

**Rede von
Herrn Dr. Udo Helmbrecht
Präsident des Bundesamtes für Sicherheit in der Informationstechnik**

anlässlich

der Jahrestagung der Gesellschaft für Informatik (GI)

„Informatik 2003“

am 30. September 2003

in Frankfurt/a.M.

Titel: „IT-Sicherheit – Hauptaufgabe der Informatik“

(Es gilt das gesprochene Wort!)

Sehr geehrter Herr Prof. Dr. Mayr,
sehr verehrte Damen und Herren,

als ich vor wenigen Monaten - im Mai diesen Jahres – zu dieser Tagung eingeladen wurde und gefragt wurde, ob ich als Keynote-Sprecher auftreten wolle, so war ich darüber sehr erfreut. Nicht weil ich erst seit Mitte März das Amt des BSI-Präsidenten inne habe, sondern weil es zeigt, dass das Thema Sicherheit zunehmend in das Bewusstsein der Informatikerinnen und Informatiker rückt. Eine Tatsache, die aus meiner Sicht nicht unbedingt selbstverständlich ist. Und deshalb möchte ich mich nochmals ausdrücklich bei allen Verantwortlichen der Tagungsleitung für die Einladung bedanken.

Im Vorfeld eines solchen Tages macht man sich viele Gedanken darüber, wie man Sie - liebe Zuhörer - für eine Weile in den Bann der Worte ziehen kann. Ich habe meinen heutigen Beitrag unter die Frage: „IT-Sicherheit – Hauptaufgabe der Informatik?“ gestellt. Hierbei halte ich mich an die Chinesische Philosophie. Bestimmt kennen Sie den Ausspruch: „Verantwortlich ist man nicht nur für das, was man tut, sondern auch für das, was man nicht tut.“ Natürlich konnte sich der chinesische Philosoph Lao Tse dabei nicht auf die Informationstechnik des 21. Jahrhunderts beziehen. Doch obwohl dieser Satz schon über 2000 Jahre alt ist – finde ich ihn außerordentlich passend, wenn wir uns mit der Verantwortung, die das Fachgebiet der Informatik trägt, auseinandersetzen.

Das große Wort „Verantwortung“ steht im Raum. Verantwortlich ist man für das, was man tut – also ist man zunächst verantwortlich für sich selbst. Verantwortlich ist man aber auch für seine Familie, seine Angehörigen. Verantwortlich ist man in dem, was man tut. Also auch im Beruf. In jedem Beruf gibt es Momente, in denen man sich mit ethischen Fragen konfrontiert sieht. Bei Berufen wie Polizist, Arzt oder Politiker ist dies offensichtlich. Bereits bei der Berufsplanung macht man sich Gedanken über Auswirkungen und Richtigkeit des eigenen Handelns. Für einen Informatiker sind solche Gedanken oft weniger naheliegend. Doch mit dem noch immer fortschreitenden Einzug von Informationstechnik in alle Lebensbereiche bestimmen Sie (die Informatiker) maßgeblich direkt oder indirekt mit, wer über was und wie informiert ist, was an Handlungen in einem System möglich ist und wie damit Macht ausgeübt werden kann.

Daraus abgeleitet erübrigt sich die Frage danach, ob die Informatik eine gesellschaftliche Verantwortung trägt. Natürlich tut sie das. Es ließen sich unzählige Autoren nennen, die sich mit dieser Fragestellung beschäftigen. Die Verantwortung der Informatik ist – zurecht - ein vieldiskutiertes Thema. Dabei kommt man nicht umhin, die Gedanken von Joseph Weizenbaum bei dieser Diskussion aufzugreifen (dem morgen

die Ehrenmitgliedschaft der GI verliehen wird, wozu an dieser Stelle herzlich gratulieren möchte). Ihm zufolge sind alle relevanten Probleme weder technischer noch mathematischer, sondern ethischer Natur. Ich zitiere „Wir leben jedoch in einer Gesellschaft, in der eine große Scheu davor besteht, Verantwortung zu übernehmen. Verantwortung ist keine technische, sondern eine gesellschaftliche Frage. Unsere Gesellschaft hat die Technik entwickelt, Verantwortung so zu verteilen, dass sie niemand hat.“¹ Nun frage ich Sie, meine Damen und Herren, hat Joseph Weizenbaum Recht? Haben wir es uns mit der Technik vielleicht zu einfach gemacht? Schieben wir nicht so manche Diskussion auf die Technik ab, weil wir der gesellschaftlichen Diskussion darüber aus dem Weg gehen möchten? Welche Rolle spielt also die Informatik in der Gesellschaft? Welche Rolle spielt der Mensch in der Informatik oder noch allgemeiner: Welche Rolle spielt der Mensch in der Wissenschaft?

Bei dieser Fragestellung liegt es nahe auf den Fachbereich „Informatik und Gesellschaft“ der Gesellschaft für Informatik (GI) und speziell auf den Arbeitskreis „Informatik und Verantwortung“, zu verweisen, der 1994 die Ethischen Leitlinien der GI verabschiedet hat. Durch die sich ändernden Arbeitsbedingungen im Umfeld der Informations- und Kommunikationstechnologie müssen die Ethischen Leitlinien ständig fortgeschrieben werden. Daran arbeitet auch der Workshop „Ethik in der Informatik“ am Donnerstag Vormittag.

Meine Damen und Herren,
der Diskurs über ethische Fragen in der Informatik ist meines Erachtens nach für unsere Gesellschaft unerlässlich. Und als Physiker zitiere ich gern aus dem Stück „Die Physiker“. Friedrich Dürrenmatt schrieb „Was alle angeht, können nur alle lösen. Jeder Versuch, eines Einzelnen, für sich zu lösen, was alle angeht, muss scheitern.“

Natürlich ließen sich an dieser Stelle noch weitere Thesen zur Verantwortung der Informatik erläutern. Es gibt unzählige Vorlesungen und Veröffentlichungen dazu. Ich weiß, dass sich viele unter Ihnen mit diesem Thema ausführlich beschäftigen oder in der Vergangenheit beschäftigt haben. Ich muss Ihnen gestehen, dass ich es nicht habe. Ich bin „einfacher Naturwissenschaftler“ und kein Computer- oder gar Gesellschaftskritiker wie beispielsweise Weizenbaum es ist. Doch in dieser Rolle möchte ich auch gar nicht vor Ihnen stehen. Mir geht es heute vielmehr darum, Ihnen allen den Aspekt „Sicherheit“ vor Augen zu führen. Sicherheit als einen maßgeblichen Aspekt, wenn wir von der Verantwortung der Informatik für die Gesellschaft sprechen.

¹ Joseph Weizenbaum: Computermacht und Gesellschaft, Suhrkamp Verlag, 2001

Meine sehr verehrten Damen und Herren,
lassen Sie mich dabei – ausnahmsweise – ganz von vorn anfangen und einen kurzen Blick auf die noch junge Geschichte der Informatik werfen.

Der Begriff Informatik – dieses Kunstwort aus Information und Mathematik – wurde – und auch das dürfte für keinen von Ihnen etwas Neues sein – Ende der fünfziger Jahre von der Firma SEL für seine Produkte geschützt. Nachdem das französische "informatique" bei der Académie Française offiziell wurde, verbreitete sich die Bezeichnung "Informatik" auch in Deutschland als Ersatz für das schwerfällige Wort "Informationsverarbeitung". Aber: In den USA und vielen anderen englischsprachigen Ländern setzte sich statt dem Begriff Informatik der Begriff "computer science" durch. Besonders diese Bezeichnung macht deutlich, dass die Informatik als eine Weiterentwicklung der algorithmischen Aspekte der Mathematik und Logik sowie der Nachrichtentechnik verstanden wurde - als "Computer-Wissenschaft". Eine Wissenschaft, die sich im Wesentlichen mit der Entwicklung von Rechenmaschinen beschäftigt.

Und genau hier liegt der Kern des Problems: Allein die Konzentration auf die Technik wird der Aufgabe nicht gerecht. Allein die Orientierung an der Technik, ohne gesellschaftliche Aspekte mit einzubeziehen, reicht nicht aus. Um es nochmals zu verdeutlichen: Informatik schafft Technik. Technik verändert unsere Gesellschaft. Und damit ist wieder der Beweis erbracht – Sie ahnen es schon – welche gewaltige Verantwortung die Informatik trägt.

Dabei stellen die steigende Leistungsfähigkeit der IT, verbunden mit der zunehmenden Komplexität der Systeme, neue und erhöhte Ansprüche an die Verantwortung derer, die diese Systeme erdenken, entwickeln und betreiben, also an Sie (die Informatiker). Das gilt zum einen für die Entwicklung und den Einsatz der Hardware maschineller Systeme. Das gilt zum anderen in noch weit höherem Maße für die Software: Sie stellt die eigentliche Verbindung zwischen Anwendung und Maschine her und legt fest, wie, in welchem Umfang und mit welchen Auswirkungen informationsverarbeitende Prozesse, die ursprünglich dem Menschen vorbehalten waren, auf Maschinen übertragen werden können oder dürfen.

Um die Verantwortung vor allem derer, die Software programmieren, noch deutlicher zu machen, frage ich Sie: Fallen Ihnen auf Anhieb spektakuläre Ereignisse ein, die teilweise auch auf Programmierfehler zurückzuführen sind?

Bestimmt. Ich nenne nur ein paar Stichworte: Das Jahr 2000-Problem, das Ariane 5 Unglück 1996, die kritische Landung der Airbus 320-Maschine in Warschau, die tödliche Überdosierung von Patienten durch medizinische Bestrahlungsgeräte vom Typ Therac 25. Von diesen Beispielen gibt es noch etliche mehr. Da liegt die Frage nahe: Wie sicher kann man eigentlich sein, dass das neue Mobiltelefon, die Steuerung der neuen Waschmaschine, des gestern oder noch heute Morgen benutzten Flugzeuges oder der Sicherheitsfunktionen im Auto immer so funktioniert, wie man es erwartet? Oder woher weiß man, dass dadurch nie eine Katastrophe ausgelöst wird? Es gibt den bekannten Vergleich: Wären Brücken wie Software erbaut, würde kein Mensch über Brücken fahren.

Robert Baber schrieb dazu schon Anfang der 80er Jahre: "Natürlich hat jede Ingenieurdisziplin ihre Fehlschläge. Fehlschläge auf dem Gebiet der Softwareentwicklung sind jedoch viel häufiger als in jedem anderen Bereich des Ingenieurwesens. Der Einsturz eines Gebäudes oder einer Brücke ist ein berichtenswertes Ereignis; die Öffentlichkeit ist überrascht, eben weil solche Ereignisse selten sind. Die Entdeckung eines Konstruktionsfehlers von ähnlicher Tragweite bei der Wartung eines zivilen Flugzeuges, um ein anderes Beispiel zu nehmen, ist ein ebenso ungewöhnliches und überraschendes Ereignis. Solche Fehler machen in der Regel Schlagzeilen, führen zu Änderungen in der Praxis auf dem entsprechenden Gebiet der Ingenieurwissenschaft und werden zu Schlüsselbeispielen in der Ausbildung von Ingenieuren. Wenn solche Fehler entdeckt werden, erwartet man, dass der Verursacher Schadenersatz leistet, wozu er in der Regel auch gesetzlich verpflichtet ist. Auf dem Gebiet der Software sind größere Zusammenbrüche jedoch so häufig, dass nur die größten und spektakulärsten für erwähnenswert gehalten werden; die meisten erregen relativ wenig Aufmerksamkeit. Sie lösen Enttäuschung aus, gewiss, aber nicht Überraschung. Sie werden akzeptiert als die Regel, die sie nun einmal sind, da sie so häufig vorkommen, dass es unrealistisch wäre, vom Verursacher Schadenersatz zu erwarten."²

Und ich habe einen weiteren Vergleich parat: Die Physiker haben die Grundlagen für die Kerntheorie entwickelt. Kernkraftwerke werden jedoch von Ingenieuren erbaut. Die Informatiker entwickeln Software. Sollten sie das Programmieren vielleicht auch den Ingenieuren überlassen?

Warum stelle ich solche Fragen?! Natürlich um nachdenklich zu machen: Wie sicher und verlässlich ist eigentlich die Software all der eingebetteten Systeme, denen wir Tag für

² Robert L. Baber, *Softwarereflexionen*, Springer Verlag, 1982

Tag unser Leben anvertrauen? Ich glaube, darauf hat niemand sofort eine Antwort parat.

Und deshalb beginne ich bei mir selbst: Als Naturwissenschaftler weiß ich nur zu gut, dass ein Programm Ergebnisse liefern muss. Die Frage nach Robustheit und Sicherheit hatte in meiner Vergangenheit wahrlich keine Priorität. Vielmehr galt der Aspekt Sicherheit als Störfaktor. Dabei käme kein Wissenschaftler, also konkret kein Fahrzeugentwickler, kein Anlagenbauer, kein Flugzeug- oder Schiffskonstrukteur, überhaupt kein Ingenieur käme je auf den Gedanken, in seinem Anwendungsbereich den Aspekt Sicherheit zu vernachlässigen.³ Gerade im Bereich Verkehr ist Sicherheit inzwischen zu einem wichtigen Verkaufsargument geworden. Oder würden Sie heutzutage ein Auto ohne Airbag kaufen? Im Bereich der Informationstechnik herrscht noch immer die Mentalität, dass man Sicherheit bei Bedarf nachträglich einbauen könne. Dann, wenn sich bei der Anwendung Sicherheitslücken auftun. Denn offenbar scheint ausgerechnet in der Informationstechnik alles ganz anders zu sein: Getreu dem olympischen Motto „schneller, höher, weiter“ ergötzen sich die Techniker an den Taktraten und Funktionalitäten. Mehr Leistung, mehr Funktionen, mehr Vernetzung. Die Frage mit welchen Mitteln, um welchen Preis, mit welchen Folgen wird nicht gestellt! Sicherheit und Schutz sind – wenn überhaupt - ein notwendiges Übel. Es regiert das Prinzip Hoffnung.

Während in der Vergangenheit zunächst die Security – also der physische Schutz von Informationen - betrachtet wurde, so kommt dem Aspekt Safety – dem Schutz von Menschen und Sachwerten vor dem Versagen technischer Systeme – eine immer größere Bedeutung zu.

Das BSI definierte 1992 den Begriff „IT-Sicherheit“ mit dem Ausschluss bzw. der Verminderung von Gefahren und der Betrachtung von technischen Gefährdungen wie Bedienungsfehler, technisches Versagen, katastrophenbedingten Ausfällen und absichtlichen Manipulationsversuchen. Es ging damals vorwiegend um den physischen Schutz von Informationen. Natürlich darf die Gebäudesicherheit gerade bei Rechenzentren oder der Schutz der Daten vor Verlust, Feuer, Diebstahl usw. nicht vernachlässigt werden. Aber vor dem Hintergrund der steigenden Abhängigkeit von den IT-Systemen muss der Schutz des Menschen vor dem Versagen der technischen Systeme noch wichtiger werden.

³ G.Weck/R.Dierstein: „Werden wir IT-Sicherheit lernen?“, Mai 2002, www.gi-ev.de

Meine Forderung lautet daher: IT-Sicherheit muss als notwendige Eigenschaft aller Systeme und Netze erkannt und akzeptiert werden. Nur so kann der Mensch ausreichend geschützt werden.

Dieses Ziel ist sicherlich hochgesteckt, denn es setzt Wissen und Verständnis bei den Betreibern voraus, und zwar nicht nur bei den Technikern, sondern auch bei den Planern und IT-Beschaffern. Allen Beteiligten muss klar sein, dass die beiden Grundkomponenten der IT-Sicherheit - Verlässlichkeit und Beherrschbarkeit - unverzichtbare Bestandteile jedes IT-Systems sein müssen. Leistungsfähigkeit ohne Sicherheit ist ein Widerspruch in sich!

Meinen Damen und Herren,

wie Sie wissen, wurde die Informatik in der Vergangenheit zunächst als Spezialgebiet innerhalb anderer wissenschaftlicher Disziplinen betrieben. Seit 1960 kann sie jedoch nicht mehr nur als Ansammlung von aus anderen Wissenschaften - z.B. Logik, Mathematik, Elektrotechnik - entlehnten Methoden und Regeln aufgefasst werden. Die Informatik hat sich zu einem zusammenhängenden, theoretisch fundierten Gebäude und damit zu einer neuen Grundlagenwissenschaft entwickelt, die auf andere Wissenschaften ausstrahlt.

Mit dem Aspekt Sicherheit in der Informationstechnik verhält es sich ähnlich. Die IT-Sicherheit ist ein Querschnittsthema. Es berührt nahezu alle Gebiete der Informatik und hat darüber hinaus Bezug zu anderen Wissenschafts- und Gesellschaftsbereichen, z. B. zur Mathematik und zu Ingenieursdisziplinen. Und wenn – wie bereits nicht erst seit heute festgestellt - informationstechnische Systeme in immer größerem Umfang unser Leben durchdringen und wir uns immer stärker vom Funktionieren der Technik abhängig machen, dann muss es das Ziel der IT-Sicherheit sein, die dadurch entstehenden Risiken zu minimieren, offen zu legen und möglichst beherrschbar zu machen.

Ich frage Sie: Wie schaffen wir es, dass die Sicherheit einen höheren Stellenwert in der Informatik erhält? Natürlich indem wir bei der Informatik-Ausbildung beginnen. Wir müssen in den Köpfen der jungen Menschen verankern, wie wichtig gerade der Aspekt Sicherheit ist. Gleich vorweg genommen: Erfreulicherweise gibt es einige Hochschulen, die sich sehr intensiv mit dem Thema auseinandersetzen. Doch wie sieht es allgemein aus? Wie ist es um die Ausbildung hierzulande bestellt?

Durch meinen eigenen Werdegang kann ich einen Teil der Antwort erneut bei mir selbst suchen: Als Physiker bin ich im Grunde Autodidakt, wenn es ums Programmieren geht. Ende der 70er Jahre habe ich die damals gängigen Programmiersprachen im

Rechenzentrum der VEBA Oel AG in Gelsenkirchen gelernt. Inzwischen gibt es jedoch über 700 Programmiersprachen. Ich frage mich: Wer hat eigentlich noch den Überblick? Bei dieser ungeheuren Dynamik der Technik und der Programmiersprachen ist es doch sehr verwunderlich, dass sich die heutigen Rechner noch immer nicht vom „von Neumann-Prinzip“ gelöst haben. "Speicher, Leitwerk, Rechner, Anweisung, Operanten, Variablen, Daten, ... Information", diese Dinge haben sich seit der Definition eines Computers durch John von Neumann 1947 nicht verändert.

Und Fakt ist doch auch, dass es bei Programmierkursen an der Uni immer darum geht: Wie löse ich ein Problem mit dem Rechner? Das Denken wird bestimmt vom Algorithmus, vom Programm, vom Ergebnis. Und am Ende entstehen schöne Tabellen und Graphiken. Mehr Komponenten werden nicht mit einbezogen. Nach anderen als den technischen Aspekten des zu lösenden Problems fragt – wenn wir ehrlich sind – doch fast keiner. Das müssen wir ändern.

Zwar gibt es in einigen Universitäten Vorlesungen bzw. Arbeitsgruppen, die den Titel „Informatik und Gesellschaft“ tragen – wie z. B. an der Universität Dortmund oder der Technischen Universität zu Berlin – doch das ist die Ausnahme. Dabei geht es um die gesellschaftlichen Voraussetzungen und Folgen des IT-Einsatzes. D.h. es geht weit über die erkenntnistheoretischen Probleme der Informatik und die Ansätze einer Computerethik hinaus. Viele junge Informatiker fragen, was darf ich tun, was darf ich nicht tun? Gemeinsam mit diesen jungen Menschen müssen wir darauf Antworten finden. Nach Weizenbaums Überzeugung sollte jeder Informatiker über die Beschränkungen seines Werkzeugs ebenso sprechen wie über seine Möglichkeiten – auch das gehört zur Informatik dazu.

Wenn man von der Vermittlung der gesellschaftlichen Verantwortung einmal absieht, und schaut, wie das Thema IT-Sicherheit im Studium vermittelt wird, so ergibt sich kein erfreuliches Bild. Wie überall hängt sehr viel vom persönlichen Engagement und Interesse der Dozenten ab. Noch immer gibt es keine standardisierten Lehrpläne, die den Aspekt Sicherheit beinhalten.

Mir drängt sich dabei die Frage auf: „Sind Wirtschaftsinformatiker vielleicht die besseren – weil sicheren - Informatiker?“ Nach Gesprächen mit meinen Mitarbeitern könnte man das tatsächlich meinen. IT-Sicherheit wird immerhin im Studium behandelt, zwar nicht im Grundstudium, aber doch verpflichtend im Hauptstudium. Fast kein Wirtschaftsinformatiker verlässt also die Universität, ohne das Thema Sicherheit jemals behandelt zu haben. Auch hier gilt natürlich die Einschränkung, dass es nicht auf alle Universitäten zutrifft und abhängig ist vom jeweiligen Lehrplan.

Resultierend aus meinen bisher gewonnenen Erkenntnissen komme ich deshalb zu dem Schluss: Noch immer gibt es zu wenig Lehrstühle in Deutschland, die sich dediziert mit dem Thema IT-Sicherheit auseinandersetzen. Gerade mal ein Dutzend, vielleicht noch ein oder zwei mehr – mehr aber auch nicht. Die Universitäten Frankfurt, Bochum, Darmstadt, Aachen, Hamburg und die Fachhochschule Rhein-Sieg seien beispielhaft genannt. Natürlich weiß ich, dass das Thema von vielen Universitäten implizit unter der Informatikflagge bearbeitet wird – aber ich meine: Das reicht nicht aus!

Darüber hinaus schließe ich mich voll und ganz der Forderung des GI-Arbeitskreises „Sicherheit in der Ausbildung“ an: Nur wenn IT-Sicherheit als integraler Bestandteil der Ausbildung zum Informatiker gesehen wird, besteht Hoffnung, das notwendige Wissen auf eine so breite Grundlage zu stellen, dass Sicherheitsanforderungen ernst genommen und nicht als überflüssiges Beiwerk oder sogar als Nörgelei abqualifiziert werden. IT-Sicherheit muss als unverzichtbares Thema in die Informatik- und Wirtschaftsinformatik-Studiengänge aufgenommen werden. Die Grundlagen dafür müssen schon im Informatikunterricht an den Schulen gelegt werden, denn dort werden die ersten prägenden Erfahrungen für den verantwortungsvollen Umgang mit der Informationstechnik gelegt.

Genauso wenig wie ein Informatiker sein Fach ohne eingehende Kenntnisse von Datenstrukturen und Algorithmen wirklich versteht, ebenso so wenig darf sich jemand Informatiker nennen, der sich mit IT-Sicherheit noch nie ernsthaft befasst hat.

Deshalb fordere ich: Schon im Grundstudium – oder zumindest zu Beginn des Hauptstudiums – sollten alle notwendigen Sicherheitsaspekte behandelt werden. Dazu gehören meiner Ansicht nach die Themen: Virenschutz, technische Schutzmaßnahmen wie Firewalls und Intrusion Detection Systeme, die Verschlüsselung von Daten, die Datensicherheit, aber auch die Internetsicherheit, der IT-Grundschutz und die Zertifizierung. Hier sollte mindestens ein Basiswissen aufgebaut werden.

Lassen Sie mich es Ihnen am Beispiel Zertifizierung verdeutlichen: Die technische Funktionsweise von IT-Produkten (und Systemen) ist für weite Kreise der Anwender nicht durchschaubar. Aber gerade die Transparenz hinsichtlich der Sicherheitseigenschaften von IT-Produkten ist wie eine magische Formel, wenn es um Vertrauen der Benutzer in die IT geht. Die Prüfung und Bewertung von IT-Produkten und -Systemen nach einheitlichen Kriterien durch unabhängige Stellen ist eine Möglichkeit Transparenz zu schaffen. Ein Arbeitsschwerpunkt des BSI ist daher die Vergabe von Sicherheitszertifikaten für IT-Produkte (Systeme oder Komponenten). Die Zertifizierung eines Produktes erfolgt nach den IT-Sicherheitskriterien (Common Criteria / ITSEC) und

wird auf Veranlassung des Herstellers oder eines Vertreibers durchgeführt. Darüber hinaus bietet das BSI das IT-Grundschutzzertifikat an, das durch einen vom BSI lizenzierten IT-Grundschutz-Auditor erteilt wird.

Zertifizierung ist eines der Themen, das für einen Informatiker schon beim Eintritt ins Berufsleben kein Fremdwort mehr sein sollte. Die Absolventen können dieses Wissen bei ihrem späteren Arbeitgeber in dreifacher Hinsicht einbringen: Erstens können sie bei der Entwicklung von Produkten dafür sorgen, dass diese auch zertifiziert werden. Zweitens sind sie in der Lage beim Einkauf von IT-Produkten die Zertifizierung als ein Entscheidungskriterium zu berücksichtigen. Und drittens ergeben sich neue Beschäftigungschancen, indem sie selbst als Zertifizierer tätig werden. All das sorgt insgesamt für die Erhöhung der IT-Sicherheit.

Aber zurück zur Ausbildung: Neben der Vermittlung von Basiswissen würde ich mir zusätzlich wünschen, dass die Universitäten eigene Schwerpunkte setzen und Spezialthemen anbieten. Das können beispielsweise die Themen Abhörsicherheit, Abstrahlschutz, Lauschabwehr, Mobilfunksicherheit oder der Schutz Kritischer Infrastrukturen sein.

Lobenswert ist in diesem Zusammenhang das Engagement des eben schon erwähnten GI-Arbeitskreises „Sicherheit in der Informatik-Ausbildung“. Er arbeitet an Empfehlungen, wie der Aspekt Sicherheit in den Lehrplänen sowohl in der Hochschulausbildung als auch bei allen übrigen Aus- und Weiterbildungswegen integriert werden kann. Ende des Jahres werden weitere Überlegungen dazu veröffentlicht, auf die ich sehr gespannt bin.

Wenn man sich mit der Ausbildung der Informatiker beschäftigt, darf man einen Punkt nicht vergessen: Zwei Drittel aller IT-Fachkräfte sind Quereinsteiger ohne einschlägige berufliche Qualifikation. Traditionelle Weiterbildungsangebote konnten bisher kaum Abhilfe schaffen: Mehr als 300 unterschiedliche Abschlüsse stehen zur Auswahl – begrenzt auf Deutschland, ohne internationale Kompatibilität.⁴ Es reicht also nicht aus, allein über die Hochschulausbildung zu sprechen. Welchen Stellenwert haben Zertifizierungen in der Ausbildung von IT-Spezialisten?

Meine Damen und Herren,
wir sind uns glaube ich einig, dass Ausbildungsabschlüsse/Zertifizierungen in der beruflichen Karriere von IT-Spezialisten – gerade wegen der rasanten Entwicklung -

⁴ BITKOM, September 2003, www.bitkom.org

eine enorm wichtige Rolle spielen. Das eigene Know-how nachweisen zu können, ist nicht nur bei der Suche nach einem neuen Job unabdingbar. Noch vor drei Jahren – in den Boomzeiten - war es für Quersteiger relativ einfach interessante Jobs zu finden. Doch in wirtschaftlich schlechteren Zeiten wird klar: Ein anerkannter Abschluss ist wichtiger denn je. Denn oft ist jahrelange Berufserfahrung nicht automatisch gleichwertig zu einem Abschluss.

Es gibt sehr viele Anbieter von Zertifizierungen für IT-Spezialisten – und zunehmend finden sich Zertifizierungen für Sicherheitsexperten. Hier tummeln sich sehr viele Anbieter: neben Hochschulen und kommerziellen Veranstalter auch Gremien und Organisationen wie TeleTrust und BITKOM. Dementsprechend gibt es auch Weiterbildungen mit den unterschiedlichsten Zielen und für diverse Zielgruppen. Die Lehrinhalte und die Ausbildungsdauer differieren stark. Dies hat bisher zur Folge, dass die Abschlüsse keine hohe Anerkennung genießen. Im deutschsprachigen Raum gibt es trotz einer hohen Nachfrage sowohl bei Sicherheitsexperten als auch bei potenziellen Auftrag- bzw. Arbeitgebern keine allgemein oder gar international anerkannten Ausbildungen im Bereich Informationssicherheit. Fragen nach einer staatlich anerkannten Prüfung zum IT-Sicherheitsexperten werden immer wieder an das BSI herangetragen. Das starke Interesse hieran spiegelt sich auch an der hohen Zahl von IT-Grundschutz-Auditoren wieder – bisher die einzige Möglichkeit, vom BSI eine Anerkennung von Fachwissen zu erhalten.

Neben der Möglichkeit eines Studiums oder einer Zertifizierung gibt es auch den Weg der dualen Ausbildung. Hier sind besonders die Industrie- und Handelskammern bzw. die Handwerkskammern gefragt. Auch sie müssen bei der Vergabe der Abschlüsse den Aspekt Sicherheit noch stärker integrieren. Denn wir brauchen nicht nur Diplom-Informatiker, sondern auch Fachinformatiker, IT-Systemelektroniker und Informatikkaufleute, die für Sicherheitsaspekte sensibilisiert sind.

Wenden wir unseren Blick von der Ausbildung der Informatik hin zur öffentlichen Diskussion und Wahrnehmung der Thematik in der Öffentlichkeit. Erlauben Sie mir an der Stelle die Diskussion darüber, wann etwas öffentlich ist, zu sparen. Wichtiger ist meines Erachtens nach die Frage: Was können wir gegen die steigende Abhängigkeit aller Aspekte des täglichen Lebens von der Informationstechnik tun? Sollen wir sie quasi als gegeben hinnehmen? - Wohl kaum! Ist es nicht auch eine Frage von Verantwortung vielleicht bewusst auf Entwicklungen zu verzichten? Und damit meine ich nicht die ethischen Diskussionen, wie sie beispielsweise in der Biotechnologie vorkommen.

Vor dem Hintergrund des steigenden IT-Einsatzes besonders bei militärischen Auseinandersetzungen wird deutlich, dass Computer erst durch ihre Nutzung zur Waffe werden können. Alles liegt in der Verantwortung des Menschen. Algorithmen und Rechenpower werden nicht von selbst zur Waffe, werden aber vom Menschen als solche eingesetzt. Organisationen oder Einrichtungen mit (lebens-) wichtiger Bedeutung für das staatliche Gemeinwesen müssen deshalb in besonderer Form geschützt werden – dies ist eine gesamtstaatliche Aufgabe zur Gewährleistung der Inneren Sicherheit. Die kurzzeitig geführten Spekulationen darüber, ob am amerikanischen Blackout im August der Computerwurm Blaster Schuld sei, zeigen die Brisanz des Themas.

Meine sehr verehrten Damen und Herren,

wir alle wissen: 100 Prozent Sicherheit kann und wird es nicht geben. Jede Form von Sicherheit ist relativ. Nur, wer ist für die IT-Sicherheit zuständig, wer kann sie prüfen? Noch ist nicht eindeutig festgelegt, wer an welcher Stelle für den Schutz von Daten, Informationen und IT-Infrastrukturen verantwortlich ist. In anderen Bereichen gibt es das Luftfahrtbundesamt, das Kraftfahrtbundesamt oder den TÜV. Letzter sorgt dafür, dass unsichere Autos aus dem Verkehr gezogen werden. Wer sorgt dafür, dass unsichere Software aus dem Verkehr gezogen werden? Denn wie auf der Straße ist auch im IT-Bereich jeder einzelne Nutzer für die Sicherheit des Internets mitverantwortlich. Aber deshalb können nicht alle kontrolliert werden. Das ist auch nicht das Ziel. Das Ziel sollte es vielmehr sein, die Hersteller und damit die Entwickler, also auch Sie meine Damen und Herren, dazu zu bringen, die IT-Sicherheit als maßgeblichen Aspekt nicht außer acht zu lassen. Im Gegenteil: Sie sind aufgefordert, Sicherheit als festen Bestandteil bereits bei der Konzeption der Produkte und Systeme mit einzubeziehen.

Und es stellt sich auch die Frage: Ist IT-Sicherheit schon verpflichtend oder noch freiwillig? In den Unternehmen gibt es inzwischen überall einen Beauftragten für Arbeitsschutz, aber noch in den wenigsten Unternehmen und Behörden einen IT-Sicherheitsbeauftragten. Natürlich dauern alle Veränderungen ihre Zeit. Der Arbeitsschutz hat sich im Laufe von Jahrhunderten erst etablieren müssen. Aber benötigen wir immer erst Gesetze, um das Bewusstsein zu ändern? Denn wie so oft hinkt die Gesetzgebung der technischen und gesellschaftlichen Entwicklung hinterher. Erschwerend kommt hinzu, dass es mit der sinkenden Bedeutung von Ländergrenzen angesichts der weltweiten Vernetzung zunehmend schwieriger wird, nationales Recht durchzusetzen.

Nur ein generelles Umdenken kann helfen, Wege aufzuzeigen und zu beschreiten, die aus dieser Situation herausführen. Dies setzt als erstes ein besseres Wissen um die

IT-Sicherheit voraus, als es der normale Benutzer und selbst der durchschnittliche Informatiker heute besitzt.

Mein Fazit lautet: Wir brauchen in Deutschland eine angemessene Sicherheitskultur! Die damit verbundene IT-Sicherheitskompetenz umfasst bei den Nutzern zwei Dinge: Sie müssen das notwendige Bewusstsein für das Thema haben und – wie bereits eben gesagt - auch über das entsprechende Wissen verfügen. Anders ausgedrückt: Die Nutzer müssen individuell einschätzen und entscheiden können, welches Risiko sie bei der jeweiligen IT-Anwendung in Kauf nehmen können und wollen - und welches nicht.⁵

Meine sehr verehrten Damen und Herren,
wir müssen alles daran setzen, gemeinsam das Bewusstsein für die Sicherheit der Informationstechnik zu fördern. Denn die Sicherheit der Informationsgesellschaft liegt in unserer gemeinsamen Verantwortung. Je weniger Wissen die Kunden um die IT-Sicherheit haben, desto eher werden sie danach auch gar nicht verlangen. Es wäre jedoch erstrebenswert, dass die Sicherheit der IT-Produkte ein maßgeblicher Aspekt bei der Kaufentscheidung wird. Mein Wunsch wäre es, dass ein Nutzer beim Kauf des neuen PC die Sicherheitseigenschaften ebenso kritisch unter die Lupe nimmt, wie beim Kauf seines neuen Autos. Die Begriffe Virenschutz, Firewall, Verschlüsselung müssen ebenso selbstverständlich werden wie Airbag, ABS und Seitenaufprallschutz.

Dieses Verhalten setzt jedoch voraus, dass der Benutzer um die Bedeutung der IT-Sicherheit weiß und die dafür notwendigen Maßnahmen akzeptiert. Der Benutzer – und wenn Sie sich selbst fragen, werden Sie dem zustimmen - wägt ab zwischen Sicherheit und Funktionalität der Anwendung. Es ist also eine Frage der Bequemlichkeit. Noch immer herrscht bei vielen die Stimmung: Mich wird es nicht treffen. Das subjektive, persönliche Risiko wird nicht als hoch eingestuft, weshalb niemand zugunsten der Sicherheit Abstriche bei der Funktionalität einer Anwendung machen möchte.

Ausgehend von den Ergebnissen unserer aktuellen Technologietrendstudie rechnen wir bei den Privatanwendern damit, dass es bis 2007 – also noch vier Jahre – dauern wird, bis sich das Bewusstsein durchgesetzt hat, dass bei einem Produkt auch Sicherheitskriterien für den Kauf entscheidend sind.

Interessant ist, das laut einer Umfrage des Meinungsforschungsinstituts Emnid vom Mai diesen Jahres 46 Prozent der Befragten den Nutzer selbst als den Hauptverantwortlichen für die Sicherheit des Internets ansehen. Nur zwölf Prozent

⁵ Anja Hartmann/Pia Karger: Sicherheitskompetenz – ein häufig vergessener Baustein in der Informationsgesellschaft, 7. Deutscher IT-Sicherheitskongress des BSI, SecuMedia Verlag, 2001

machen den Gesetzgeber für die Sicherheit im Internet verantwortlich. Das bedeutet, dass das Umdenken in der Bevölkerung bereits begonnen hat. Aber kein Wunder, haben doch schon rund 65 Prozent der Nutzer schon einmal schlechte Erfahrungen mit dem Internet gemacht.⁶ Nur ein Viertel der Befragten hält das Internet für sicher. Attacken wie durch den Internet-Wurm Blaster tragen natürlich zu einer weiteren Verunsicherung bei.

Und auch Ereignisse wie der 11. September 2001 fördern das Bewusstsein für IT-Sicherheit. Sie zeigen, wie verwundbar unsere Gesellschaft ist. Das Interesse nach Sicherheit – und damit auch an der Sicherheit der Informationstechnik - ist seitdem gestiegen. Aber: Diese Entwicklung steht und fällt mit dem öffentlichen Interesse. Denn das Interesse an Sicherheit wird zu einem großen Maße durch das Medieninteresse hergestellt - besonders wie es nach diesen Terroranschlägen der Fall war.

Bei der Aufklärung über die Bedeutung der Sicherheit der Informationstechnik darf nicht vergessen werden, zu vermitteln, dass Technik immer nur Hilfsmittel sein kann. Und fest steht auch: IT-Sicherheit kann nicht durch einzelne Software erreicht werden, sondern ist das Ergebnis aus dem Zusammenspiel unterschiedlichster Faktoren. Dazu gehört der vernünftige Umgang mit der Technik, genauso wie das regelmäßige Einspielen von Updates.

Die Informatiker können den Benutzern aber einen Großteil dieser Aufgabe schon abnehmen: Die Anwendungsprogramme dürfen beispielsweise nicht so komplex sein, dass die User von zu vielen Funktionalitäten abgeschreckt werden – das gilt vor allem für Anwendungen, die auch für ältere und unerfahrenere Nutzer gedacht sind. Bei zuviel Komplexität passieren Anwendungsfehler. Und die Technik kann noch so sicher sein, wenn sie menschliches Versagen oder Fehler zulässt, ist sie es nicht mehr.

Die Sicherheitsgröße des „human factor“ ist demzufolge signifikant, wenn wir über IT-Sicherheit diskutieren. Einer Studie⁷ vom August diesen Jahres hat beispielsweise herausgefunden, dass drei Viertel der deutschen IT-Chefs menschliches Versagen als größte Gefahrenquelle für die IT-Sicherheit in Ihrem Unternehmen ansehen. Die rund 700 befragten IT-Leiter gaben erst später die Risiken Feuer (54 Prozent), Ausfallzeiten durch Wartungsarbeiten (50), Virusangriffe (48), Sabotage durch Hacker oder Kriminelle (40) an. Diese Einschätzung ist keineswegs neu und deckt sich mit Ergebnissen zahlreicher Studien aus den vergangenen Jahren. Aber diese Zahlen muss man sich vorstellen! Denn sie bedeuten: Der Weg, den wir vor uns haben, ist noch sehr lang.

⁶ Emnid-Umfrage, Mai 2003

⁷ Hitachi Data Systems: European Storage Index, August 2003

Ein bedeutsamer Schritt auf diesem Weg wurde im Februar letzten Jahres mit der Gründung des GI-Fachbereichs „Sicherheit – Schutz und Zuverlässigkeit“ getan. Mittlerweile besteht der Fachbereich aus mehr als ein Dutzend Fachgruppen. Das BSI ist mit mehreren Vertretern dabei. Ich begrüße die Entscheidung der GI, dass sich der neue Fachbereich mit der Teiltagung Sicherheit einer breiten Öffentlichkeit vorstellen kann, die die erste große Veranstaltung des Bereiches ist. Vor allem die Zusammenlegung der beiden Communities "Safety" und "Security" im neuen Fachbereich ist wegweisend. Denn die Vielzahl der sicherheitskritischen Anwendungen in Verbindung mit der Öffnung vormals dedizierter Systeme und die Diskussion um die entsprechenden Schnittstellen zeigen das starke Zusammenwachsen dieser Themenbereiche.

Innerhalb der Teiltagung Sicherheit ist das BSI selbst mit einer Reihe von Beiträgen beteiligt. Kurz nennen möchte ich die Workshop-Reihe Critical Infrastructure Protection, die von Dr. Willi Stein moderiert wird und bereits seit gestern läuft. Dabei geht es um den Schutz Kritischer Infrastrukturen (KRITIS) mit dem Ziel einer Bestandsaufnahme in Europa. Denn fest steht: Mehrere europäische Länder haben ähnliche Herausforderungen zu bewältigen wie Deutschland und sind bisher unterschiedlich weit gekommen. Kein europäisches Land kann jedoch vollkommen eigenständig im Bereich KRITIS agieren. Daher wäre eine komplementäre Zusammenarbeit wünschenswert. Der Workshop versucht letztlich dem Thema eine Identität zu stiften und eine Expertengemeinde in Europa zu etablieren.

Meine sehr verehrten Damen und Herren,
die Gesellschaft für Informatik ist für das BSI in den letzten Jahren ein außerordentlich wichtiger Partner geworden - mit einem intensiven Austausch auf höchster Ebene. Der Know-how-Transfer zwischen der GI und dem BSI ist für beide Seiten wichtig und dient der Förderung der IT-Sicherheit. Ich bin stolz sagen zu dürfen, dass wir mit Isabel Münch auch an prominenter Stelle vertreten sind. Sie wurde im letzten Jahr zur stellvertretenden Sprecherin des Fachbereichs Sicherheit gewählt, weil die Zusammenarbeit mit dem BSI von den übrigen Fachbereichsmitgliedern für außerordentlich wichtig erachtet wurde.

In vielen Fachgruppen des GI-Fachbereichs Sicherheit ist das BSI an den Diskussionen zur Förderung von Sicherheitsthemen aktiv beteiligt. Hierzu gehören beispielsweise Themen wie

- die Sicherheit von E-Government,
- die Erkennung und Beherrschung von Sicherheitsvorfällen (CERTs),
- Fragen zur Evaluation, Zertifizierung und Normung im Bereich Sicherheit,

- das Management von Informationssicherheit (hier spielt besonders das IT-Grundschriftbuch als eine Vorgehensweise zur Planung und Durchsetzung von Sicherheit in Behörden und Unternehmen eine zentrale Rolle).

Meine sehr verehrten Damen und Herren,

ich möchte meine Ausführungen noch einmal kurz zusammenfassen. Ich denke jedem ist klar, welche vielschichtige Verantwortung das Fachgebiet Informatik trägt. Unterscheidet man es nur in die beiden Hauptaspekte gesellschaftliche und technische Verantwortung, so heißt das: Der Diskurs um die ethischen Fragen in der Informatik ist noch längst nicht zu Ende. Er muss - im Gegenteil - noch intensiviert werden. Im Bereich der technischen Verantwortung der Informatik geht es mir in erster Linie um den Aspekt Sicherheit. Jeder Informatiker muss Sicherheit als notwendige Komponente betrachten und nicht mehr länger als Störfaktor.

Denn eines ist auch unverkennbar: Insgesamt betrachtet, steht die IT-Sicherheit anderen - klassischen - Sicherheitsfragen in nichts nach. Die Innere Sicherheit ist heute untrennbar mit sicheren IT-Infrastrukturen verbunden. Zwar ist die physische Fühlbarkeit von Schadensereignissen innerhalb der Informationstechnik natürlich eine andere als etwa bei Verkehrsunfällen, aber gerade die gesamtwirtschaftliche Bedeutung der Informationstechnik macht ihren zuverlässigen Schutz so wichtig. Es kann daher keine Innere Sicherheit ohne IT-Sicherheit geben.

Meine Damen und Herren,

für die folgenden Tage wünsche ich Ihnen allen viele neue Erkenntnisse – natürlich vor allem im Bereich IT-Sicherheit – und angeregte Diskussionen. Das Tagungsprogramm gibt Ihnen dazu ausreichend Gelegenheit.

Und in der Goethe-Stadt Frankfurt liegt es für mich nahe mit den Worten des großen Klassikers abzuschließen: „Wer sichere Schritte tun will, muss langsam gehen.“ – Dem hinzufügen möchte ich lediglich: Wir sollten uns ein wenig beeilen und in die richtige Richtung laufen.