarkeit

Ein System der Informationstechnik ist **beherrschbar,** d.h. sicher aus Sicht der Betroffenen, wenn gilt:

> Die Funktionen des Systems und deren Ergebnisse können bestimmten oder bestimmbaren Veranlassern[9] (auslösenden Instanzen) **zugeordnet** werden, und zwar so, dass die Zuordnung revisionsfähig, also auch Dritten gegenüber **beweisbar** ist.

Komponenten der Beherrschbarkeit

Für die Beherrschbarkeit, also die Sicht der Betroffenen in der IT-Sicherheit, können aus dieser Forderung zwei weitere grundlegende Eigenschaften sicherer IT-Systeme abgeleitet werden.

Zurechenbarkeit (accountability)

Von jedem Prozess (jeder Funktion) und dessen Ergebnissen muss während des Ablaufs oder danach feststellbar sein, welcher Instanz er zuzurechnen ist, d.h. welche Komponente – u.a. welche Person – ihn ausgelöst oder verursacht hat. Das bedeutet im Einzelnen

- Nachweis des Auslösers oder Veranlassers einer Aktion (Person, Systemkomponente oder System)
- Nachweis des Erzeugers oder Ursprungs eines Datums (Quelle)
- Nachweis des korrekten Zusammenhangs Subjekt (Veranlasser)↔Objekt (Ergebnis, Vorgang)
- Verfügbarkeit der Protokoll- oder (Begleitdaten) einer Aktion
- Verhinderung falschen Abstreitens (*non-repudiation*)

Revisionsfähigkeit oder Rechtsverbindlichkeit (legal liability)

Von jedem Prozess (jeder Funktion) und dessen Ergebnissen muss auch Dritten gegenüber dessen Rechtsverbindlichkeit beweiskräftig nachweisbar sein. Das heißt vor allem.

- beweiskräftiger Nachweis der verantwortlichen Instanz
- beweiskräftiger Nachweis der Ordnungsmäßigkeit von Abläufen und Ergebnissen durch Dritte
- Beweisbarkeit von Ergebnissen und Vorgängen gegenüber Dritten
- Beweis der Originalität

4.3 Fundamentalkomponenten

Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Revisionsfähigkeit (oder Rechtsverbindlichkeit) spannen den semantischen Raum, d.h. das

[9] *Bestimmbare Veranlasser* darf nicht dahin missverstanden werden, als müsse zu jedem Datenverarbeitungs- oder Kommunikationsvorgang eine ganz bestimmte *natürliche* Person als Veranlasser authentisch feststellbar sein (s. Abschnitt *Fundamentalkomponenten).*

Bedeutungsfeld des Begriffs duale Sicherheit auf. Sie sind in diesem Sinne für den Begriff Sicherheit **konstituierende semantische Dimensionen**. Deshalb werden sie als **Fundamentalkomponenten dualer IT-Sicherheit** bezeichnet.

Als ***fundamental*** sind diese fünf semantischen Komponenten in dem Sinne zu verstehen, dass sie prinzipiell in einem IT-System als implementierbare – nicht notwendig bereits implementierte – Eigenschaften vorhanden sein müssen, wenn denn dieses System im dualen Sinn als sicheres System angesehen werden können soll.

Fundamental heißen diese Komponenten auch, weil sie das Bedeutungsfeld, die Semantik, des Begriffs duale Sicherheit *umfassend* beschreiben. Daraus folgt unmittelbar, dass in jedes Sicherheitskonzept und jede Evaluation (Audit) alle semantischen Dimensionen einzubeziehen sind.

Fundamental sind sie auch in dem Sinne, dass sie als konstituierende Komponenten *notwendige Bestandteile* der dualen Sicherheit eines IT-Systems sind; keine von ihnen darf vernachlässigt oder gar übergangen werden. Wird eine vernachlässigt, muss dies explizit begründet werden.

Das bedeutet nicht, dass jede von ihnen in allen Anwendungen gleiches Gewicht hat. Denn je nach den Anforderungen, die an die Sicherheit eines IT-Systems gestellt werden, kann den Fundamentalkomponenten in verschiedenen Anwendungen unterschiedliches Gewicht zugemessen werden (vgl. Abschn. 4.6).

4.4 Ziele dualer IT-Sicherheit

Aufgabe eines sicheren Systems der Informationstechnik ist es,

Vertraulichkeit, Integrität und Verfügbarkeit von Geräten, Daten, Programmen und Personen zu schaffen und zu erhalten

Zurechenbarkeit aller Vorgänge und Ergebnisse zu definierbaren Veranlassern zu gewährleisten und die

Revisionsfähigkeit (Rechtsverbindlichkeit), d.h. die Beweisbarkeit von Vorgängen und Ergebnissen gegenüber Dritten, zu ermöglichen.

Semantische Dimensionen sicherer IT-Systeme

Als Eigenschaften sicherer IT-Systeme beschreiben die semantischen Dimensionen gleichzeitig die **Aufgaben** eines jeden IT-Sicherheitskonzepts und sind damit die übergreifenden **Ziele** dualer IT-Sicherheit.

Verschiedene Ausprägungen dualer Sicherheit ergeben sich einfach dadurch, dass jede der fünf Komponenten in einem semantischen Raum für verschiedene Anwendungen verschieden gewichtet werden kann. Aus der Zusammenschau der verschieden gewichteten Komponenten ergibt sich die Auslegung des Begriffs Sicherheit für jeden gegebenen Anwendungsfall.

Fundamental heißt ferner, dass jede der *Komponenten für sich betrachtet und untersucht werden kann.* Es heißt aber nicht, dass die Fundamentalkomponenten voneinander unabhängig sind. Im Gegenteil, in vielen, wenn nicht gar in den meisten Anwendungsfällen sind sie eng ineinander verwoben und hängen wechselseitig voneinander ab.

Wie, in welcher Form, durch welche Maßnahmen oder Mechanismen die Fundamentalkomponenten in realen IT-Systemen in der Praxis tatsächlich verwirklicht werden, das hängt entscheidend von den Anforderungen ab, die an die Sicherheit einer Anwendung von außen her gestellt werden, aber auch von den technischen – und wirtschaftlichen – Möglichkeiten, sie in der Praxis umzusetzen.

Ob beispielsweise bei der Zurechenbarkeit eine einzelne natürliche Person als auslösende Instanz eines bestimmten Prozesses oder Ergebnisses unter ihrer persönlichen Authentizität festzuhalten ist oder unter einem Pseudonym oder gar anonym, kann erst aus den Anforderungen an den Anwendungsfall abgeleitet werden. Vorgänge, bei denen im klassischen Ablauf, d.h. bei Kommunikation und Informationsverarbeitung ohne Hilfe von Computern, die Teilnehmer anonym bleiben oder unter einem Pseudonym handeln (Beispiel: Einkäufe mit Bargeld), müssen auch mit moderner Informationstechnik in vergleichbarer Form abgewickelt werden können. Damit ein IT-System jedoch im Sinne dualer Sicherheit als sicher angesehen werden kann, muss es bei anonym oder pseudonym abgewickelten Vorgängen dennoch imstande sein, die Forderungen nach Zurechenbarkeit mit vergleichbarer Vertrauenswürdigkeit zu erfüllen wie bei klassischem Vorgehen.

Entsprechendes gilt für alle übrigen Fundamentalkomponenten. Auch sie sind Zielvorgaben und müssen nur verwirklich**bar** sein, wenn dies gefordert wird. Die Forderungen wiederum müssen den Anwendungen angepasst sein. Diese Anpassung ist immer eine Aufgabe, die für die Konzeption der Sicherheit eines IT-Systems von außen vorgegeben wird und nicht aus dem System selbst oder aus seinem Verhalten abgeleitet werden kann. Welche Forderungen an die fünf Fundamentalkomponenten im einzelnen Anwendungsfall gestellt werden müssen, ist Sache eines passenden Anforderungskatalogs (→ Sicherheitsziele).

Ein einfaches Beispiel dazu: Die Anforderung, die drei Farben Rot, Gelb und Grün als Daten (Ergebnisse) einer Ampelsteuerung vertraulich zu halten, lässt sich schwerlich als für diese Aufgabe geeignete Sicherheitsanforderung einordnen.

4.5 Semantischer Raum (Bedeutungsfeld)

Fundamental heißt aber nicht, dass mit den fünf beschriebenen Komponenten das Bedeutungsfeld des

Begriffes Sicherheit ein für allemal erschöpfend beschrieben wäre. Je nachdem, in welchem Zusammenhang, der Begriff Sicherheit gebraucht wird, reicht seine Bedeutung in die Bedeutungsfelder einer ganzen Reihe anderer Begriffe hinein. Dazu gehören Begriffe wie

Plausibilität
Robustheit
Zuverlässigkeit
Vertrauenswürdigkeit
Wartbarkeit
Funktionalität
Beobachtbarkeit
Steuerbarkeit
...

Diese und weitere Aspekte können Bestandteil des Bedeutungsfeldes des Begriffs *IT-Sicherheit* sein, wenn denn dieser Begriff umfassend und allgemeingültig interpretiert werden soll. Offen bleibt dabei, ob und wann eine dieser Komponenten zu gegebener Zeit und in bestimmtem Zusammenhang sinnvoll als *konstitutiv*, also als *Fundamentalkomponente* (semantische Dimension) angesehen werden soll.[10]

Der semantische Raum des Begriffs Sicherheit: kann damit je nach dem Kontext, in dem er gebraucht wird, zu einem vieldimensionalen Gebilde werden, dessen verschiedene Teilaspekte (Dimensionen) auf vielfältige und komplexe Weise voneinander abhängen.

Für die Praxis heißt das: die erste Aufgabe bei der Erstellung eines Sicherheitskonzepts ist, zunächst festzustellen oder festzulegen, wie denn der Begriff Sicherheit in dem Anwendungsbereich überhaupt zu verstehen ist, für den das Konzept aufgestellt werden soll. Soll das Schwergewicht auf der Vertraulichkeit liegen, auf der Verfügbarkeit oder auf der Integrität? Welche Rolle spielen in dem zu untersuchenden Anwendungsfall Robustheit, Plausibilität und andere der genannten ergänzenden Komponenten? Sind sie zusätzlich zu den Fundamentalkomponenten zu beachten oder kommt ihnen womöglich eine Hauptrolle zu? In welcher Weise hängen die verschiedenen Aspekte voneinander ab?

Erst wenn für den Anwendungsbereich – oder für den einzelnen Anwendungsfall – geklärt ist, wie der Begriff Sicherheit zu verstehen und wie seine Komponenten zu gewichten sind, kann man sich mit einiger Aussicht auf Erfolg daran machen, für ein Unternehmen, für eine Behörde, für eine bestimmte Aufgabe ein sinnvolles Sicherheitskonzept zu erstellen.

[10] Beispielsweise ist die Diskussion darüber, ob ***Authentizität*** eine *semantische Dimension* des Begriffs Sicherheit (= semantische Komponente = Ebene 2 des Modells) ist oder aber eine Grundfunktion (= notwendige Eigenschaft sicherer IT-Systeme = Ebene 3), noch immer offen.

4.6 Klassische Schwerpunkte der IT-Sicherheit

Man braucht gar nicht auf neuere Auslegungen für spezielle Anwendungsbereiche zurückzugreifen; auch in den klassischen Interpretationen wird der Schwerpunkt des Bedeutungsfeldes von *Sicherheit* auf ganz verschiedene Teilaspekte geschoben, je nachdem welchen Anwendungsbereich man Auge hat.

- Für Anwendungen in den Bereichen Militär oder Politik wurde die Forderung nach sicherer Informationsverarbeitung vielfach gleichgesetzt mit der Forderung, dass unberechtigte Dritte Informationen (Daten) weder zur Kenntnis nehmen noch erschließen, d.h. interpretieren oder verstehen können. Der Schwerpunkt der Sicherheit lag – und liegt vielfach noch immer – seit den Zeiten Cäsars (→ „Cäsar-Chiffre") in diesem Anwendungsbereich auf dem Teil des Bedeutungsfeldes, der gemeinhin mit *Vertraulichkeit* bezeichnet wird. Das bedeutet kurz
  - kein Einsehen von Daten oder Erschließen von Information
  - immer kontrollierter Zugriff auf Daten und Funktionen
- In der Verwaltung, im Bank- und Rechtswesen lag und heißt sichere Verarbeitung in erster Linie *Integrität* von Systemen, Programmen und Daten. Die Verarbeitung von Daten ebenso wie die Daten selbst müssen vor allen Arten von Beeinträchtigungen, insbesondere vor unberechtigten, unbemerkte Veränderungen gesichert sein (englisch: *tamper free*), damit deren Rechtsverbindlichkeit gewährleistet werden kann. Kurz zusammengefasst:
  - keine unbemerkte Veränderung der Daten
  - keine unbemerkten Veränderungen an Funktionen
  - beweisbare Zuordnung von Subjekten und Objekten
  - Authentizität der Daten und Funktionen
- Für die Steuerung und Regelung von Prozessen in der Echtzeitdatenverarbeitung (*real time processing*) ist wichtiger als jeder andere Aspekt der Sicherheit, dass eine geforderte Funktion zum richtigen Zeitpunkt und in Übereinstimmung mit den zeitlichen Randbedingungen (Zeitrahmen) des zu steuernden Prozesses ausgeführt wird. Deshalb werden in der Echtzeitdatenverarbeitung die Begriffe *Verfügbarkeit* und Sicherheit häufig als beinahe synonym angesehen (Gefahr des *denial of service*.).

Soll der Begriff des sicheren IT-Systems möglichst allgemeingültig gefaßt werden, soll seine Bedeutung nicht vorschnell eingeschränkt werden auf den Blickwinkel irgendeines speziellen Anwendungsbereichs, dann muss jede der fünf Fundamentalkomponenten in die Auslegung des Begriffs Sicherheit mit einbezogen werden.

5. Ein semantisches Modell der IT-Sicherheit[11]

Bei der Vielzahl der mit dem Thema „Sicherheit“ zusammenhängenden Begriffe, bei der Vielfalt der mit ihnen verbundenen Beziehungen und Abhängigkeiten empfiehlt es sich, die Begriffe, ihre Bedeutungen (ihre Semantik) und die zwischen ihnen bestehenden Strukturen in eine überschaubare Ordnung zu bringen. Verschiedene Modellstrukturen sind denkbar. Zwei der häufig verwendeten Ansätze für solch ein semantisches Modell sind das Schalen- und das Schichtenmodell.

Schalenmodell

Anordnung gleichartiger (gleichwertiger Begriffe in einem Kreisring → Anordnung der Ringe konzentrisch ineinander

Schichtenmodel

Anordnung gleichartiger (gleichwertiger) Begriffe in einer Ebene → Stapelung der Schichten übereinander

Semantisches Schichtenmodell der Begriffe

IT-Sicherheit								
①	**Sichten**							
Verlässlichkeit Sicherheit *des* Systems				**Beherrschbarkeit** Sicherheit der Betroffenen*)				
②	**Semantische Dimensionen** oder **Ziele**							
Vertraulichkeit	Integrität	Verfügbarkeit	Zurechenbarkeit	Rechtsverbindlichkeit, Revisionsfähigkeit	...			
③	**Grundfunktionen**							
Authentisierung	Rechteverwaltung	Rechtekontrolle	Protokollierung	Fehlerkompensation	Überwachung	...		
④	**Mechanismen**							
Personenkontrollen	Trennung der Befugnisse	Kryptographie	Biometrie	elektronische Signaturen	Zugriffskontrolle	Redundanz	organisatorische Maßnahmen und Verfahren	...

*) Auch ***Sicherheit vor dem System***

it-security								
①	**views** or **facets**							
assurance security of systems				**controllability** security of users**)				
②	**semantic dimensions** or **targets**							
confidentiality	integrity	availability	accountability	liability, auditability	...			
③	**basic functions**							
authentication	administration of rights	control of rights	protocolling	error compensation	supervision	...		
④	**mechanisms**							
control of persons	separation of rights	cryptography	biometric	electronic signatures	access control	redundancy	organizational measures and procedures	...

) Also ***security against the system*

11) ***Semantik*** = Lehre von der Bedeutung der Zeichen und Wörter

Für das hier beschriebene hierarchisches Schichten- oder Ebenenmodell gelten zwei grundlegende Regeln:

1. Das Wort Sicherheit wird als der **übergeordnete Begriff** verwendet.
2. **Alle** Begriffe, die zu Sicherheit gehören, werden in dieses Modell eingeordnet.

Beides wurde schon in den deutschen IT-Sicherheitskriterien [BSI89] mit Erfolg begonnen

5.1 Anmerkungen zum semantischen Schichtenmodell

Bezeichnungen

Für die Schichten (Ebenen) sind verschiedene Bezeichnungen gebräuchlich, die wahlweise benutzt werden können, solange keine Verwechslungen zu befürchten sind.

① **Sichten**, Aspekte, Seiten, …
(engl. *views, aspects,…*)

② **semantische Dimensionen** oder Fundamentalkomponenten, Sicherheitsziele, Facetten, …
(engl. *facets, targets, components*, …)

③ **Grundfunktionen**, Basisfunktionen, Grundeigenschaften, Attribute, …
(engl. *generic headings, basic functions, characteristics, security components*)

④ **Maßnahmen**, Mechanismen, Verfahren, …
(engl. *mechanisms, methods*)

Offene Struktur des Modells

Das Modell ist als „offene Struktur" zu verstehen. Das heißt:

- Die ***Anzahl der Elemente*** ist keine „Naturkonstante".
- Bestimmte Elemente des Modells können als ***fundamental*** bezeichnet werden, wenn sie für den Begriff IT-Sicherheit konstituierend, unverzichtbar sind (vgl. Beispiel 1).
- Zwischen den Elementen verschiedener Schichten besteht im Allgemeinen eine ***m:n–Relation*** (vgl. Beispiel 2). Das heißt, *m* Elemente der einen Schicht können mit *n* Elementen einer anderen in Beziehungen stehen oder voneinander abhängig sein.

Insbesondere darf das Modell ja nicht so missverstanden werden, als gehörten die ersten drei semantischen Dimensionen (Fundamentalkomponenten, Ziele) ausschließlich zur Verlässlichkeit und die beiden übrigen zur Beherrschbarkeit. Auch zwischen den Ebenen ② und ③ gilt die *m:n*-Relation, sozusagen als „Über-Kreuz"-Beziehung. Drei Beispiele veranschaulichen die Aussagen über die Modellstruktur.

Beispiel 1

In der Ebene ② (semantische Dimensionen, Sicherheitsziele, …) müssen die fünf Fundamentalkomponenten Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Rechtsverbindlichkeit ggf. durch weitere ergänzt werden, sobald diese für bestimmte Anwendungen als „fundamentale" Komponenten angesehen werden müssen. Ein typischer Kandidat für solch eine Ergänzung auf der Ebene ② kann z.B. die Komponente ***Robustheit*** sein. Dazu gehören u.A.

- Unempfindlichkeit gegen externe Einflüsse (Umwelt, physikalische Einwirkungen, Kontext, …)
- Toleranz gegen Bedienungs- und Eingabefehler
- Toleranz gegen fehlerhafte Eingangsdaten und Abweichungen
- numerische Stabilität
- Stabilität trotz technischer Fehler (Ausfälle, Störungen, …)

Beispiel 2

Ein Beispiel für die ***m:n-Beziehung*** zwischen Elementen zweier verschiedener Ebenen ist der Zusammenhang zwischen den Sicherheitszielen (Ebene ②) und Elementen darunter liegender Schichten, z.B. den kennzeichnenden Eigenschaften (Grundfunktionen auf der Ebene ③).

- Ist Vertraulichkeit einer Übertragung gefordert, so genügt es nicht, die Authentizität von Sender, Empfänger und Nachricht sicherzustellen („Sind die Veranlasser und die Nachricht wirklich die, die sie zu sein vorgeben?") Um sicher zu sein, müssen auch die Fragen beantwortet werden
- „Wer soll wozu befugt sein?" und
- „Ist der Veranlasser der gerade laufenden Aktion tatsächlich dazu befugt?"

Neben der Authentisierung werden Rechtevergabe und Rechtekontrolle als kennzeichnende Eigenschaften (Grundfunktionen, Ebene ③) für die Vertraulichkeit bei dieser Aufgabe benötigt.

Beispiel 3

In der Ebene ③ (Grundfunktionen, Attribute, …) ist eine weitere Grundeigenschaft zu bedenken, die in allen *menschlichen* Erwägungen zur Verlässlichkeit – im Sinne von Vertrauenswürdigkeit – von Ergebnissen, wie auch von Abläufen, eine beinahe ausschlaggebende Rolle spielt: die ***Plausibilität***., Bislang stoßen alle Versuche noch auf ganz erhebliche Schwierigkeiten, diese dem Menschen für seine Entscheidungen quasi unmittelbar zugängliche Funktion sinnvoll auf maschinelle Systeme abzubilden.

6. Die Beziehung Mensch ⇔ Maschine als Besonderheit

Datenverarbeitung und Kommunikation sind ursprüngliche Tätigkeiten des Menschen, ja sie sind für ihn geradezu kennzeichnend. Das bewusste Aufnehmen, Aufbewahren, Verändern, Weitergeben und Nutzen von Daten, zusammenfassend oft Informationsverarbeitung genannt, ist wie kaum etwas Anderes charakteristisch für das Mensch-Sein.

Es verwundert nicht, dass der Mensch auch in diesem Bereich schon in einem sehr frühen Entwicklungsstadium begonnen hat, Tätigkeiten Schritt für Schritt zu „mechanisieren", also ganz oder teilweise auf Maschinen zu übertragen. In diesem Bereich hat er das für Tätigkeiten und Vorgänge getan, die von Haus aus eigentlich darauf zugeschnitten sind, vom Menschen selbst ausgeführt zu werden.

Der Begriff *mechanisieren* ist bei dieser Übertragung sehr allgemein zu verstehen: Der Mensch macht sich in der Informationsverarbeitung, so wie in anderen Bereichen auch, schon seit Jahrtausenden maschinelle, nicht-menschliche Hilfsmittel (Werkzeuge) zunutze, um mit diesen Werkzeugen und Verfahren seine eigene Leistungsfähigkeit zu steigern.

Die Ziele solcher Übergänge Mensch→Maschine sind vielfältig: Vereinfachung, Verbesserung, Beschleunigung, Erleichterung vertrauter Tätigkeiten und Vorgänge, aber auch Entdeckung oder Erschließung neuer, bisher nicht beherrschbarer oder nicht einmal bekannter Funktionen.

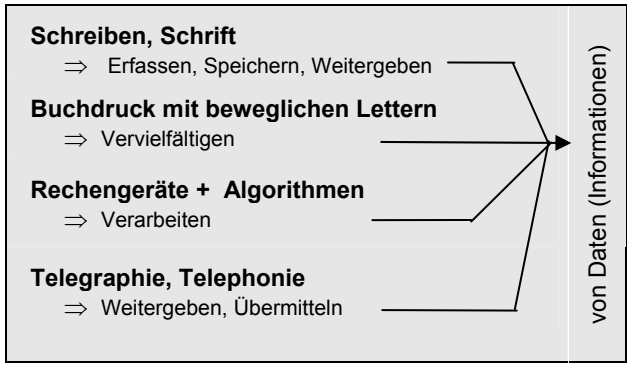
Wirkung und Folgen dieser Übergänge Mensch→ Maschine in der Kommunikation und Informationsverarbeitung waren aber nicht auf Ablauf und Eigenschaften der Vorgänge selbst beschränkt. Sie wirkten sich vielmehr auf Beziehungen zu anderen Bereichen aus und damit auf die Gesellschaft. Diese Auswirkungen waren fast immer so stark, dass grundsätzliche Strukturen und eingeübte Verhaltensweisen der Gesellschaft ins Wanken gerieten. Fünf Stufen in diesen Übergängen sind besonders bemerkenswert:

1. die Entwicklung und Nutzung der ***Schrift***
2. die Erfindung des ***Buchdrucks*** mit beweglichen Lettern
3. die Erfindung und Einführung der ***Telekommunikation*** (Telegraphie und Telephonie)
4. die ***Automatisierung*** von informationsverarbeitenden Prozessen (algorithmische Darstellung und Mechanisierung von Abläufen)
5. die Erfindung des speicherprogrammierten ***Rechenautomaten***

Der Computer ist erst das allerletzte Glied in der Kette von Übergängen, bei denen der Mensch Schritt für Schritt Tätigkeiten der Datenverarbeitung und Kommunikation ganz oder teilweise auf Maschinen übertragen hat. Die Auswirkungen dieses letzten Schrittes auf die Gesellschaft übertreffen allerdings alles Vorangegangene.

6.1 Stufen maschineller Informationsverarbeitung

Die vier ersten Stufen dieser Übergänge Mensch → Maschine in der Vergangenheit sind bekannt.



Das Wort *Stufen* möge hier nicht im Sinne eines zeitlichen Nacheinander missverstanden werden; denn manche dieser Übergänge liefen über Jahrzehnte, Jahrhunderte nebeneinander her. Automatisierung und algorithmische Beschreibung von Prozessen. Beschreibungen von Automaten finden sich zum Beispiel schon bei *Heron von Alexandria* (um 62 v. Chr.), eine Darstellung von Algorithmen für logische Schlussfolgerungen in Form graphischer Verfahren schon bei Ramón Lull (um 1275 in Spanien).

Was für Werkzeuge in anderen Lebensbereichen galt, war erst recht für die Datenverarbeitung und Kommunikation gefordert:

- die Werkzeuge mussten **verlässlich** sein und
- sie durften ihren Benutzer und dessen Umwelt **nicht beeinträchtigen**.

Wie einschneidend sich aber jeder dieser vier Übergänge direkt und indirekt auf das Verhalten der Menschen auswirkte, wie die dadurch Möglichkeiten der Informationsverarbeitung und Kommunikation erweitert, verändert oder auch völlig neu geschaffen und damit die gesamte Gesellschaft von Grund auf veränderte wurden, das macht man sich viel zu selten und viel zu wenig bewusst.

Denn mit jeder der Stufen änderte sich zwangsläufig mit Art und Weise der Kommunikation auch das Verhalten des Menschen und damit die Struktur der Gesellschaft. Wenn der Mensch ***das*** durch Sprache, Bewusstsein und Kommunikation bestimmte Wesen ist, dann musste jede Veränderung dieser Komponenten ungeheure Auswirkungen auf ihn haben – und hatte sie auch.

Der schreibende Steuereinnehmer der Sumerer hatte plötzlich ein Beweismittel „in der Hand", im Buchstabensinne des Wortes.

Die übersetzte und tausendfach vervielfältigte Bibel bestätigte Luthers Thesen in für jedermann nachlesbarer Weise. Die neue Lehre breitete sich wie ein Waldbrand aus, flächendeckend und mit bis dahin ungekannter Geschwindigkeit. Jan Hus (1370–1415) oder Girolamo Savonarola (1452–98) hatten von solchen Auswirkungen nicht einmal träumen können, weil für sie der Druck mit beweglichen Lettern noch nicht verfügbar war. Die Urheber der anstößigen neuen Lehren wurden „warm entsorgt", und damit war ihrer „Irr"-Lehre ein rasches Ende bereitet.

Bei Luther war den Herrschenden dieser Aus–Weg verbaut. Viel zu Viele hatten seine Ideen bereits gelesen und für gut gehalten – aus welchen Beweggründen auch immer –, als dass man ihn noch hätte einfach so verschwinden lassen können. Mehr noch: der Wunsch selbst lesen, sich selbst „informieren" zu können, verlangte nach „Leseschulen", nach Lehren, die die neue Kunst weitergeben, nach Stätten in den man den Lesstoff ungestört, ungehindert, ungefiltert (!) aufbewahren und wiederfinden konnte. Gründung von Universitäten, Einführung des römischen *„imprimatur",* die positiven wie die negativen Folgen von Gutenbergs Erfindung sind Legion!.

In vielen Fällen wogen die indirekten Auswirkungen neuartiger maschineller Informationsverarbeitung weit schwerer noch als die direkten. Die Einführung der Automatisierung in die Fertigung, so z.B. die Erfindung und der Einsatz programmgesteuerter Webstühle an der Wende vom 18. zum 19. Jahrhundert *(J.-M. Jacquard*, 1752–1834), hatte soziale Umwälzungen unvorhergesehenen Umfangs zur Folge, bis hin zur Zerstörung der neuen Werkzeuge und Manufakturen und die Beseitigung ihrer Besitzer durch die aufgebrachten, verarmten Weber (Irland, Schweiz, Frankreich, Schlesien)..

Drei grundlegende Aussagen lassen sich für die ersten vier Stufen des Übergangs Mensch → Maschine in der Informationstechnik festhalten:

1. Alle Schritte, bei denen der Mensch informationsverarbeitende Tätigkeiten maschinellen Hilfen („*maschinell"* im weitesten Sinne) übertrug, wirkten sich nicht nur auf die Art und Weise des Umgangs mit Daten (Informationen) aus, sondern sie wirkten direkt und indirekt ***gesellschaftsverändernd.***
2. Quantität und Qualität der Auswirkungen und Veränderungen waren zwar nur zum Teil *vorhersehbar*: Die neuen Werkzeuge selbst aber, ihr Aufbau und ihre Wirkungsweise, waren jedoch für den einzelnen noch weitgehend ***durchschaubar und nachvollziehbar***, zumindest im Grundsätzlichen.
3. Damit waren die Betroffenen – die Benutzer, die Erfinder und Erzeuger der neuen Techniken, die Gesetzgeber, die Verantwortlichen – in der Lage, sich selbst und die Gesellschaft den veränderten Techniken der Informationsverarbeitung und Kommunikation durch adäquate Änderung der ***Rechts- und Gesellschaftsstrukturen anzupassen.***

Denn soviel ist ohne großes Nachforschen erkennbar: zu keiner Zeit gab es zwischen Menschen uneingeschränkte Verfügbarkeit oder völlig freizügigen Austausch von Daten. Wer wann was worüber wissen sollte oder konnte (Geheimwissen der Priester und Medizinmänner, Berufs-, Zunft- und Standesgeheimnisse, …), wer welche Kenntnisse an wen weitergeben durfte (Beicht- und Bankgeheimnis, Arztgeheimnis, geheime Nachrichten in Politik und Militärwesen, Briefgeheimnis, …), das war geregelt – meist sogar streng geregelt – durch Gesetzgebung, Verordnungen, Rechtsprechung, durch Verhaltensnormen und Gewohnheiten und nicht zuletzt durch passende technische und organisatorische Hilfsmittel.

Nachrichten in versiegelte Umschläge zu stecken oder Boten umzubringen, nachdem sie ihre Nachricht überbracht hatten, sind zwei Beispiele für solche technischen oder organisatorischen „Regelungen" mit gleicher Wirkung: die Botschaft blieb vertraulich, – wenn auch aus Sicht der Boten die Sicherheitsmaßnahmen wohl sehr unterschiedlich zu bewerten waren..

All wohlerwogenen Maßnahmen, Regelungen und Organisationsformen für einen sicheren Umgang mit Daten (Informationen) wurden in den vergangenen Jahrhunderten kontinuierlich fortgeschrieben und neuen Entwicklungen angepasst: versiegelte Briefe und kryptographische Verfahren mit dem Aufkommen der Schrift, päpstliches Imprimatur nach der Erfindung des Buchdrucks, gesetzliches Verbot des willkürlichen Abhörens nach der Erfindung von Telegraf und Telefon, usw. usw.

6.2 Der Übergang zum speicherprogrammierten digitalen Rechenautomaten

Die fünfte und – einstweilen – letzte Stufe der Übergänge Mensch→Maschine in der Informationstechnik ist die Erfindung des **speicherprogrammierten, digitalen Rechenautomaten**, des ***Computers,*** durch Konrad Zuse in den Jahren 1936–41.

Mit diesem letzten Schritt hin zur *programmgesteuerten automatisierten digitalen Datenverarbeitung* werden für die Verlässlichkeit und Beherrschbarkeit der Informations- und Kommunikationstechnik Fragen aufgeworfen, wie sie in dieser Art noch bei keinem der vorhergehenden Übergänge Mensch → Maschine aufgetreten waren. Einige dieser Besonderheiten sind in den vorhergehenden Abschnitten besprochen worden.

Digitaler Rechenautomat (Computer)
⇒ Daten (Informationen) selbsttätig (automatisch) verarbeiten

Die 5. Stufe des Übergangs Mensch → Maschine

Noch ein Hinweis: Sicherheit in ihren verschiedenen Formen war in der Vergangenheit ein Thema, das in der Datenverarbeitung häufig genug erst in zweiter Linie, sehr oft – zu oft? – nur ganz am Rande angeschnitten wurde. Leistungsfähigkeit, im Wesentlichen gleichgesetzt mit Rechengeschwindigkeit, Speicherkapazität und Funktionsumfang, waren über Jahrzehntee hinweg die Ziele, auf das hin Datenverarbeitungssysteme nicht nur entworfen, konstruiert und betrieben, sondern auch die Richtwerte, nach denen sie in aller Regel analysiert und bewertet wurden.

Wer vor einer unbegrenzten und unkontrollierten Nutzung automatisierter Datenverarbeitung warnte, wer auf die Gefahren uneingeschränkter maschineller Informationsverarbeitung für die menschliche Gesellschaft hinwies, gehörte vor nicht all zu langer Zeit – oder noch immer? – zu einer unbedeutenden Minderheit von Informatikern, die nicht selten als Pessimisten, als Bilderstürmer oder praxisferne Phantasten angesehen wurden.

Es bleibt noch übrig, eine Antwort zu finden auf die Frage, warum gerade in der Informationstechnik Sicherheit noch immer so nachlässig, viel zu nachlässig behandelt wird. Denn andere Disziplinen kennen diese Nachlässigkeit nicht. Man denke nur an Beispiele wie Verkehrstechnik, Kernenergie oder Biotechnik, insbesondere die Gentechnik.

7. Erworbene Sorglosigkeit – eine Fehleinschätzung

Aus Überlegungen zur Sicherheit der Informationstechnik wie denen der vorhergehenden Abschnitte wird zuweilen der Schluß gezogen, moderne Informationstechnik sei von Grund auf Teufelswerk und müsse deshalb weitestgehend wieder abgeschafft werden, wenn man unsere Gesellschaft in ihrer jetzigen Form nicht nachhaltig schädigen wolle. Nichts unsinniger als das! So wie unsere Gesellschaft gegenwärtig aufgebaut ist mit allem, was zu ihr gehört, ihrem sozialen Gefüge, ihrer Wirtschaft, ihrer Wissenschaft und nicht zuletzt ihrer Kultur, kann sie ohne moderne Informationstechnik nicht mehr überleben.

Dann aber dürfen Schutz und Sicherheit nicht mehr nur Randerscheinungen sein, sondern müssen ins Zentrum der gesamten Entwicklung moderner Informationstechnik gerückt werden. Dann darf Sicherheit nicht mehr nur als eine Zusatzforderung gesehen werden, die in einigen abgrenzbaren und als besonders gefährdet angesehen Anwendungsbereichen ausdrücklich verlangt werden muss, sondern sie muss Konstruktionsprinzip sein, das gleichwertig neben der Forderung nach Leistungsfähigkeit steht. Dann tritt eine alte Frage in einem neuen Gewand auf und wird zur Grundsatzfrage. Es darf dann nicht mehr heißen:

> **Ist es möglich,** zur Lösung eines bestimmten, wohldefinierten Problems der Informations- und Kommunikationstechnik ein bestimmtes maschinelles System einzusetzen oder nicht, sondern:
>
> **Ist es zulässig?**

Zulässig heißt hier selbstverständlich „zulässig im Hinblick auf die Sicherheit", auf *duale* Sicherheit.

Die Antwort auf diese Grundsatzfrage darf auch nicht destruktiv verteufelnd, sondern muss konstruktiv gegeben werden:

> Man setze Werkzeuge der Informationstechnik überall dort ein, wo ihre Stärken zum Tragen kommen und ihre Schwächen sich umgehen oder vermeiden lassen.

Bedenklich ist der Übergang überall dort, wo subjektive und damit von „menschlicher" Interpretation abhängige Bewertungen und Entscheidungen in die Lösung einer Aufgabe eingehen.

Stark sind Automaten überall da, wo gleichartige Prozesse auf große Datenmengen wiederholt angewendet werden müssen (*Verarbeitung von Massendaten*), und die Interpretation der Daten durch Algorithmen vollständig oder zumindest hinreichend genau wiedergegeben werden kann (vgl. die Abschnitte *Interpretation* und *Kontext*). Bei solchen Aufgaben können Computer durch ein Höchstmaß an Verlässlichkeit glänzen, das von Menschen auch nicht annähernd erreicht wird.

Oder um es vermenschlicht auszudrücken: Weil kein Mensch imstande ist, in solch kurzer Zeit solch riesige Zeichenmengen durchzuarbeiten und dabei so wenige Fehler zu machen, wird dem Computer ein besonders hohes Maß an Zuverlässigkeit zugemessen. Dieser Eindruck wird noch verstärkt durch

- die quantitative und qualitative Verbesserung der Übertragung als Voraussetzung für eine Verbesserung des Daten- (Informations)-Flusses; damit
- die Überwindung von Raum – und Zeit – durch moderne Telekommunikation;
- Archivierung größter Datenbestände auf kleinstem Raum, verbunden mit der
- Verbesserung des Wiederauffindens von Daten (Retrieval) mit Hilfe leistungsfähiger Interpretationstechniken und -systeme und damit wiederum
- die Möglichkeit, qualitativ und quantitativ andere, verbesserte Verknüpfungen zwischen den Daten aufzuspüren oder herzustellen.

7.1 Fehleinschätzung der „Zuverlässigkeit“ des Computers

Gerade diese spezielle Form der Verlässlichkeit, die wieder und wieder zitierte „Zuverlässigkeit des Computers”, ist es aber, die den Menschen zu einer unzulässigen Verallgemeinerung und zu einem falschen Glauben an die „Objektivität” und Vertrauenswürdigkeit automatisierter Datenverarbeitung verführt. Nur wenige Menschen, auch unter den Mitarbeitern in der Datenverarbeitung, erkennen und bedenken, dass Daten in Maschinen völlig anderes verarbeitet werden als durch Menschen und dass aus dieser Andersartigkeit sehr wohl neue Gefahren für den Einzelnen und die Gesellschaft entstehen, ja schon entstanden sind. Hier verstärken sich die im Abschnitt *Grundbegriffe* geschilderten Probleme gegenseitig, das Fehlen der unmittelbaren Wahrnehmung, die Andersartigkeit der Interpretation und die veränderten oder fehlenden Kontexte in automatisierten IT-Systemen..

Diese ungute Situation wird durch zwei Phänomene noch verstärkt, durch Fehleinschätzung und erworbene Sorglosigkeit:

Fehleinschätzung

Menschen schätzen Gefahren (und damit Risiken) um so geringer ein, je weniger sie deren Auswirkungen direkt wahrnehmen oder erkennen können.

Erworbene Sorglosigkeit

Für Menschen in positiven oder als positiv empfundenen Zuständen sinken Motivation und Fähigkeit, Gefahren und negative Folgen ihres Handelns zu erkennen. In einem Zustand der **erworbenen Sorglosigkeit**[12] werden negative Auswirkungen nicht mehr sachlich in das Handeln, mehr noch: in die Entscheidungen als Voraussetzungen allen Handelns mit einbezogen.

Diese Fehleinschätzungen werden durch eine **Zeitabhängigkeit** noch verstärkt: kurzfristige Folgen werden in ihrer Bedeutung oft überschätzt, langfristige fast immer unterbewertet.

Für die Einführung der Informationstechnik, d.h. für den Ersatz oder die Ergänzung menschlicher informationsverarbeitender Tätigkeiten durch Maschinen (Automaten) gelten beide Sätze in besonderem Maße. Sie gelten insbesondere in einer Zeit, in der informationsverarbeitende Tätigkeiten mit Hilfe von Automaten nicht mehr einer „geschlossenen Gesellschaft” von Spezialisten vorbehalten, sondern Handwerkszeug für jedermann geworden sind.

7.2 Fehleinschätzung durch fehlende direkte Wahrnehmung

Die Aussage über die Fehleinschätzung stimmt offensichtlich.

- Der Mensch hat kein Sinnesorgan, mit dem er die Gefahren unmittelbar erkennen könnte, die hinter einer unkontrolliert oder auch nur unbedacht eingesetzten automatisierten Datenverarbeitung lauern können.

Er hat nicht einmal ein Sinnesorgan, mit dem er die Objekte *direkt* wahrnehmen kann, die in modernen IT-Systemen verarbeitet oder übertragen werden (vgl. Abschnitt *Grundbegriffe*).

Es ist ähnlich wie beim Verkehr. Der Mensch empfindet zwar Beschleunigung als Kraft, die auf seinen Körper einwirkt. Er hat aber kein Organ, das Geschwindigkeit unmittelbar wahrnimmt, es sei denn, sie muss vom eigenen Körper erzeugt und aufrecht erhalten werden (Gehen, Laufen, Schwimmen, Rad fahren). Der Blick aus dem Wagenfenster hilft nur sehr bedingt und in engen Grenzen. Solange keine scharfen Kurven oder kräftiges Bremsen uns direkt die Auswirkungen zu schnellen Fahrens spüren lassen als Fliehkraft oder Beschleunigung, müssen wir mühsam die Folgen hoher Geschwindigkeit in Gedanken erschließen und – hoffentlich – unsere Fahrweise danach richten.

Nicht anders in der Datenverarbeitung. Der missbrauchte Rhein stinkt, missbrauchte Daten oder Systeme nicht. Wer macht sich wirklich klar, welche Folgen der Ersatz von Menschen durch Automaten in der Informationsverarbeitung letztlich hat? Wer bedenkt wirklich, welche Konsequenzen es hat, wenn ein Arzt den Befund oder die Diagnose nicht mehr auf der handgeschriebenen Überweisung seines Kollegen liest, – dessen Urteil er aus alter „Freundschaft” noch nie sonderlich getraut hat! – sondern auf der „unbestechlichen, objektiven und verlässlichen Patientenchipkarte”, die nichts anderes ist als ein kleines (?) maschinelles IT-System?

Wer macht sich die Mühe, darüber nachzudenken, ob die schnellere Abwicklung von Vorgängen in einer Behörde mit Hilfe von PCs oder Arbeitsplatzsystemen noch genau so korrekt und verlässlich ist, wie der Bürger dies seit Generationen erwartet, zumindest in Deutschland? Und zwar korrekt, verlässlich und beherrschbar im umfassenden Sinne dualer Sicherheit und nicht eingeschränkt auf den Zuverlässigkeitsbegriff der Massendatenverarbeitung. Wer durchschaut noch, welche Folgen es für ihn hat, wenn er seine Einkäufe nicht mehr anonym im Kaufhaus erledigt, sondern „beweglich, freizügig und bequem” vom Mobiltelefon aus unter Angabe (*Preis*gabe?) seines Aufenthaltsorts, Datum, Uhrzeit, Rufnummer, Kreditkartennummer und … und …?

[12] *Frey, Lüthgens* und *Schulz-Hardt* verwenden in einem Projekt über Entscheidungsverhalten den Begriff *gelernte Sorglosigkeit*.

Kern der Überlegungen zum Einsatz moderner Informationstechnik darf nicht allein die Frage nach höherer Leistung sein, nach Geschwindigkeit, Durchsatz, Performanz. (sic!) und was solch bedenklicher, neudeutsch-olympischer Ziele mehr sind. Die Frage nach den Veränderungen, nach den Beeinträchtigungen für die Betroffenen und damit für die Gesellschaft, die mit dem Übergang der Datenverarbeitung und Kommunikation auf automatisierte Systeme verbunden sind, muss mit beantwortet werden, und zwar nicht erst vom Anwender oder Verbraucher, sondern von Anfang an, vom Planer, vom Entwickler, vom Hersteller, vom Verkäufer, vom Betreiber, von jedem Beteiligten. Jeder in dieser Kette ist ***Betroffener***.

Wo das nicht geschieht, klafft eine Lücke in der dualen Sicherheit. Informations- und Kommunikationstechnik muss nicht nur verlässlich sein in technischer Sicht, sie muss auch beherrschbar bleiben aus der Sicht der Betroffenen.

7.3 Sorglosigkeit – falsche Euphorie

Die Einführung moderner Informations- und Kommunikationstechnik an jedem beliebigen Arbeitsplatz (*individuelle Datenverarbeitung*) bestätigt in allen Teilen auch die zweite Aussage. Schon allein die ins Auge stechenden quantitativen Leistungen des neuen Werkzeugs führen geradezu zwangsläufig zu einer euphorischen Grundhaltung der Beteiligten. Der Katzenjammer über nicht beherrschte Systemabstürze, verlorene Daten, unvorhergesehene Reaktionen, nicht durchschaubare („Was macht ***ER*** denn nun schon wieder?") und nicht funktionierende – und von niemandem mehr wartbare – Programme, stellt sich erst später ein.

Die Gefährdung – das ist das Neue – betrifft heute aber nicht mehr nur eine ganz bestimmte Gruppe von Spezialisten, sondern jeden, der mit moderner Informationstechnik zu tun hat – und das ist in den entwickelten Industriegesellschaften de facto jedermann, beruflich und auch privat.

8. Fazit

Was ist die Folge? Bilderstürmerei ist unsinnig. Unsere Gesellschaft kann ohne moderne Informationstechnik nicht mehr überleben. Euphorie ist gefährlich. Sie verführt zu unbedachten Handlungen, zu Missbrauch.

Ein gesundes Misstrauen dagegen ist gegenüber der modernen Informationstechnik angebracht! Das Fazit der Überlegungen kann in fünf einfachen Thesen niedergeschrieben werden, die sich in einem einzigen, Grundsatz zum Thema IT-Sicherheit zusammenfassen lassen.

Grundsatz und fünf Thesen zur IT-Sicherheit[13]

These 1

Die Informationstechnik hat als wesentlicher, ja entscheidender Faktor auf Struktur und Arbeitsweise der Gesellschaft stärker verändernd eingewirkt als irgendeine andere Einflussgröße.

These 2

Sicherheit der Informationstechnik muss immer dual gesehen werden. Sie hat zwei komplementäre Sichten,

- ***die Sicherheit der Systeme***
  d.h. die technische und organisatorische Verlässlichkeit der IT-Systeme, d.h. der auf ihnen laufenden Prozesse und der mit ihrer Hilfe erzeugten Ergebnisse, und
- ***die Sicherheit der Betroffenen***
  d.h. der Einzelnen und der Gesellschaft, vor unerwünschten Auswirkungen des Einsatzes neuer Technologien und neuer Verfahren in der Informationstechnik und das heißt deren Kontrollierbarkeit und Beherrschbarkeit.

In diesem Sinne ist Sicherheit der Informationstechnik immer

duale Sicherheit.

These 3

Soll Informationstechnik in der Gesellschaft sicher, d.h. ordnungsmäßig, verlässlich und beherrschbar bleiben, auch unter wesentlich veränderten technischen und strukturellen Randbedingungen, so sind dafür

- neue Techniken und Werkzeuge
- neue Verfahren
- neue Organisationsformen[14]

unabdingbar.

These 4

Duale Sicherheit im Sinne dieser zwei zueinander komplementären Sichten ist unverzichtbarer Bestandteil jeder Planung, jeder Entwicklung und jeder Nutzung der Informationstechnik.

These 5

Bei zunehmender Individualisierung und Vernetzung der modernen Informationstechnik muss jeder Einzelne die Gefahren kennen, die ihm und der Gesellschaft drohen, und er muss diejenigen Werkzeuge in die Hand bekommen, mit denen er Sicherheitslücken nach bestem Wissen, nach seinen Anforderungen und nach dem Stand der Technik schließen kann.

Grundsatz

Leistungsfähigkeit[15] und duale Sicherheit sind gleichrangige Konstruktionsprinzipien sicherer IT-Systeme.

---

[13] Der Grundsatz erstmals veröffentlicht zur Datenschutz-Fachtagung DAFTA ’78, die Thesen auf der DAFTA ’84

[14] Darin sind notwendig neue **rechtliche Regelungen** eingeschlossen *(Verrechtlichung der Informationstechnik, Medienrecht)*.

[15] Beachte: Leistungsfähigkeit umfasst nicht nur ***quantitative*** Komponenten wie Geschwindigkeit, Kapazität, ..., sondern vor allem auch ***qualitative*** (Flexibilität, Benutzerfreundlichkeit *(usability),* Vertrauenswürdigkeit, etc.).

9. Veröffentlichungen

BSI89 ZSI – *IT-Sicherheitskriterien – Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT) – 1.Fassung 1989*
Zentralstelle für Sicherheit in der Informationstechnik (heute: BSI – Bundesamt für Sicherheit in der Informationstechnik), herausgegeben im Auftrag der Bundesregierung, Bundesanzeiger Verlagsgesellschaft mbH, Bonn 1989, 107 Seiten, ISBN 3-88784-192-1

BSI2000 BSI Bundesamt für Sicherheit in der Informationstechnik – *IT-Grundschutzhandbuch – Maßnahmenempfehlungen für den mittleren Schutzbedarf*
Verlag Bundesanzeiger Köln 2002 (auch auf CD)

CC96 CCEB *Common Criteria for Information Technology Security Evaluation Criteria (CC) – Version 1.0*
Common Critria Editorial Board (CCEB) 1996

Dst90 Dierstein, R. *The Concept of Secure Information Processing Systems and Their Basic Functions*
Proceedings of the IFIP SEC '90, 6th International Conference and Exhibition on Information Security, Espoo (Helsinki), Finland, May 1990

Dst97 Dierstein, R.*; Duale Sicherheit – IT-Sicherheit und ihre Besonderheiten*
in: Pfitzmann, A./ Müller, G. (Hrsg.) – Mehrseitige Sicherheit in der Kommunikationstechnik; Addison-Wesley-Longman, Bonn– Reading (Mass.) 1997, p.31–60, ISBN 3-8273-1116-0

prov94 Roßnagel, A./ Bizer, J./ Hammer, V./ Kumbruck, Chr./ Pordesch, U./ Schneider, M.J. (provet)/ Sarbinowski, H. (GMD) – *Die Simulationsstudie Rechtspflege – Eine neue Methode zur Technikgestaltung für Telekooperation*
edition Sigma, Berlin 1994, 302 Seiten, ISBN 3-89404-373-3

RPM96 Rannenberg, K./ Pfitzmann, A./ Müller, G. *Sicherheit, insbesondere mehrseitige IT-Sicherheit*
it+ti Informationstechnik und technische Informatik, 38. Jahrgang 1996, Heft 4, S. 5-10, München

8.1 Einige weitere Veröffentlichungen

Chau85 Chaum, D. – *Security without Identification: Transaction Systems to make Big Brother Obsolete*
Communications of the ACM 28/19 (1985), S. 1030–1044

CTCP93 CSSC – *The Canadian Trusted Computer Product Evaluation Criteria – Version 3.0e*
Canadian System Security Centre, Communication Security Establishment, Government of Canada, Jan. 1993, XXV+208 Seiten

D21 Projektgruppe IT-Sicherheitskriterien und IT-Grundschutz-Zertifikat/Qualifizierung *IT- Sicherheitskriterien im Vergleich*
Herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik, Bonn 2001

Dst84 Dierstein, R. *Zugriffsberechtigung, Datenschutz und Datensicherung bei zunehmendem PC-Einsatz – Empfehlungen für ein Datensicherungskonzept*
Proc. 2. Europäischer Kongress über Büro-Systeme & Informations-Management – Der PC im Büro, CW-Edition, München 1984, S. 873–894

Dst86 Dierstein, R. *Basic Functions of Secure Systems*
Proceedings Securicom ‘86 – 4ème Congrès Mondial de la Protection et de la Sécurité Informatique et des Communications, Paris 1986, S. 467–476

DIN88 DIN – *Deutsche Norm – Informationsverarbeitung Begriffe Teile 1–9*
Deutsches Institut für Normung; Beuth Verlag GmbH, Berlin November 1988

ITSEC91 CEC – Directorate General XIII *Information Technology Security Evaluation Criteria (ITSEC) – Provisional Harmonised Criteria*
Office for Official Publications of the European Communities, Luxembourg, Juni 1991, 163 p., ISBN 92-826-3004-8

8.2 Zur Kryptologie

Beut93 Beutelspacher, Albrecht *Kryptologie – Eine Einführung*
Verlag Vieweg GmbH, Braunschweig, 2. Aufl. 1991, 179 S., ISBN 3-528-18990-8

Bit01 Bitzer, Frank/ Brisch, Klaus M. *Digitale Signatur*
Springer-Verlag, Heidelberg*,2001, 195 S.*

Sta01 Stallings, William *Sicherheit im Internet*
Addison-Wesley-Longman, Bonn–Reading (Mass.) 2001, 471 S.

FumR94 Fumy, Walter / Rieß, Hans Peter *Kryptographie – Entwurf, Einsatz und Analyse symmetrischer Kryptoverfahren*
2. Auflage, R.Oldenbourg Verlag, München, 1995, 392 Seiten, ISBN 3-486-22213-9

Schnei96 Schneier, Bruce*; Angewandte Kryptographie – Protokolle, Algorithmen und Source-Code in C*
1. Auflage deutsch, Addison-Wesley Publishing Company, Bonn –Reading (Mass.), 1996, ISBN 3-89319-854-7

Singh02 Singh, Simon*; Geheime Botschaften*
Deutsche Ausgabe, Carl Hanser Verlag München Wien 2002, ISBN 3-89319-854-7