Verletzlichkeit der Informationsgesellschaft – Überprüfung von Gestaltungsvorschlägen und Thesen von 1988

Urs Andelfinger, Volker Hammer,
Ulrich Pordesch, Alexander Roßnagel,
Roland Steidle

provet
Projektgruppe verfassungsverträgliche Technikgestaltung e.V.

Zur elektronischen Publikation im Verlag kassel university press
Kassel, Januar 2015; Version 1.0

Download: *www.provet.org/* > Publikationen > 2015

Inhalt

1 Motivation

Die "Projektgruppe verfassungsverträgliche Technikgestaltung“ (provet) führte von 1986 bis 1988 das Forschungsprojekt "Informatisierung der Gesellschaft: Verfassungsverträglichkeit und Verletzlichkeit des sozialen und politischen Systems" durch.[1] Im Untersuchungsteil „Verletzlichkeit“ war abzuschätzen, welche Schäden für das soziale und politische System der Bundesrepublik Deutschland durch Ausfall oder Missbrauch von Informations- und Kommunikationssystemen entstehen können, wenn Wunschvorstellungen einer umfassenden Informatisierung der Gesellschaft umgesetzt würden. Einerseits sollten die Ergebnisse des Projekts für das Problem der Verletzlichkeit sensibilisieren, andererseits war zu untersuchen, was zu dessen Entschärfung getan werden könnte. In diesem Sinn zielte das Projekt auf eine self-destroying Prophecy.

Die Ergebnisse des Projekts gründeten wesentlich auf einem Szenario zur Informatisierung der Gesellschaft, dessen Zeithorizont damals auf etwa 20 Jahre gewählt wurde. Basierend auf dem Szenario wurden unter anderem 10 Thesen zur künftigen Verletzlichkeit der Gesellschaft[2] und darauf abgestimmte Gestaltungsvorschläge[3] für die Entscheidungsträger in Politik und Wirtschaft entwickelt.

Nachdem der Zeithorizont der Studie inzwischen überschritten wurde, ist ein Rückblick reizvoll. Allerdings kann anders als bei gewöhnlichen Prognosen nicht gefragt werden, ob sich Vorhersagen bewahrheitet haben, denn das Ergebnis des Projekts war keine Vorhersage. Vielmehr wurden Annahmen und Wünsche einer umfassenden Informatisierung damaliger Protagonisten zu einem Szenario zusammenführt, um dessen unbeabsichtigten Nebenfolgen zu untersuchen. Gefragt werden kann aber, inwieweit das Szenario und die diesbezügliche angenommene Verletzlichkeit eingetreten sind. Und es kann gefragt werden, ob eine Gegensteuerung gegen zu viel Verletzlichkeit stattfand und welche Rolle die Gestaltungsprinzipien dabei spielten, die in unserer Studie als wesentlich herausgearbeitet wurden. Daraus lässt sich dann mittelbar auch erkennen, wie nützlich der gewählte methodische Ansatz der Technikfolgenforschung (konditionale Prognosen) und die entwickelten Gestaltungsprinzipien waren und heute sein können.

Um diesen Rückblick zu erstellen, haben Autoren der Verletzlichkeitsstudie und später zur Projektgruppe verfassungsverträgliche Technikgestaltung hinzugestoßene Wissenschaftler einen Workshop in Le Tholy durchgeführt. Dieser Workshop und darauf folgende Arbeiten und Diskussionen ergaben eine Einschätzung, die hier dokumentiert wird. Auch wenn wegen der begrenzten Ressourcen keine erneute wissenschaftliche Aufbereitung möglich war, kann das Ergebnis für mit dem Thema Befasste interessant sein. Es soll deshalb hier dokumentiert werden. Der Beitrag soll als eine kritische Rückschau verstanden werden. Gestaltungsvorschläge und Thesen im Lichte der Entwicklungen neu zu formulieren wäre dagegen Gegenstand eines eigenen Projekts.

Kapitel 2 stellt den Kontext dieses Rückblicks vor. Es gibt einen Überblick über die Begriffe, die Vorgehensweise und Ergebnisse der Verletzlichkeitsstudie, zur

1 *Roßnagel/Wedde/Hammer/Pordesch 1990b.*

2 *Roßnagel/Wedde/Hammer/Pordesch 1990b,* 208.

3 *Roßnagel/Wedde/Hammer/Pordesch 1990b,* 231.

Veränderung der politischen und gesellschaftlichen Randbedingungen seit 1988 und zur Relevanz des Themas seit 1988. In Kapitel 3 bewerten wir, ob die Thesen der Verletzlichkeitsstudie zutreffend waren. In Kapitel 4 wird untersucht, ob die Gestaltungsvorschläge praktische Relevanz hatten. Kapitel 5 fasst die Ergebnisse zusammen. Abschließend werden im Ausblick einige Forschungsfragen zur aktuellen Verletzlichkeit der Informationsgesellschaft gestellt.

2 Kontext der Überprüfung

Zum besseren Verständnis der weiteren Ausführungen werden in diesem Abschnitt die wichtigsten Begriffe für die Diskussion der Verletzlichkeit und der damalige Kontext der Thesen wie auch des heutigen Reviews kurz vorgestellt.

2.1 Begriffe

Verletzlichkeit bezeichnet im Zusammenhang der hier dargestellten Studie die Möglichkeit großer Schäden für die Gesellschaft.[4] Im Mittelpunkt der Untersuchung von 1988 standen dabei die Schadenspotentiale, die für die Gesellschaft als Ganzes relevant sind und durch den Einsatz von IuK-Technik verändert oder spezifisch hervorgerufen werden.

Unter **Verwundbarkeit** werden die Störungsmöglichkeiten für technische Systeme ohne Betrachtung der Folgen für das soziale und politische System (Schäden) verstanden. Ist zu erwarten, dass die Schäden für die Gesellschaft nur gering ausfallen, spielt die Verwundbarkeit eines IuK-Systems für die Verletzlichkeit der Gesellschaft keine Rolle. Unter einer **Störung** eines technischen Systems wird ein Ereignis oder ein Verlauf verstanden, der zu Folgen führt, die nicht dem Einsatzzweck des Systems entsprechen.[5] Aus der Bewertung der Summe aller Folgen einer Störung ergibt sich die Schadenshöhe. Die Folgen einer Störung betreffen zunächst Individuen und Organisationen, in ihren Kumulation und deren Folgen dann möglicherweise aber auch die gesamte Gesellschaft. Diese gesamtgesellschaftlichen Folgen sind gemeint, wenn hier von der Verletzlichkeit der Gesellschaft gesprochen wird.

Die **Bewertung der Schadenshöhe** einer technischen Störung ist für unterschiedliche soziale System verschieden, z. B. für eine Organisation anders als für die Gesellschaft der Bundesrepublik. Als Orientierung für den Bewertungsmaßstab bietet sich die Beeinträchtigung der Überlebensfähigkeit des betroffenen sozialen Systems an.[6] Große Schäden im Sinne der Studie von 1988 sind solche, die das soziale System der Bundesrepublik nicht oder sehr selten verkraften kann. Spätestens mehrere Schäden in dieser Größenordnung würden die Existenz der gesellschaftlichen Ordnung insgesamt bedrohen, d.h. wesentliche sozialen Funktionen, z. B. Gesundheitsversorgung, Demokratie oder Versorgung der Bevölkerung, können nur auf einer niedrigen Stufe oder nicht mehr aufrecht

4 *Roßnagel/Wedde/Hammer/Pordesch 1990b, 7. Zur qualitativen Differenzierungen der Schadenshöhe siehe Hammer 1999, 22 ff.*

5 *Roßnagel/Wedde/Hammer/Pordesch 1990b,* 8.

6 *Hammer 1999 22 ff.* Überlegungen zur Verletzlichkeit können auch für Organisationen oder für Individuen angestellt werden. Dies war aber nicht Gegenstand der Studie und wird deshalb auch hier ausgeklammert.

erhalten werden. Beispiele für Störfalle mit schweren Schäden für die Gesellschaft sind die Finanzmarktkrise oder die Erdbeben- und Atomkatastrophe in Japan. Diese haben allerdings keine unmittelbaren Ursachen im IT-Einsatz.

2.2 Vorgehensweise und Ergebnisse der Verletzlichkeitsstudie

Ausgangspunkt des Projekts waren Prognosen, Annahmen und Wünsche maßgeblicher Befürworter einer weitgehenden Informatisierung der Gesellschaft. Diese wurden zu einem im Trend liegenden Szenario verdichtet, das die Entwicklung der IuK-Technik bis 2008 und deren Einsatz in verschiedenen Bereichen von Wirtschaft und Gesellschaft beschrieb. Unter Berücksichtigung angenommener gesellschaftlicher Randbedingungen wurde dann untersucht, wie sich - ebenfalls dem Trend entsprechend - das Ausmaß möglicher Schäden und die Wahrscheinlichkeit ihres Eintritts verändern würden. Auf der Basis dieses Gedankenexperiments wurde die Verletzlichkeit der 'Informationsgesellschaft' bewertet und in zehn Thesen zusammengefasst. Im Ergebnis wurden negative Entwicklungen für die Gesellschaft erwartet, die unter anderem in sozialen Sicherungszwängen münden (siehe dazu unten die Thesen).

Zusammenfassend wurde als Ergebnis der Studie erwartet, dass die Verletzlichkeit der Gesellschaft zunimmt, wenn nicht gegengesteuert würde. Die negativen Effekte wurden jedoch nicht als unvermeidbar angesehen: IuK-Technik kann sehr vielfältig gestaltet und in vielfältigen Varianten genutzt werden. In der Studie von 1988 wurden daher 10 grundlegende Gestaltungsvorschläge für die IuK-Technik und ihren Einsatz entwickelt, die die negativen Effekte abschwächen oder sogar vermeiden sollten. Diese Empfehlungen konzentrierten sich auf Risikominderungsstrategien, die den Zwang zu sozialen Sicherungsmaßnahmen vermindern sollten. Vor allem sollten das Schadenspotential reduziert und katastrophale Schadensentwicklungen unterbunden werden.

2.3 Veränderung der politischen und gesellschaftlichen Randbedingungen seit 1988

In diesem Abschnitt werden schlaglichtartig verkürzt einige Veränderungen der politischen und gesellschaftlichen Randbedingungen seit der Veröffentlichung der Thesen und Gestaltungsvorschläge skizziert.

Der Kontext für die Thesen und Gestaltungsvorschläge wird bestimmt durch die gesellschaftlichen und politischen Randbedingungen der Jahre 1986 – 1988 und damit der Zeit, in der es (welt)politisch noch zwei deutsche Staaten gab und technologiepolitisch u.a.: noch das Quasi-Monopol der Deutschen Bundespost. Eckpfeiler dieser Art gaben der damaligen Welt klare Orientierungspunkte.

Die seitdem in vielen gesellschaftlichen Bereichen eingetretenen und auch gezielt eingeführten De-Regulierungen, die generelle gesellschaftliche Durch-Öko-

nomisierung und die weltpolitischen Umwälzungen haben zu wesentlich veränderten Rahmenbedingungen geführt. Hinzu kam u. a. eine gewaltige Pluralisierung von Wertevorstellungen. Die wichtigsten Veränderungen von Randbedingungen lassen sich dabei als drei Trends konstatieren:

(1) Der Vorrang der ökonomischen Betrachtungsweise in inzwischen fast allen Lebensbereichen hat sich in einer beispiellosen und zum Zeitpunkt der Erstellung der Thesen unerwarteten Weise durchgesetzt. Dazu gehören im Infrastrukturbereich beispielsweise neben der bereits in der Vergangenheit weitgehend privatwirtschaftlich organisierten Energiewirtschaft auch die umfassende De-Regulierung des Telekommunikationssektors oder die Versuche, die Deutsche Bahn zu privatisieren.[7] Die Globalisierung durch verteilte, flexible Produktionskapazitäten und vielfältige Logistikketten führen sowohl zu sehr hoher internationaler Konkurrenz als auch zur engen Verflechtung von Produktionsprozessen. Die Ökonomisierung führt zu erheblichem Druck auf die Marktteilnehmer, effiziente Produktionsmethoden einzusetzen und befördert damit auch die Informatisierung von Produktions- und Vertriebsprozessen. Das Weltfinanzsystem ohne einheitliche Regulierung, Spekulationsmöglichkeiten in Milliardenhöhe und defizitäre Staatshaushalte können sogar auch die wirtschaftliche und politische Stabilität westlicher Demokratien gefährden, wie die weltweiten Finanzkrisen seit 2008 zeigen.

(2) Die quasi-monopolistische Bundespost-Ära wurde in nicht absehbarer Weise durch private Netzbetreiber, vielfältige Netzdienstleistungen und die flächendeckende Einführung von Mobilfunknetzen zusätzlich zur leitungsgebundenen Telekommunikation abgelöst. Diese Entwicklungen haben zu einer ‚Pluralisierung' technischer und infrastruktureller Möglichkeiten geführt. Damit wurde indirekt auch die flächendeckende Nutzung des Internets möglich.

(3) Schließlich hat die Durchdringung praktisch aller gesellschaftlichen Lebensbereiche mit IuK-Anwendungen die Informatisierung der Gesellschaft ebenfalls in einem nicht erwarteten Ausmaß geprägt. Neben der klassischen Telekommunikation bestehen vielfältige neue Nutzungsformen der allgegenwärtigen IuK-Infrastrukturen, allen voran das Internet mit seinen Suchmaschinen, Portalen und sozialen Netzwerken. Die Anwendungsgebiete wurden vom beruflichen und öffentlichen Sektor in praktisch alle privaten Lebensbereiche verbreitert, nicht zuletzt durch E-Mail, Customer Self Services und Online-Handel. Die Computerisierung und Vernetzung der verschiedensten Maschinen und Gebrauchsgegenstände zum ‚Netz der Dinge' ist eine der aktuellen Visionen und wird auf der Anwendungsebene zu einer weiteren Durchdringung aller Lebensbereiche mit IuK-Technologien führen.

Im Kontext der Überprüfung der Thesen und Gestaltungsvorschläge zur Verletzlichkeit ist insbesondere das Verhältnis zwischen der Pluralisierung der IuK-Infrastrukturen (2) und der allgegenwärtigen Durchdringung praktisch aller gesellschaftlichen Bereiche mit IuK (3) interessant. Es zeigt gegenläufige Entwicklungen zwischen möglicher Entschärfung der technischen Verwundbarkeit auf der Infrastrukturebene und einer möglichen Verschärfung der Verletzlichkeit auf der

[7] Lediglich die Wasserversorgung und Abwasserentsorgung wird nach wie vor im Wesentlichen von den Kommunen verantwortet.

Anwendungsebene. So könnte ein lokaler Ausfall einer IuK-Infrastruktur, z.B. Telefon oder kabelgebundenes Internet, beispielsweise partiell durch den Wechsel auf z.B. mobilen Internetzugang ersetzt werden, was die technische Verwundbarkeit etwas begrenzt. Die flächendeckende und mobile Verfügbarkeit von Kommunikationsinfrastrukturen hat aber auf der Anwendungsebene dazu geführt, dass praktisch alle Lebensbereiche inzwischen von der jederzeitigen Verfügbarkeit und korrekten Funktionsfähigkeit von IuK-Anwendungen abhängig sind. Schlagworte wie ‚Social Web' zeugen auch umgangssprachlich davon, dass wir die Informatisierung unserer Gesellschaft inzwischen weitgehend als gegeben hinnehmen: die Anwendungen des Web führen zu neuen Möglichkeiten des Sozialen. Die gesellschaftliche Verletzlichkeit, d.h. die Möglichkeit von großen Schäden durch Ausfall der auf diese Infrastrukturen angewiesenen Anwendungen, hat daher zugenommen.

2.4 Relevanz des Themas seit 1988

Die Verletzlichkeitsstudie von provet war nicht die einzige Untersuchung zur Verletzlichkeit der Informationsgesellschaft. Etwa 10 Jahre vorher legte das schwedische 'Verwundbarkeits-Komitees' (SARK) die Studie "Datenverarbeitung und die Verwundbarkeit der Gesellschaft" vor.[8] Seit Ende der 90er Jahre analysieren staatliche Stellen in verschiedenen Ländern verstärkt die Verletzlichkeit durch IT-Infrastrukturen oder versuchen, steuernd Einfluss zu nehmen.[9]

In Deutschland ließ das Bundesamt für Sicherheit in der Informationstechnik (BSI) 2002 im Rahmen des Anti-Terror-Programms der Bundesregierung vor dem Hintergrund der zunehmenden IT-Nutzung und IT-Abhängigkeiten sieben Studien zu „Kritischen IT-Infrastrukturen" für verschiedene Infrastruktursektoren erstellen.[10] Im Rahmen der Initiativen der Bundesregierung werden unter dem Titel „Schutz kritischer Infrastrukturen" verschiedene Ansätze verfolgt, die auch die Verletzlichkeit der informatisierten Gesellschaft beeinflussen können. *„Um einen umfassenden Schutz der Informationsinfrastrukturen in Deutschland sicherzustellen, gibt die Bundesregierung mit dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen" drei strategische Ziele vor:*

- *Prävention: Informationsinfrastrukturen angemessen schützen*
- *Reaktion: Wirkungsvoll bei IT-Sicherheitsvorfällen handeln*
- *Nachhaltigkeit: Deutsche IT-Sicherheitskompetenz stärken – international Standards setzen"*[11]

8 *SARK 1979.*

9 Siehe zu einer Übersicht *BSI 2008.*

10 Die Infrastrukturbereiche waren: (1) Telekommunikation und IT, (2) Energie, (3) Finanz- und Versicherungswesen, (4) Transport- und Verkehrswesen, (5) Gesundheitswesen, (6) Notfall- und Rettungswesen und (7) Behörden und Verwaltung. Die Projektergebnisse sind vertraulich.

11 Aus BMI 2005, 6.

In der *Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)*[12] werden vier technische Basisinfrastrukturen und fünf sozioökonomische Dienstleistungsinfrastrukturen genannt. In einer kurz gefassten Bilanz des BMI in diesem Dokument[13] wird festgestellt, dass *„mit dem IT-Grundschutz für die Informationsinfrastrukturen, mit dem Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) sowie dem darauf aufbauenden Umsetzungsplan KRITIS (UP KRITIS) ... wichtige Konzepte und konkrete Maßnahmen erarbeitet worden"* seien, die gemeinschaftlich mit der Wirtschaft umgesetzt würden.[14] Eingeführt worden sei auch der vorbeugende personelle Sabotageschutz, zu dem bestimmte öffentliche und nicht öffentliche Einrichtungen verpflichtet sind.[15] Auch nehme die Versorgungssicherheit im Sinne einer Ausfallsicherheit etwa im Bereich der Stromversorgung im Vergleich zu anderen Staaten einen der oberen Plätze ein. Die Energieversorgungsunternehmen wie auch die TK-Diensteanbieter seien durch gesetzliche Regelungen zu Sicherheitsmaßnahmen verpflichtet. Zu anderen Infrastrukturbereichen wird allerdings keine Aussage getroffen. Es wird auch festgestellt, dass die Leistungen der Infrastrukturen in der Mehrheit durch private oder kürzlich privatisierte (!) Unternehmen bereitgestellt werden.[16]

Technische Basisinfrastrukturen	**Sozioökonomische Dienstleistungsinfrastrukturen**
Energieversorgung	Gesundheitswesen, Ernährung
Informations- und Kommunikationstechnologie	Notfall- und Rettungswesen, Katastrophenschutz
Transport und Verkehr	Parlament, Regierung, öffentliche Verwaltung, Justizeinrichtungen
(Trink-)Wasserversorgung und Abwasserentsorgung	Finanz- und Versicherungswesen
	Medien und Kulturgüter

Tabelle 1: Kritische Infrastrukturen (nach BMI 2009)

Das BMI stellt außerdem fest, dass sich durch hohe Sicherheitsstandards und eine hohe Versorgungssicherheit ein trügerisches Gefühl von Sicherheit entwickelt und daher die Auswirkungen eines „Dennoch-Störfalls" überproportional hoch seien. Dies wird vom BMI als Verletzlichkeitsparadoxon bezeichnet, das sich kontinuierlich verstärke: *„In dem Maße, in dem ein Land in seinen Versorgungsleistungen weniger störanfällig ist, wirkt sich jede Störung umso stärker aus."*[17] Das BMI kommt in dem Dokument zu dem Schluss, dass Verletzlichkeitsüberlegungen auch in der Technikfolgenabschätzung weiter an Bedeutung gewinnen sollten.[18]

12 BMI 2009.

13 BMI 2009, 3 ff.

14 BMI 2009, 4.

15 S. Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz - SÜG) vom 20.4.1994.

16 BMI 2009, 6.

17 BMI 2009, 8

18 BMI 2009, 8

Das „Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag“ (TAB) führte 2009 eine Studie zur „Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung“ durch,[19] in der auch die Aufrechterhaltung der Kommunikationswege untersuchte wurde. Nach dem „Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen“[20] sollen Prävention, Reaktion und Nachhaltigkeit für die Informationsinfrastrukturen in Zusammenarbeit zwischen dem Bund und den Unternehmen, die die Infrastrukturleistungen erbringen, gesichert werden. Inzwischen wird an einem ersten IT-Sicherheitsgesetz gearbeitet.

Zusammenfassend kann festgestellt werden, dass die vor 25 Jahren in der provet-Studie analysierten Probleme der Verletzlichkeit in der Wirtschaft und Verwaltung allgemein akzeptiert sind und vielfältige Aktivitäten auslösten. Allerdings hat der Staat im Bereich der IuK-Technologien, insbesondere der Kommunikationsinfrastruktur, durch die Privatisierung Steuerungsmöglichkeiten aus der Hand gegeben. Im Zuge der Globalisierung und Liberalisierung der Wirtschaft sind außerdem generell die Einflussmöglichkeiten des Staates auf die wirtschaftliche und technologische wie auch soziale Entwicklung zurückgegangen. Es müsste also vermutlich rereguliert werden, um überhaupt wieder Einflussmöglichkeiten in Hinblick auf eine Verringerung der Verletzlichkeit der Gesellschaft zu gewinnen.

3 Bewertung der Thesen

Aus der konditionalen Prognose ergaben sich negative Erwartungen an die Entwicklung der Verletzlichkeit der Informationsgesellschaft. Es wurde erwartet, dass die Verletzlichkeit durch die weitere Durchdringung der Gesellschaft mit Informationstechnik wächst. Diese Erwartungen wurden zusammenfassend in 10 Thesen formuliert. In diesem Kapitel wird untersucht, ob diese Thesen zutreffend waren.

Wir stellen in je einem eigenen Abschnitt die These aus der Studie von 1988 voran (grau unterlegt). Für jede These werden dann Indizien für oder gegen ihre Gültigkeit dargestellt. Diese werden in jeweils einem Bewertungsergebnis für die Gültigkeit zusammengefasst.

Die Darstellung beruht – wie oben schon angedeutet – nicht auf einer umfassenden wissenschaftlichen Untersuchung. Hierfür fehlten die notwendigen Ressourcen. Vielmehr geben wir hier unsere Einschätzung in Form von Anmerkungen zu den damaligen Thesen wieder. Dies hilft einzuschätzen, wie geeignet die damals gewählte Methodik der Technikfolgenabschätzung war und noch heute sein könnte.

19 http://www.tab.fzk.de/de/projekt/skizze/stromausfall.htm (Stand: 29.09.2009)

20 BMI a.

(1) Ansteigende Verletzlichkeit

1. Die Verletzlichkeit der Gesellschaft wird künftig ansteigen und zu einem zentralen Problem der 'Informationsgesellschaft' werden.

Der wachsenden Bedeutung dieses Problems ist bisher keine gebührende Beachtung geschenkt worden - weder in den Zukunftsplanungen der Entscheidungsträger noch in der öffentlichen Diskussion. Wie sehr die Verletzlichkeit ansteigt, hängt sehr stark ab von politischen Gestaltungsentscheidungen.

Einschätzung der Gültigkeit

In den letzten 25 Jahren konnten keine Schadensereignisse mit schweren Schäden für die Gesellschaft beobachtet werden, die durch Störungen in der Informations- und Kommunikationstechnik ausgelöst wurden. Es gab zwar eine Vielzahl öffentlichkeitswirksamer Ereignisse im Zusammenhang mit IT-Störungen oder -Angriffen. Deren Schäden erreichten aus gesellschaftlicher Perspektive aber kein hohes Schadensniveau. Hohe Schäden für eine oder mehrere Nationen wurden dagegen beispielsweise durch Umwelteinflüsse (Hochwasser 2002 und 2013 in den östlichen Bundesländern und Polen), physische Gewalt (Terroranschläge vom 11. September 2001 mit mehr als 3000 Toten) und Wirtschaftsschäden in Höhe vieler Milliarden Euro oder die Finanzmarktkrise ab 2007 ausgelöst.

Politisch wird gelegentlich versucht, Monopole zu begrenzen, z. B. durch EU Wettbewerbsverfahren wie im Falle Microsoft. In manchen Fällen könnten solche Bestrebungen auch zu verletzlichkeitsreduzierenden Nebeneffekten führen.[21] Beispiele sind die Privatisierung und Regulierung des Telekommunikationssektors, die (vorsichtige) Aufteilung der Bahn in eigenständige Bereiche und die unternehmerische Trennung von Energieerzeugung und Verteilnetzen. Wesentlicher Treiber für diese Einflussnahmen waren und sind ökonomische Gründe und nicht Aspekte der Verletzlichkeit. Insgesamt hat der Staat aber Einflussmöglichkeiten aufgegeben. Während er in den 80er Jahren noch der Betreiber der nationalen Infrastrukturen war, sind diese inzwischen weitgehend privatisiert. Die Politik setzt jetzt nur noch die Rahmenbedingungen für die unternehmerischen Entscheidungen.

Die politischen Handlungsspielräume sind dafür aber z. B. durch die Internationalisierung ohne damit einhergehende internationale Regelungen, die Begrenzung des Einflusses auf Unternehmen und die De-Regulierung von Infrastrukturen gegenüber 1988 eingeschränkt. Die politischen Steuerungsmöglichkeiten wurden durch die gewachsene Globalisierung begrenzt, sowohl durch ein geringeres Gewicht der Politik gegenüber großen internationalen Konzernen als auch durch die geringeren Handlungsspielräume von Unternehmen durch den gestiegenen internationalen Konkurrenzdruck.

Die Automatisierungsanstrengungen in Wirtschaft und Verwaltung, der konsequente Einsatz des Internets und die genannten Rahmenbedingungen führten zur Ausweitung und zu veränderten Strukturen des IT-Einsatzes. IuK-Systeme

[21] Dem liegt die Annahme zu Grunde, dass zum einen Störungen bei Monopolisten weitreichender sein können als bei aufgeteilten Märkten und zum anderen IT-Unternehmen mit Monopolstellung selbst weitreichende Störungen gezielt auslösen könnten.

dürften enger gekoppelt und komplexer verknüpft sein, als dies 1988 der Fall war. So werden z. B. Substitutionsmöglichkeiten durch manuelle Prozesse nur noch in wenigen Störfallszenarien anwendbar sein.

Bewertungsergebnis

Auch wenn in den vergangenen Jahren keine Störfälle mit schweren Schäden für die Gesellschaft aufgetreten sind, ist die Abhängigkeit von IuK-Technik gewachsen. Es ist dabei zugleich eine Verbreiterung der Abhängigkeit von der IuK-Infrastruktur auf die IuK-Anwendungsebene zu beobachten. So ist durch die generelle ‚Informatisierung' der Gesellschaft eine Verbreiterung der Abhängigkeit von wenigen zentralen Anwendungen hin zu einer Abhängigkeit von vielen kleineren Anwendungen eingetreten, die jedoch in der Summe ebenfalls relevant sein dürfte.

Wenn überhaupt, dann wurden politische Gestaltungsmöglichkeiten nur in engem Rahmen genutzt. Die Steuerungsmöglichkeiten der Politik sind gegenüber 1988 geringer geworden.

Die Abhängigkeit von IuK-Technik wird an einzelnen Störfällen immer wieder sichtbar. Inzwischen wird das Problem auch stärker in Politik und Verwaltung erkannt. Insofern traf die These zu. Allerdings kann man nicht davon sprechen, dass die Verletzlichkeit in der Wahrnehmung der Öffentlichkeit das zentrale Problem der (‚Informations-)Gesellschaft' darstellen würde. Maßnahmen zur Begrenzung der gesellschaftlichen Verletzlichkeit dürften dementsprechend in Unternehmen, Verwaltung und Politik mit eher geringer, zumindest aber mit sehr unterschiedlicher Priorität behandelt und ergriffen werden.

(2) Veränderte Struktur der Verletzlichkeit

Die Struktur der Verletzlichkeit wird sich im Tatsächlichen wie im Wissen gegenüber heute verändern.

> *Während die Chancen steigen, Fehler zu vermeiden und Missbrauchsaktionen zu verhindern, wird sich das Ausmaß der Schäden für den Fall, dass ein IuK-System dennoch ausfällt oder nicht korrekt funktioniert, deutlich erhöhen. Eine ebenso disparate Entwicklung zeichnet sich für das Wissen über die beiden Faktoren der Verletzlichkeit ab. Während das Ausmaß möglicher Schäden weitgehend bekannt ist, lassen sich viele Faktoren, die die Wahrscheinlichkeit solcher Schäden bestimmen, schwer oder gar nicht einschätzen - etwa Fehlermöglichkeiten in komplexen Systemen, Störungen durch die elektronische 'Umweltverschmutzung', neue Softwareangriffe oder kollektive Aktionen. Soweit die Wahrscheinlichkeit von Schäden unbekannt ist, kann die Verletzlichkeit der Gesellschaft nur nach dem Schadenspotential einer Technikanwendung bewertet werden.*

Einschätzung der Gültigkeit

Der Wettlauf zwischen den Angreifern, insbesondere im Internet, und den Verteidigern in den Rechenzentren wird auf absehbare Zeit kein Ende finden. Die zunehmende Automatisierung von Angriffen (z. B. Toolkits für Viren und Trojaner, Bot-Netze), die Grenzen der Usability von Sicherheitsmaßnahmen (z. B. Verständlichkeit von Zertifikatprüfungen für normale Benutzer, Notwendigkeit zusätzlicher Komponenten wie Smartcards und Chipkartenleser oder umständli-

chere Verfahren bei der “m-TAN“) und immer neue Systeme mit weiter wachsender Komplexität führen dazu, dass die Wahrscheinlichkeit von Störungen kaum sinken dürfte. Auch andere Faktoren für die Bewertung der Wahrscheinlichkeit von Störungen, wie die Motivlagen, das Bestimmen und Abgrenzen von potentiellen Angreifergruppen, die Bewertung des erreichten tatsächlichen Sicherheitsniveaus oder die Fehleranfälligkeit von Systemen unterliegen weiter großer Unsicherheit. Trends wie ‚Cyber-War’ nutzen jedoch offensichtlich zunehmend den Wettlauf zwischen Angreifern und Verteidigern strategisch aus, um beispielsweise militär- oder wirtschaftspolitische Zielsetzungen ohne unmittelbare physische Gewalt zu verfolgen. So wird der Stuxnet-Angriff auf Steuersoftware von Siemens im September 2010 nach übereinstimmenden Presseberichten eindeutig in den Bereich des ‚Cyber-Wars’ eingeordnet, auch wenn nicht ganz geklärt ist, ob es hier um Militärpolitik oder um Wirtschaftskriminalität geht.[22]

Für Schadenspotentiale können zwar einfache Annahmen getroffen werden, vielfach sind die Abhängigkeiten und damit auch konkrete Störungsverläufe nicht wirklich abschätzbar. Globale Szenarien, z. B. für den Ausfall der Stromversorgung, können entwickelt werden. Die Folgen von IT-Abhängigkeiten lassen sich aber schwerer bewerten.

Keine Verminderung, aber wesentliche Änderungen in der Struktur der Verletzlichkeit werden sich durch das Cloud Computing ergeben. Z. B. könnte die Wahrscheinlichkeit von Datenverlusten durch die Möglichkeit, Daten in die Cloud zu duplizieren und weltweit zu verteilen, vermindert werden. Dagegen könnten die Missbrauchsrisiken für die ausgelagerten Daten eben aus diesen Gründen deutlich zunehmen. Abnehmen werden außerdem die Transparenz von Datenverarbeitungsprozessen, insbesondere im Fall von Web-Anwendungen und für die Orte der Datenspeicherung, sowie die Möglichkeiten, Sicherheitsvorkehrungen zu prüfen.

Bewertungsergebnis

Die Verletzlichkeit hat sich strukturell verändert. Allerdings haben wir den Eindruck, dass sich die Wahrscheinlichkeit von Störungen nicht verringert hat. Eine wesentliche Änderung ergibt sich daraus, dass die Schadenpotentiale intransparenter werden. Die These trifft bedingt zu.

(3) Praktische Grenzen des Sicherheitsniveaus

Das Sicherungsniveau könnte sehr hoch sein, wird in der Praxis aber deutlich unter den theoretischen Möglichkeiten liegen.

Die IuK-Technik selbst bietet zusammen mit gezielten organisatorischen Maßnahmen theoretisch viele Möglichkeiten, die Verletzlichkeit zu verringern. Wenn für alle schadensträchtigen Anwendungen das jeweils optimale Konzept zur Reduzierung des Schadenspotentials und zur Sicherung gegen Missbrauch und Versagen des Technik-Systems realisiert würde, wäre ein hohes Sicherheitsniveau[23] trotz zunehmender Nutzung der IuK-Technik zu erreichen. In der breiten Anwendung erfährt jedoch jedes Sicherungskonzept Abstriche

22 Vgl. hierzu z.B. http://www.heise.de/security/meldung/Stuxnet-Wurm-weitere-Tricks-im-Cyberwar-1098197.html

23 *Roßnagel/Wedde/Hammer/Pordesch 1990b* stellt in der These auf S. 209 auf ein „hohes Schadensniveau“ ab, was im Kontext dieser These falsch ist und wenig Sinn ergäbe. Richtig ist dagegen "Sicherheitsniveau".

durch wirtschaftliche Überlegungen, organisatorische Schwierigkeiten, Interessen der inneren Sicherheit und den Widerstand der von ihm Betroffenen. Die Verlässlichkeit des Sicherungssystems wird folglich immer gefährdet sein, weil es weder das stets fehlerfreie Funktionieren der mit Sicherheitsaufgaben betrauten Personen noch die soziale und politische Stabilität, die es voraussetzt, sicherstellen kann.

Einschätzung der Gültigkeit

Organisationen als Betreiber von IT-Systemen treiben unterschiedlichen Aufwand, um ihre Systeme abzusichern. Dementsprechend werden auch sehr unterschiedliche Sicherheitsniveaus erreicht.

Die tägliche Erfahrung als IT-Sicherheitsbeauftragter oder IT-Sicherheitsexperte bestätigt diese These. Dabei spielen jedoch neben technischen Aspekten oft auch organisatorische Unzulänglichkeiten eine wesentliche Rolle. So sind oft auch Budgetknappheit oder unklare organisatorische Verantwortlichkeiten dafür verantwortlich, dass IT-Systeme unterhalb der Grenzen eines angemessenen Sicherungsniveaus genutzt werden. Der Reibungsverlust zwischen technischer Dynamik und der Notwendigkeit, für viele Technologien vor einem betrieblichen Einsatz von Sicherheitssystemen mit Beschäftigtenvertretern Betriebsvereinbarungen abzuschließen, kann ebenfalls bessere Sicherheitsmaßnahmen verzögern. Oft bestehen auch widersprüchliche Anforderungen, beispielsweise die Vorgabe viele verschiedene und komplexe Passworte zu verwenden, diese häufig zu wechseln, aber diese Passworte irgendwo zu notieren.

Im privaten Bereich wird die Gültigkeit der These ebenfalls bestätigt. Von privaten Anwendern ohne Spezial-Know-How kann auf Grund der Komplexität der Zusammenhänge und der Zielkonflikte zwischen verfügbarer Zeit, Handhabbarkeit, Kosten und Sicherheitsmaßnahmen bei realistischer Einschätzung höchstens ein Basis-Sicherheitsniveau erwartet werden. In der Folge stehen Angreifern über Bot-Netze umfangreiche Ressourcen zur Verfügung, die sie für ihre Zwecke einsetzen können.

Vorfälle in der Praxis zeigen, dass auch schwere Störungen für Organisationen immer wieder auftreten. Die Ursachen liegen gleichermaßen in der Komplexität der Systeme und des Betriebs, beispielsweise der Notwendigkeit ein kontinuierliches Projektmanagement zu betreiben und gleichzeitig die betriebliche Stabilität der Systeme und ihres Zusammenwirkens sicherzustellen. Beispiele für schwere Störfälle sind der Ausfall der Erreichbarkeit vieler T-Mobile-Kunden im April 2009 für mehrere Stunden[24]) oder im Januar 2010 konnten 1/3 der ec-Karten wegen eines Fehlers nur eingeschränkt an Bargeld-Automaten eingesetzt werden. Sie liegen aber auch in den inhärenten Grenzen von Sicherungsmaßnahmen oder einfach darin, dass mögliche Sicherungsmaßnahmen unzureichend genutzt werden. So konnten im Juli 2011 Hacker bei einem Dienstleister des Pentagon 24.000 Dokumente kopieren und Sony war seit April 2011 mehrfach Ziel erfolgreicher Attacken, in denen u. a. große Mengen von Kreditkartendaten ausgeforscht wurden.

[24] Durch eine Störung in zwei von drei Home Location Registern konnten viele Kunden von T-Mobile nicht angerufen werden und selbst nicht telefonieren.

Bewertungsergebnis

Die These wird von der Situation der IT bis 2014 bestätigt.

(4) Lücken in Sicherungssystemen

Die Sicherungssysteme werden sich sehr unterschiedlich entwickeln und immer wieder Lücken aufweisen.

Die begrenzte Wirksamkeit, kontraproduktive Effekte und organisatorische Koordinationsschwierigkeiten von Sicherungsmaßnahmen lassen immer wieder Sicherungslücken entstehen. Während sich Missbrauchsmotive und Aktionsformen dynamisch entwickeln, ist das Abwehrsystem durch seine technische und organisatorische Verfestigung eher statisch. Es wird immer wieder Angriffen ausgesetzt sein, die neu sind und auf die es nicht vorbereitet ist.

Wenigen gut gesicherten werden viele unzureichend geschützte Anwendungen gegenüberstehen. Viele Sicherungsmaßnahmen dürften sich nur langsam durchsetzen. Neben modernsten Sicherungs- und Sicherheitssystemen werden auch ältere, längst überholte Konzepte zu finden sein. Zwischen den Sicherungssystemen von Großbetrieben oder wichtigen Verwaltungen und denjenigen von Klein- und Mittelbetrieben oder weniger finanzstarken Behörden wird eine große Effektivitätskluft entstehen.

Einschätzung der Gültigkeit

Beispiele für Lücken in Sicherungssystemen gibt es zahlreiche – in großen Unternehmen und viel mehr noch in KMU. Unterschiedliche Sicherheitsniveaus in Unternehmen zeigten sich z. B. an der Umstellung von Betriebssystemgenerationen. Während einige Unternehmen bereits das als sicherer bewertete Windows 8 und auch noch Windows 7 einsetzten, verharrten andere noch beim Einsatz von Windows XP. Entsprechendes gilt für Server, Sicherheitssysteme und das Patch-Management.

Viele Web-Anwendungen werden ebenfalls nicht unter Sicherheitsgesichtspunkten entwickelt. In der Praxis treten immer wieder die gleichen Lücken auf.[25] Dabei haben KMUs sehr große Hürden, überhaupt Ressourcen für sichere Softwareeinzusetzen.

Bewertungsergebnis

Die These wird von der Situation der IT 2014 voll bestätigt – zum einen aufgrund der aktuellen technologischen Dynamik und zum anderen aufgrund der immer komplexer werdenden ‚sozio-technischen Gesamtsysteme', die eigentlich zu sichern wären.

25 Siehe dazu z.B. die Top 10 des Open Web Application Security Projects (OWASP): *https://www.owasp.org/images/b/b8/OWASPTop10_DE_Version_1_0.pdf* (Abfrage: 13.09.2014).

(5) Zunahme von Missbrauchsmotiven

Zahl und Intensität der Missbrauchsmotive nehmen überproportional zu.

Künftig werden nicht nur alle Varianten aus dem breiten Spektrum bisheriger Missbrauchsmotive entsprechend dem Anstieg von IuK-Anwendungen vermehrt zu finden sein, sondern außerdem zusätzliche spezifisch durch die IuK-Technik hervorgerufene Missbrauchsmotive entstehen. IuK-Technik wird das wirtschaftliche, gesellschaftliche, politische und private Leben nachhaltig verändern - und dabei nicht allen Menschen lediglich Vorteile bringen. Zerstörung überkommener Lebensformen, wirtschaftlicher Abstieg, berufliche Dequalifizierung, erzwungene Anpassungsleistungen und andere Benachteiligungen bringen neue Missbrauchsmotive hervor. Zusätzlich zu den bekannten Motiven werden IuK-Systeme auch zu Objekten von Agressionen. Die IuK-Technik bleibt damit nicht - wie bisher - vorrangig Mittel zur Erreichung eines Missbrauchszwecks, sondern wird künftig auch primäres Ziel von Aktionen.

Einschätzung der Gültigkeit

Die Annahme, dass dequalifizierte Menschen politischen Widerstand gegen den Einsatz von Informationstechnik leisten, bestätigt sich bisher nicht.

Allerdings werden IuK-Systeme von verschiedene Gruppen in der Gesellschaft genutzt, um politisch Druck auszuüben und politische Veränderungen zu erzielen. Beispiele hierfür sind die Veröffentlichungen geheimer Dokumente über Wikileaks oder aktuell zunehmend die Nutzung sozialer Netzwerke zur Organisation von Protest.

Die Zahl der wirtschaftlich motivierten Angriffe ist hingegen unerwartet weit und überproportional gegenüber anderen Motiven gestiegen. Die Angriffe können durch die automatisierte Erstellung von Angriffstools vergleichsweise leicht durchgeführt werden. „Unterstützung“ für solche Aktionen wird kommerziell angeboten.

Ursache für die starke Steigerung wirtschaftlicher Motive ist u.a. dass über IuK-Systeme immer mehr auch Geschäfte abgewickelt werden. Dieser Trend war in der Studie erwartet, in seiner Bedeutung jedoch nicht ausreichend gewürdigt worden. Damals nicht absehbar war auch die aus der Auflösung der politischen Systemblöcke und der Ost-West-Konfrontation resultierende Zunahme der Wirtschaftsspionage. Für eine Bewertung der daraus motivierten Aktionen fehlt allerdings belastbares Material.

Die Erwartung, dass IT-Systeme zunehmend nicht nur als Mittel für Aktionen von Angreifern eingesetzt werden, sondern primäres Ziel solcher Aktionen sind, hat sich bisher noch nicht bestätigt. Die üblichen Denial-of-Service-Aktionen gegen Webauftritte oder andere Dienste von Organisationen zielen in der Regel nicht auf die IT als solche, sondern sollen Öffentlichkeitswirkung gegen die Organisation erreichen. Inwieweit durch erste direkte Angriffe auf IT-Systeme und deren Funktionalitäten, wie z. B. Stuxnet im September 2010 auf die Funktionalität von SCADA-Systemen, hier eine Trendwende in Richtung unserer früheren Annahmen vorliegt, muss noch abgewartet werden. Szenarien unter der Bezeichnung ‚Cyber-Warfare’, wonach IT-Systeme aufgrund ihrer vitalen Bedeutung für alle

Industriestaaten zunehmend gezielt das nächste systematische Gebiet der militärischen Kriegsführung werden könnten, deuten jedoch durchaus in diese Richtung.[26]

Die Bedrohung von IT-Einrichtungen durch Terroristen scheint derzeit auch weniger relevant, als dies in der Studie angenommen wurde. Dies ist vermutlich darauf zurückzuführen, dass im Vergleich zu Bombenanschlägen gegen Menschen die Öffentlichkeitswirkung von IT-Störungen relativ gering ist.

Bewertungsergebnis

Die These, dass Zahl und Intensität der Motive zum Missbrauch der IuK-Technik überproportional zunehmen würde, wurde bis heute nicht bestätigt. In Bezug auf die IuK-Technologie kommen heute wie früher insbesondere wirtschaftliche Motive zum Tragen. Eine überproportionale Zunahme kann aber nicht festgestellt werden.

Angenommene politische Motive für unmittelbare Angriffe auf technische Systeme und Infrastrukturen gibt es zwar tatsächlich, jedoch haben sich die Angreifer andere Ziele gesucht als die Informations- und Kommunikationstechnologie.

(6) Keine Sicherheit vor Insidern und Angriffen mit Malware

Während die Erfolgswahrscheinlichkeit von Angriffen einzelner Externer erheblich reduziert werden kann, wird es keine ausreichende Sicherheit gegen Missbrauchsaktionen von Insidern geben. Insbesondere gegen die Angriffsformen des 21. Jahrhunderts sind keine zuverlässigen Sicherungen in Sicht.

Angriffsformen des 19. und 20. Jahrhunderts, wie Bomben- oder Brandanschläge, können durch Sicherungsmaßnahmen erheblich erschwert und durch Ersatzrechenzentren und Sicherungskopien in ihrer Wirksamkeit begrenzt werden. Dadurch werden Zerstörungsaktionen auf weniger gut gesicherte IuK-Systeme abgedrängt. Auch die Chancen für das Eindringen Externer oder nichtprivilegierter Benutzer in ein Computersystem können reduziert werden. Dagegen ist noch nicht abzusehen, wie gegen den Missbrauch durch privilegierte Insider ausreichende Sicherheit gewährleistet werden könnte, die gerade aufgrund ihrer umfassenden Aufgaben und Funktionen weitreichende Schäden verursachen können. Insbesondere für sie bietet die IuK-Technik neue, effektive Formen der Sabotage und Spionage, des Betrugs und der Untreue. Sie erst hat die Möglichkeit geschaffen, mit Hilfe von Trojanischen Pferden, Viren, Würmern, Falltüren und logischen Bomben die IuK-Technik mit ihren eigenen Mitteln anzugreifen.

Sicherungssysteme sind in der Regel gegen einen, selten gegen mehrere Angreifer konzipiert. Sie setzen das sozialkonforme Verhalten aller übrigen Beteiligten voraus. Schon das Zusammenwirken von zwei Angreifern setzt viele Sicherungsmaßnahmen außer Kraft. Kaum oder keinen Schutz vermögen sie zu bieten, wenn viele Angreifer koordiniert vorgehen oder in gesellschaftlichen Konfliktsituationen ein sozialkonformes Verhalten nicht mehr erwartet werden kann.

[26] Quelle z.B.: *http://en.wikipedia.org/wiki/Cyberwarfare* mit einer Zusammenstellung von Fallbeispielen von ‚Cyberwarfare"

Einschätzung der Gültigkeit

Die Annahme, dass Externe von Angriffsmöglichkeiten weitgehend ausgegrenzt werden könnten, muss zumindest teilweise revidiert werden. Durch die intensivere Vernetzung und den Einsatz des Internets bestehen nach wie vor große Probleme bei der konsequenten Absicherung von Systemen gegenüber externen Angreifern. Die Zahl der kritischen Fehler in Betriebssystemen und Applikationen, die Schwierigkeiten eines konsequenten Patch-Managements und unbeabsichtigte Aktionen von Anwendern führen immer wieder zu Lücken, die von externen Angreifern ausgenutzt werden können. Die auf Unternehmensportalen immer häufiger eingesetzten Webapplikationen sind oft unzureichend qualitätsgesichert und schlecht geschützt. Sie ermöglichen Angreifern beispielsweise den unberechtigten Zugriff, die Änderung oder Löschung von Daten, z. B. über SQL-Injection.

Viren und Trojaner haben bereits Millionen Rechnern befallen und dadurch Schäden in Milliarden-Höhe verursacht. Dennoch wurden bisher noch keine schweren Schäden für die Gesellschaft – im Sinne der Definition der Verletzlichkeit – realisiert. Das Potential für entsprechende Aktionen dürfte aber weiter bestehen.

Innentäter, insbesondere die Administratoren in Rechenzentren, haben nach wie vor die Möglichkeit, weitreichende Störungen auszulösen. Je größer die Rechenzentren, desto stärker wird aber innerhalb der Rechenzentren Arbeitsteilung eingesetzt. Zudem werden höhere Aufwände in die Steuerung von Change-Prozessen und das kontinuierliche Monitoring von IT-Prozessen investiert. Durch diese Maßnahmen wird die Schwelle für Aktionen von Innentätern erhöht und die Wahrscheinlichkeit für eine frühe Entdeckung von weitreichenden Aktionen steigt. Außerdem werden mit zunehmender RZ-Größe die Maßnahmen zur Schadensreduktion, insbesondere durch Vorhalten von Backups, durch Aufstellung von CERT-Teams und ein Business Continuity Management konsequenter realisiert.

Allerdings vergrößert der Trend zum Outsourcing von IT-Dienstleistungen, häufig mit Ketten von Unter- und Unter-Unterauftragnehmern, bis hin zum Cloud-Computing, die Angriffsfläche für Insider der Auftragnehmer beträchtlich. Durch die immer kleineren und billigeren Massenspeichermedien, z.B. USB-Sticks, können Insider sehr große Datenbestände einer Organisation einfach ‚kopieren' und dann z.B. die Organisation damit erpressen. Beispiele hierfür sind z.B. die sogenannten Steuer-CDs, die seit 2008 in vielen Fällen dazu beigetragen haben, Steuerhinterziehung aufzudecken.

Bewertungsergebnis

Die These ist aus heutiger Sicht für die klassischen Angriffsformen weitgehend zutreffend. Die Bedeutung unbeabsichtigter Störungen mit großer Reichweite dürfte derzeit genauso hoch sein wie die von Angriffen. Uneingeschränkt ist auch zu bestätigen, dass Innentätern weitreichende Möglichkeiten für Angriffe offenstehen. Dagegen war die Annahme, dass die elektronischen Angriffsmöglichkeiten Externer wesentlich beschränkt würden, zu optimistisch.

(7) Unbeherrschbare IT-Systeme

Komplexe IuK-Systeme sind nicht beherrschbar.

Während gegen Hardwarefehler sowie Software- und Anwendungsfehler in einfach strukturierten Systemen künftig ausreichende Sicherungen möglich erscheinen, muss in komplexen und eng gekoppelten IuK-Systemen immer damit gerechnet werden, dass unerkannte Systemfehler auftreten, die mit anderen Fehlern auf undurchschaubare Weise interagieren und zu einem Systemversagen führen. Komplexe Softwaresysteme können nicht ausreichend getestet und verifiziert werden. Ob sie fehlerfrei sind, bleibt unsicher. Ebenso ungeklärt muss bleiben, ob ihr Modell allen Situationen der Wirklichkeit angemessen ist. Werden Systeme, von denen zwar bekannt ist, dass sie versagen können, jedoch nicht, an welchen Stellen und in welchem Maße, mit hohen Schadenspotentialen verknüpft, entstehen unverantwortbare Hochrisikosysteme.

Einschätzung der Gültigkeit

Es gibt keine „einfachen“ technischen Systeme mehr: Motorsteuerungen von Kfz können nur noch mit Analyse-Tools überprüft werden, Mobil-Telefone enthalten mehr Software als die Raketen-Steuerungen der Apollo-Mondmissionen, Haushaltsgeräte sollen künftig mit dem Smart Grid interagieren, moderne betriebliche CRM-, ERP- und Finanz-Anwendungssysteme werden auf der Basis von Datenbanken und Webservices generisch konfiguriert und enthalten mehrere 10.000 Tabellen. Dennoch muss festgehalten werden, dass die IT-Systeme und die Systeme, in die IT eingebettet wurde, in der Praxis meist funktionieren und weitreichende Störungen nur selten bekannt werden, solche mit einer spürbaren gesellschaftlichen oder politischen Relevanz im Grunde gar nicht.

Insofern kann man die These am besten in dem Sinne verstehen, dass die praktische Beherrschung von komplexen IuK-Systemen oft (noch) gelingt, jedoch diese oft nicht mehr vollständig verstanden sind. So verstehen IT-Abteilungen oft schon nicht (mehr), warum ein PC nicht mehr gut läuft. Durch einen Neustart wird er dann wieder funktionsfähig. In solchen Fällen wird die ‚unbeherrschbare' IT im Mensch-IT-Gesamtsystem auf eher heuristischer Basis verwendet. Die „echte“ Unbeherrschbarkeit wird erst dann zum Problem, wenn ein unerwarteter Störfall nicht mehr kontrolliert werden kann.

Insgesamt scheinen die folgenden Faktoren zu einem in der Praxis bisher häufig störungsarmen IT-Einsatz beizutragen:

- In Einsatzbereichen mit potentiell kritischen physikalischen oder chemischen Auswirkungen auf die Umwelt werden auf einer unteren technischen Ebene der Prozessteuerung Fail-Safe-Mechanismen realisiert, die unabhängig von den darüber liegenden komplexen IT-Systemen wirken. Dadurch wird eine Entkopplung innerhalb der Prozesssteuerung erreicht.
- Die komplexen Systeme für die Abwicklung von Geschäftsprozessen werden in betriebliche Gesamtprozesse eingebettet. Dabei wird nur ein Teil der Funktionalität der komplexen Basis-Systeme genutzt, und zwar der, der für den jeweiligen Geschäftsprozess funktioniert. Die Grenzen des Einsatzes werden oft bereits im Rahmen des Customizing und der Einführungsprozesse erkannt. Die Organisation reagiert darauf mit Workarounds oder notfalls dem Wechsel zu einem geeigneteren Produkt.

- Zwar wird für die Anpassung von Geschäftsprozessen eine immer höhere Dynamik gefordert. Derzeit dürfte aber eine systematische, planmäßige Ausgestaltung von Geschäftsprozessen noch überwiegen. Sie ist oftmals sogar die Voraussetzung für den Einsatz moderner IT-Systeme zur Unterstützung der Prozesse. Ob die Flexibilisierung der Geschäftsprozesse durch die freie Kombination von Web-Services zu einem größeren Potential für IT-Störfälle führt, bleibt abzuwarten.

Allerdings muss einschränkend festgestellt werden, dass sich diese Form der unverstandenen Beherrschbarkeit vor allem auf die „üblichen" Vorfälle im Systembetrieb und eher auf einzelne Systeme bezieht. Insbesondere für singuläre Ereignisse mit vielen Wechselwirkungen ist eine heuristische Kompensation kaum möglich. Nur selten sind dann geübte Notfallprozesse vorhanden, um eine schnelle und sichere Wiederherstellung zu erreichen.

Wenn kritische Störfälle auftreten, wie beispielsweise die weitreichende Störung des T-Mobile-Netzes im April 2009, versuchen die betroffenen Organisationen allerdings, daraus zu lernen und ihre Prozesse und IT-Systeme anzupassen.

Bewertungsergebnis

Der Einsatz der IT-Systeme bewegt sich nach den Beobachtungen der Autoren in der Praxis im Wesentlichen innerhalb der Grenze der zum jeweiligen Zeitpunkt beherrschten (jedoch nicht notwendigerweise verstandenen) Komplexität. Insofern muss die These relativiert werden. Offensichtlich ist für einen hinreichend zuverlässigen Betrieb kein „volles Systemverständnis" erforderlich. Neue Implementierungstechniken, die Auswahl von „geeigneten" oder „funktionierenden" Teilfunktionen und kontrollierte Einführungsprozesse scheinen ausreichend, um die notwendige Zuverlässigkeit zu erreichen.

Dennoch kann festgehalten werden: Die Komplexität einzelner Systeme wächst durch den IT-Einsatz kontinuierlich. Die Vernetzung von Systemen wird kontinuierlich vorangetrieben und betrifft zunehmend auch Bereiche, in denen Störungen erhebliche Schäden nach sich ziehen können, bspw. im Bereich der Luftfahrt oder der Energieversorgung. Der Trend zur Verringerung der Beherrschbarkeit dürfte daher anhalten. Selbst wenn bislang keine Störungen mit gesellschaftlich hohem Schaden aufgetreten sind, gilt dieser Trend vermutlich auch für Bereiche mit kritischen Infrastrukturen.

(8) Höheres Schadenspotential durch IT-Einsatz

Das Schadenspotential von IuK-Systemen wird deutlich zunehmen. Die Gesellschaft wird in nahezu allen Bereichen vom richtigen Funktionieren dieser Technik-Systeme abhängig sein. Gesamtgesellschaftliche Katastrophen durch den Ausfall wichtiger sozialer Funktionen, die Techniksystemen übertragen wurden, sind nicht auszuschließen.

Die IuK-Technik kann das Schadenspotential von Informationsverarbeitungs- und Kommunikationsprozessen auf spezifische Weise erhöhen. Sie ermöglicht vielfältige schädigende Aktionen und damit Kumulationsschäden. Sie kann zu einer automatischen Vervielfachung eines Schadens und damit zur Verursachung von Multiplikationsschäden genutzt werden. Die Zentralisierung von Daten und Kommunikationsverbindungen kann zu einem hohen

Einzelschaden führen. In vernetzten Systemen können sich Schäden in viele angeschlossene Systeme ausbreiten und einen Komplexschaden hervorrufen. Schließlich werden durch standardisierte Software selbst weit verteilte und isolierte Systeme sehr eng gekoppelt und können durch deren Manipulationen sogar allesamt gleichzeitig ausfallen.

Die Abhängigkeit von IuK-Technik und damit das spezifische Schadenspotential wird in dem Maße ansteigen, wie die IuK-Technik bisherige Formen der Informationsverarbeitung und der Kommunikation verdrängt. Sie kann dadurch reduziert werden, dass Substitutionsmöglichkeiten erhalten bleiben. Macht sich die Gesellschaft von einem einzigen Technik-System abhängig und erhält auch keine funktionalen Äquivalente, kann der Ausfall dieses IuK-Systems Katastrophen nationalen Ausmaßes verursachen.

Einschätzung der Gültigkeit

Während der vergangenen 25 Jahre wurden Geschäftsprozesse zunehmend durch Informationstechnik unterstützt und durch Kommunikationstechnik verbunden. Die Automatisierung wurde gleichermaßen in der Privatwirtschaft wie auch in der öffentlichen Verwaltung vorangetrieben. Dabei wurden je nach Optimierungsziel und Techniktrend auch wechselnde oder ergänzende Strategien verfolgt: sowohl Zentralisierung von IT-Prozessen als auch der Einsatz mobiler Komponenten und die engere Kopplung von dezentralen Komponenten. In der Regel führte der verstärkte Technikeinsatz auch zu höherer Abhängigkeit. Außerdem haben sich an zentralen Knotenpunkten quasi-Monopole von Produkten weniger Hersteller entwickelt, z.B. bei der IP-Vermittlungstechnik Router der Firma Cisco. Die zunehmende IT-basierte Automatisierung von Geschäftsprozessen kann im Störfall ebenfalls zu größeren Schäden führen. Daher ist das Schadenspotential deutlich gewachsen. Inwieweit die Wahrscheinlichkeit sich verändert hat, müsste hingegen noch genauer geprüft werden.

Durch Kundenbindungsprogramme wie Payback und durch Anwendungen im Social Web wie Facebook werden heute persönliche Daten in früher unvorstellbarem Umfang freiwillig preisgegeben. Außerdem werden umfangreiche Profile durch Webtracking angelegt. 1988 hätten wir dem Missbrauch solcher Datensammlungen ein hohes Schadenpotential zugeordnet, z. B. wegen persönlicher Erpressbarkeit. Mit Blick auf die öffentliche Wahrnehmung von Störungen in diesem Bereich muss dieses Schadenspotential heute relativiert werden. Durch den Wertewandel wird derzeit von vielen Menschen die Veröffentlichung vieler privater Informationen als akzeptabel oder sogar als gewünscht bewertet.

Bewertungsergebnis

Die ganz großen Schäden für die Gesellschaft durch IT-Ursachen haben sich bisher nicht realisiert. Dennoch ist davon auszugehen, dass durch den erheblich ausgeweiteten Einsatz von Informations- und Kommunikationstechnik das Schadenspotential in den vergangenen 25 Jahren gewachsen ist. Für die anhaltende Gültigkeit der These spricht beispielsweise die Entwicklung von Nationalen Strategien, wie z.B. die allgemeinen Untersuchungen des BMI zu KRITIS und der spezieller auf die IuK-Techniken zielende NPSI – Nationaler Plan zum Schutz von Informationsinfrastrukturen und in jüngster Zeit der Entwurf für ein IT-Sicherheitsgesetz. Inwieweit sich ein generelles Problembewusstsein hierzu entwickelt hat, bleibt jedoch fraglich.

(9) Zielkonflikt zwischen Sicherheit und Freiheit

Sicherheit der IuK-Technik ist nur auf Kosten von Freiheit und Demokratie möglich, Freiheit und Demokratie können nur auf Kosten der Sicherheit erhalten werden.

Die genannten Schäden müssen unbedingt vermieden werden. Sicherheit ist nicht allein durch technische Maßnahmen herzustellen, sondern setzt Sicherungsstrategien voraus, die gegen Menschen gerichtet sind. Da Angriffe künftig wahrscheinlicher und schadensträchtiger werden und keine Möglichkeit besteht, IuK-Systeme in zugespitzten gesellschaftlichen Konflikten angemessen zu schützen, wird es zum einen notwendig sein, die Sicherungslinie in die Gesellschaft hinein vorzuverlegen. Den Verantwortlichen wird daran gelegen sein, als Risiko definierte Personen oder Entwicklungen vorbeugend in den Griff zu bekommen. Die Technisierung gesellschaftlicher Funktionen (nicht nur, aber auch durch die IuK-Technik) erfordert immer nachdrücklicher gesellschaftliche Stabilität und Vertrauen in das sozialkonforme Verhalten jedes einzelnen. Diese Aufgabe legitimiert den Einsatz von Überwachungselektronik und wird das Überwachungspotential von Staat und Unternehmen anwachsen lassen - mit allen Risiken für eine sich frei entwickelnde Demokratie. Sicherheit setzt zum anderen die Vertrauenswürdigkeit der Beschäftigten voraus. Diese muss gewährleistet werden durch Überprüfungen, Verhaltensüberwachung und Arbeitskontrollen. Die Sicherung der IuK-Technik ist somit ohne Freiheitseinschränkungen nicht möglich. Und die Bereiche, in denen Freiheitseinschränkungen unumgänglich werden, wachsen mit der IuK-Nutzung.

Einschätzung der Gültigkeit

Der Zielkonflikt zwischen Freiheit und Sicherheit besteht nach wie vor. In den vergangenen 25 Jahren waren höhere Schadenspotentiale durch IuK-Technik allerdings kein Treiber für Sicherungszwänge der Gesellschaft. Die Verletzlichkeit durch IuK-Technik ist derzeit stark durch die Terrorismusbekämpfung überlagert. Für politisch motivierte Angreifer ist es wohl einfacher und hinsichtlich der Schreckenswirkung wesentlich effektiver, z. B. eine Bombe zu zünden oder ein Flugzeug zu entführen und in ein Gebäude zu steuern, als eine IuK-Infrastruktur weitreichend und lange zu stören.

Auslöser und Begründung für gesellschaftliche Sicherungsmaßnahmen waren insbesondere die Ereignisse des 11. September 2001 in den USA sowie weitere terroristische Anschläge und die Bedrohungslage aus Kriegs- und Krisenherden in der Welt. Es gibt bisher auch keine Hinweise dafür, dass Personen, die durch die IuK-Entwicklungen große Nachteile erlitten haben, durch terroristische Gruppen gezielt angeworben wurden.

Eine massive Überwachung von Mitarbeitern in Unternehmen wegen hoher Sicherungszwänge der Informationstechnik - wie in der Studie vor 25 Jahren erwartet - scheint bisher ebenfalls eher selten relevant zu sein. Die Einschränkung von Mitbestimmungsrechten aus diesem Grund ist bisher nicht erkennbar.

Bewertungsergebnis

Die IuK-Technik ist bisher keine Ursache mit so hohem Einfluss für die Entwicklung der sozialen Sicherungssysteme, wie dies in der Studie zur Verletzlichkeit der Informationsgesellschaft angenommen wurde.

(10) Sicherungszwänge für die Informationsgesellschaft

Die 'Informationsgesellschaft' setzt sich einem Sicherungszwang aus, den sie nicht mehr beherrschen kann und dessen Dynamik in sozialunverträgliche politische und soziale Verhältnisse zu führen droht.

Die Stärke des Sicherungszwangs folgt aus dem Schadenspotential und der Bedrohung von IuK-Systemen. Da die Gründe für eine solche Bedrohung zu unterschiedlich und zu komplex sind, um sie politisch zu steuern, bleibt als Instrument zur Regulierung des Sicherungszwangs nur die Beeinflussung der Schadensmöglichkeiten. Macht sich die Gesellschaft jedoch von Hochrisikosystemen abhängig, setzt sie sich dem Dauerzwang zur Ernstfallvermeidung aus. Sie verliert die Fähigkeit, den Sicherungszwang zu beherrschen, da dessen Stärke dann von der nicht beeinflussbaren künftigen Bedrohung bestimmt wird. Steigt diese an, entsteht eine Dynamik immer größerer Sicherungsanstrengungen. Sie kann durch einige katastrophale Schäden erheblich beschleunigt werden. Je sicherer die 'Informationsgesellschaft' jedoch wird, desto weniger wird sie dem Bild entsprechen, das sich heute viele von ihr machen: Ihre Verletzlichkeit fordert eine hohe gesellschaftliche Stabilität und erlaubt keine gesellschaftlichen Experimente. Die sichere 'Informationsgesellschaft' ist rigide, geschlossen, unfrei und autoritär.

Einschätzung der Gültigkeit

Offenbar wurde in den vergangenen 25 Jahren kein so hoher Sicherungszwang durch die Verletzlichkeit der IuK-Technologie ausgelöst, wie die These dies nahelegt. Wegen der bislang begrenzten Schadensfolgen aus IT-Störungen für die Gesellschaft wurde der Sicherungszwang durch IuK-Einsatz bisher nicht spürbar. Er wird stärker der allgemeinen terroristischen Bedrohung zugeschrieben. Gruppen von Beschäftigten in IT-Organisationen, wie z.B. Systemadministratoren, werden in einzelnen Unternehmen allerdings besonders sicherheitsüberprüft und ggf. auch überwacht. Ein gesellschaftsweit klarer Trend zu einem Sicherungszwang durch IuK-Einsatz ist jedoch derzeit nicht erkennbar.

Ein Aspekt des Web und der modernen Kommunikationsmittel war 1988 allerdings noch nicht im Fokus: Die offenen Netze werden immer häufiger verwendet, um kriminelle oder terroristische Aktivitäten vorzubereiten oder zu begehen. Daraus entstehen die Forderungen zur Überwachung der IuK-Nutzung, um Rechtsverstöße oder auch Anschläge zu erkennen und aufzuklären. Die Vorratsdatenspeicherung im Bereich der Telekommunikation ist ein Beispiel für diesen Zusammenhang.

Bewertungsergebnis

Die These wurde in der vorliegenden Form durch die Entwicklung der vergangenen 25 Jahre nicht bestätigt. Es gibt allerdings einen gewissen Druck, die Möglichkeiten der IuK-Technik zur Überwachung und Profilbildung zu nutzen, um dem Missbrauch der offenen Netze entgegenzuwirken.

4 Relevanz der Gestaltungsvorschläge

In diesem Abschnitt stellen wir die Gestaltungsvorschläge zur verletzlichkeitsreduzierenden Technikgestaltung vor, die in der Studie 1988 entwickelt wurden und kommentieren deren Relevanz aus heutiger Sicht. Dafür orientieren wir uns an den folgenden Leitfragen:

a) Findet sich das im Gestaltungsvorschlag enthaltene Gestaltungsprinzip in den **IT-Systemen der vergangenen Jahre und ihren Anwendungen** wieder?
b) Ist die Vermeidung von Verletzlichkeit oder sind eher andere Motive der wahrscheinliche Anstoß dafür gewesen?

(1) Reduzierung von Schadensfolgen

Der Ausschluss von Schäden und die Reduzierung von Schadensfolgen haben Vorrang vor Maßnahmen zur Verhinderung von Fehlern und missbräuchlichen Aktionen.

> *Vorrangiges Ziel jedes Sicherungssystems hat zu sein, den Sicherungszwang der IuK-Technik zu vermeiden oder zu verringern, nicht aber ihn optimal zu erfüllen. Wenn ein bestimmter Schaden gar nicht eintreten kann, ist dies immer sicherer als jeder Versuch, ihn durch zusätzliche Maßnahmen zu verhindern. Schadensmindernde Maßnahmen können nicht wie aktive Sicherungsmaßnahmen durch Verlässlichkeitsprobleme in Frage gestellt werden. Werden industrielle Prozesse mit weniger Energie betrieben, fahren Züge nicht mit der möglichen Höchstgeschwindigkeit, sind nicht alle Zweigstellen eines Unternehmens von einem einzigen zentralen Großrechner abhängig oder sind die Datenbestände auf mehrere Stellen verteilt, kann sich der zuvor mögliche größte anzunehmende Unfall nicht mehr ereignen. Dürfen Autos in Ortschaften nur 30 km/h und auf Autobahnen nur 100 km/h schnell fahren, könnte auch ohne elektronische Hilfen die Zahl der Verkehrstoten gesenkt und die Abgasbelastung reduziert werden. Jedenfalls ist darauf zu achten, dass Sicherheitsgewinne durch IuK-Technik nicht wieder durch höheren Energieeinsatz, höhere Geschwindigkeiten und komplexere Systeme 'verbraucht' werden.*

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Bezogen auf den Gestaltungsvorschlag stellen wir fest, dass zumindest auf der Ebene der gesteuerten Prozesse, also der Geschäftsprozesse, Produktionsprozesse oder anderer Abläufe in vielen Fällen Handlungsmöglichkeiten bestehen, um auf Störungen reagieren zu können. Große Unternehmen verfügen über Maßnahmen zum Business Recovery, die auch die IT-Infrastruktur einbeziehen. Auch neue technische Möglichkeiten können teilweise in diese Richtung genutzt werden, wobei diese oft auch ambivalent eingesetzt werden können. Die Folgen von Störungen werden daher insbesondere durch Notfallvorkehrungen auf der Ebene von betrieblichen Maßnahmen für IT-Anwendungen und IT-gestützten Prozessen reduziert. Dafür, dass Maßnahmen eingesetzt werden, Schadenspotentiale durch Technikgestaltung zu begrenzen, gibt es weniger Anhaltspunkte.

b) Verletzlichkeitsreduzierung als Motivation:
Maßnahmen zur Reduzierung von Schadensfolgen werden ergriffen, wenn dies im Eigeninteresse der jeweils betroffenen Organisation liegt. Die Autoren haben aber nicht den Eindruck, dass der Gestaltungsvorschlag gezielt aus Überlegungen zur Verletzlichkeit eingesetzt würde, um – insbesondere auch gesellschaftsweit – einen Technikeinsatz mit geringen Schadenspotentialen zu erreichen. Es

scheint sich niemand verantwortlich zu fühlen, einen solchen Technikeinsatz anzuregen oder gar zu steuern. Ob ein künftiges IT-Sicherheitsgesetz auch zur Reduzierung von Schadenspotentialen führt, bleibt abzuwarten.

(2) Begrenzung von Automatisierung

Techniksysteme, die auf menschlichem Zusammenwirken beruhen und gesellschaftliche Funktionen nur unterstützen, nicht jedoch übernehmen, sind soweit als möglich Automatisierungslösungen vorzuziehen.

So kann etwa das Kommunikationssystem der Briefpost als Ganzes oder in bedeutenden Teilen nicht zerstört werden, weil es auf dem Wissen und dem Können der beschäftigten Menschen und ihrem sehr differenzierten organisatorischen Zusammenhalt beruht. Es könnte allenfalls aufgrund eines bewussten, koordinierten Aktes aller Beteiligten blockiert werden. Soweit IuK-Technik in Flugzeugen, Zügen und Autos die Piloten, Führer und Fahrer in ihrer Tätigkeit unterstützen, ihre Aufmerksamkeit erhöhen oder ihre Reaktionsschnelligkeit verbessern, sind sie sehr hilfreich. Wo sie diese ersetzen, schaffen sie eine unverantwortliche Abhängigkeit vom einwandfreien Funktionieren der Technik. Die Möglichkeit von unvorhergesehenen äußeren Einflüssen, von unbedachten Systemfehlern oder unvollständigen Wirklichkeitsmodellen machen es erforderlich, dass weiterhin Menschen diese Verkehrsmittel lenken und bei einem Versagen der Technik eingreifen können.

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Die Automatisierung von Prozessen mit Hilfe von IT wird unvermindert vorangetrieben. Allerdings ist eine volle Automatisierung oft nicht möglich: In der regulären Prozessgestaltung müssen für Sonderfälle, bei Unregelmäßigkeiten und an den Schnittstellen zu externen Beteiligten Eingriffsmöglichkeiten für Anwender oder Administratoren vorgesehen werden. Dadurch verbleiben dann auch Handlungsmöglichkeiten, die für Reaktionen in Störfällen geeignet sein können.

b) Verletzlichkeitsreduzierung als Motivation:
Handlungsmöglichkeiten werden primär dort erhalten, wo dies nach der praktischen Erfahrung von Anwendern, Administratoren und Produktentwicklern erforderlich ist. Der Gestaltungsvorschlag „Begrenzung von Automatisierung“ wird dagegen nicht gezielt zur Verletzlichkeitsreduzierung eingesetzt. Im Gegenteil wird automatisiert, wenn dies wirtschaftlich sinnvoll erscheint.

(3) Substitutionsmöglichkeiten erhalten

Monopolistische Systeme, die mögliche oder bestehende Alternativen verdrängen, sind zu vermeiden, Substitutionsmöglichkeiten zu erhalten.

Ausweichmöglichkeiten zu schaffen oder zu bewahren, ist die beste Vorsorge für einen Ausfall des gefährdeten Systems. Die 'gelbe Post' auch gegen die elektronischen Kommunikationssysteme zu erhalten, hätte etwa den Vorteil, bei einem völligen oder teilweisen Ausfall des ISDN nicht jede Kommunikationsmöglichkeit zu verlieren. Hart- und Papiergeld auch neben einem elektronischen Zahlungsverkehr weiter zu nutzen, könnte bei dessen Zusammenbruch die folgende Katastrophendynamik erheblich mindern. Ist das Büro der Zukunft nicht papierlos, sondern nur papierarm, wären die Auswirkungen weniger verheerend, wenn der Rechner ausfällt oder Dateien verloren gehen.

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Zum Zeitpunkt der Verletzlichkeitsstudie war die Deutsche Bundespost der Monopolanbieter von Telefondienstleistungen und Eigentümer des deutschen Telefonnetzes. Heute wird die Nachfrage nach TK-Leistungen in Deutschland durch mehrere TK-Anbieter und auf Basis verschiedener Technologien befriedigt: klassisches Festnetz, Mobilfunk, Koax-Kabelnetze, Satellit und Glasfasernetz (im Aufbau). Die Konkurrenz auf dem Mobilfunkmarkt führte insbesondere zum Aufbau konkurrierender flächendeckender Mobilfunk-Netze. Auch im Bereich des Festnetzes ist eine Diversifikation festzustellen: Die nach der Marktöffnung aufgetretenen Anbieter bauen teilweise eigene Netze auf, insbesondere im Fernbereich. Daneben treten auch lokale Akteure, wie die Energieversorger, mit ihrer eigenen Infrastruktur als Anbieter von TK-Leistungen auf.

Die Integration verschiedener Medien in TCP/IP-Dienste führt dazu, dass das Internet zunehmend Substitutionsmöglichkeiten im Bereich der Telefonie bietet, etwa Skype. E-Mail und andere moderne Web-Dienste erlauben es, Nachrichten schnell und unkompliziert ohne Telefon auszutauschen. Die Bedeutung der Telefonie ist auch zurückgegangen, weil weitere Kommunikationsbedürfnisse, wie Bestellungen oder Statusanfragen über Portale schnell und zielgerichtet abgedeckt werden. Damit tragen auch Internet-Service-Provider, wie die Betreiber der Kabelfernsehnetze, zu einer Diversifikation der TK-Infrastruktur bei.

Allerdings wird auch erwartet, dass die klassische analoge wie auch die ISDN-Telefontechnik in den nächsten Jahren weitgehend abgelöst wird. Der Umbau der Netze zu reinen TCP/IP-Netzen erlaubt den Betreibern, die Bandbreite der eingesetzten Komponenten zu reduzieren und den Betrieb der Netze effizienter zu gestalten.

Durch die Integration der Übertragungstechnik der verschiedenen Medien in die TCP/IP-Dienste entwickelt sich das Internet zu DER kritischen Infrastruktur für TK-Dienste. Die Protokolle wurden insbesondere auch unter dem Gesichtspunkt der Ausfallsicherheit gestaltet. Dass die Netze damit unter Verletzlichkeitsgesichtspunkten für die heutige Nutzung risikoadäquat ausgelegt sind und betrieben werden können, kann daraus allerdings nicht automatisch geschlossen werden.

Das papierlose Büro ist in der öffentlichen Verwaltung auch 25 Jahre nach der Verletzlichkeitsstudie noch nicht erreicht. Inzwischen wurde aber insbesondere in großen Unternehmen und durchaus auch zunehmend in Behörden in einigen Bereichen die elektronische Dokumentenverwaltung eingeführt und zumindest in Teilen die Papierakten abgelöst. Das Einscannen von papierhaften Belegen, die Abschaffung der papiergebundenen Lohnsteuerkarte und die beleglose An- und Abmeldung von Arbeitnehmern bei der Sozialversicherung sind konkrete Beispiele hierfür. Der Ausfall der entsprechenden CRM- und Dokumentenverwaltungssysteme oder auch von E-Mail-Systemen als einer zentralen Transportinfrastruktur vom und zum Kunden oder Bürger würde alle diese Geschäftsprozesse vermutlich massiv beeinträchtigen.

b) Verletzlichkeitsreduzierung als Motivation:
Auch wenn eine deutliche Differenzierung der TK-Infrastruktur festzustellen ist,

geht diese doch nicht auf die Umsetzung des Gestaltungsvorschlags, sondern auf die De-Regulierung und die Wechselwirkungen mit den technischen Innovationen der Telekommunikation zurück. Deshalb kann nicht davon ausgegangen werden, dass die Differenzierung der TK-Infrastruktur in den vergangenen 25 Jahren systematisch erfolgte. Wir erwarten daher, dass es einige kritische Komponenten in der Infrastruktur gibt. Ob für den Fall der Störung einer solchen Komponente hinreichende Substitutionsmöglichkeiten bestehen, und wie weit ausgeschlossen werden kann, dass solche Komponenten gleichzeitig gestört werden, wäre für eine differenzierte Bewertung neu zu prüfen.

(4) Redundanzen schaffen

Soweit dies möglich ist, sind Redundanzen zu schaffen.

Sind Kommunikationsnetze vermascht, arbeiten Rechner parallel, stehen Ersatzrechenzentren bereit, sind alle Dateien und Programme mehrfach kopiert und an unterschiedlichen Orten gesichert oder ist die für den Betrieb der IuK-Systeme notwendige Infrastruktur mehrfach vorhanden, wird das Ausmaß möglicher Schäden gemindert und der Zwang zur Sicherung reduziert. Bleibt der dritte Mann im Cockpit und der Lokführer in seinem Leitstand, werden dadurch Sicherheitsreserven erhalten. Werden Programme von unterschiedlichen Teams entwickelt und vor ihrem Einsatz ausführlich getestet oder werden alle Veränderungen an einem System einer Revision unterworfen, schafft der zusätzliche Aufwand auch zusätzliche Sicherheit.

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Das Problem des möglichen „Single Point of Failure“ mit der Möglichkeit existenzieller Schäden für die Organisation wird in großen Unternehmen für Rechenzentren und TK-Anbindungen meist gesehen. Als Notfall- oder Business-Continuity-Maßnahmen werden daher Backup-Rechenzentren vorgehalten und mehrere TK-Anbindungen realisiert, nach Möglichkeit auch über unterschiedliche Provider.

Im Bereich der TK-Infrastruktur wurden zwar Netze auf- und ausgebaut. Diese Projekte sind aber durch die wirtschaftlichen Interessen der Akteure im privatisierten Markt getrieben. Daher kann nicht generell angenommen werden, dass in großem Umfang Überkapazitäten zur Störfall-Beherrschung vorgehalten werden. Redundanzen können innerhalb von Organisationen erwartet werden, wenn dies durch interne Risikobewertungen motiviert wird oder durch regulatorische Anforderungen vorgeschrieben ist. Üblicherweise werden sich die Betreiber aber um eine optimale Auslastung bemühen.

Cloud-Computing verdient eine besondere Betrachtung. Der einzelne Cloud-Anbieter kann innerhalb seiner Ressourcen die angebotenen Dienste in der Regel flexibel verschieben. Aus dieser Perspektive könnten Redundanzen gut vorgehalten und in Störfällen genutzt werden. Allerdings werden auch von den Cloud-Anbietern Redundanzen nur in wirtschaftlich vertretbarem Umfang vorgehalten. Liegen die Störungsursachen in der Software, hilft Hardware-Redundanz häufig nicht. Einzelne größere Störungen in Cloud-Diensten sind in den letzten Jahren schon aufgetreten. Es ist auch kaum anzunehmen, dass einzelne Cloud-Anbieter so große Redundanzen vorhalten, dass sie im Falle einer länger andauernden massiven Störung bei einem Mitbewerber einspringen könnten.

Mit seinen Daten und Prozessen „in die Cloud“ zu gehen, macht für einen Auftraggeber wirtschaftlich nur Sinn, wenn dafür die Speicherung oder sogar die Programmpflege in der eigenen Organisation entfallen kann. Cloud-Dienste, die *Infrastructure as a Service* oder *Platform as a Service* bereitstellen, sind vielfach vergleichbar. Der Auftraggeber könnte daher solche Dienste sogar bei unterschiedlichen Cloud-Anbietern redundant nutzen oder im Störfall bei geeigneten lokalen Backups zu einem anderen Anbieter wechseln. Bei Diensten des Typs *Software as a Service* (SaaS) sind solche Wechsel aber derzeit kaum möglich, weil Unterschiede in den Anwendungen eine Migration erfordern. Die Fähigkeit, auf schwere Störfälle zu reagieren, dürfte bei den Auftraggebern im Allgemeinen und im Besonderen bei SaaS sinken. Denn sie werden im Laufe der Zeit Hardware und auch Betriebspersonal abbauen, um Kostenvorteile zu realisieren.

Die Abhängigkeit von der TK-Infrastruktur steigt beim Cloud-Computing auf zweierlei Weise. Zum einen benötigen die Cloud-Anbieter schnelle Übertragungsleitungen, um Anwendungen zwischen Rechenzentren zu verschieben. Zum anderen können die Auftraggeber nur noch arbeiten, wenn sie per Telekommunikation ausreichend performanten Zugriff auf ihre Anwendungen in der Cloud haben. Schnelle TK-Anbindungen sind auch notwendig, wenn – soweit überhaupt vorbereitet – im Störfall Anwendungen auf andere Cloud-Anbieter verlagert werden soll.

Für die cloud-nutzenden Organisationen steigt die Abhängigkeit sowohl von der neuen Cloud-Infrastruktur als auch von der TK-Infrastruktur sowie der politischen und rechtlichen Stabilität in dem Land, in dem der Cloud-Anbieter die Daten speichert. Im Falle eines schweren Störfalls bei einem großen Cloud-Anbieter dürften weitreichende Störungen bei vielen Auftraggebern mit entsprechend hohem Schadenspotential die Folge sein.

b) Verletzlichkeitsreduzierung als Motivation:
Organisationen, die das Problem kritischer IT-Komponenten erkennen und die über die notwendigen finanziellen Ressourcen verfügen, halten redundante Komponenten vor. Insofern wird der Gestaltungsvorschlag - teilweise auch durchgängig - verfolgt. Auch in einigen Industriebereichen, wie z.B. der Finanzindustrie, gibt es inzwischen rechtliche Vorgaben oder zumindest Normen und Standards, die die Schaffung von Redundanzen vorschreiben. Ein Beispiel hierfür sind die Vorschriften des Basel-II Abkommens zum ‚Operationellen Risiko’ und ergänzende Vorgaben der MaRisk des Bundesaufsichtsamtes für das Finanzwesen (BaFin). Die Grundschutzkataloge und Standards des BSI geben ebenfalls Hinweise in diese Richtung. Von einer systematischen, auf gesellschaftlicher Ebene gesteuerten Umsetzung im Sinne eines Gestaltungsprinzips kann aber nicht ausgegangen werden. Auch wenn Verlagerungen in die Cloud im Einzelfall Redundanzstrategien schaffen, dürften sie insgesamt zu einem Abbau von Redundanzen und damit zu einer höheren Verletzlichkeit führen.

(5) Diversifizierung anstreben

Soweit möglich, ist eine zeitliche, räumliche, technische und organisatorische Diversifizierung anzustreben. Herstellermonopole sind zu vermeiden.

Die Verwendung unterschiedlicher technischer Prinzipien, Verfahrensweisen, Materialien und Herstellersysteme innerhalb eines komplexen sozio-technischen Systems verhindert, dass der gleiche Fehler, die gleiche Manipulation oder der gleiche Anschlag das gesamte System außer Funktion setzt. So verhindert beispielsweise die Ausstattung der Vermittlungsstellen im künftigen ISDN je zur Hälfte mit Systemen verschiedener Hersteller, dass ein spezifischer Fehler beide Hälften gleichzeitig zerstört. Einen ähnlich positiven Effekt hätten verschiedene Fernmeldenetze für Sprache, Daten und Bilder. Wird ein medizinisches Expertensystem nicht als einziges flächendeckend eingesetzt, sondern neben anderen Systemen genutzt, wirkt sich ein Fehler nur in einem System aus und wird durch den Vergleich mit den anderen erkannt.

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Hinsichtlich dieses Gestaltungsvorschlags sind eine Reihe von unterschiedlichen Aspekten zu betrachten. In den vergangenen Jahren wurden in manchen Bereichen Industriestandards etabliert oder erhalten, die zu faktischen **Herstellermonopolen** führen. Dies gilt beispielsweise weiterhin für die PC-Plattform mit Windows und den Microsoft-Office-Anwendungen oder für bestimmte Komponenten in der Netzwerktechnik, z.B. von Cisco. Auch im Bereich der Unternehmenssoftware verfügen einige Hersteller über sehr große Marktanteile, beispielsweise SAP. Ebenso muss für Angebote an IT- und TK-Dienstleistungen wie z.B. Google und Apple ein Konzentrationsprozess festgestellt werden.

Für einige Software-Produkte bildet das Angebot an **Open Source** Lösungen jedoch ein starkes Gegengewicht zu kommerziellen Lösungen. Dies gilt beispielsweise für Linux, MySQL, Open Office und ähnliche. Durch die kostenlosen Alternativen dürfte die kommerzielle Monopolbildung abgeschwächt werden. Allerdings gelten in kritischen Einsatzgebieten oft hohe Anforderungen an Spezialisierung und Verfügbarkeit. Wenn dazu Support eines Herstellers erforderlich ist, scheiden freie Lösungen oft aus. **Innerhalb von Unternehmen** wird häufig ein "Zoo" von Systemen und Anwendungen eingesetzt. Je größer die Unternehmen, desto vielfältiger ist die IT-Landschaft häufig gewachsen. Häufig wird aber versucht, die eingesetzten Systeme zu vereinheitlichen. Dies gilt auch im Zusammenhang mit Business-Continuity-Strategien[27]: je vielfältiger die IT-Landschaft, desto höher der Aufwand für die Redundanz-Systeme und Notfallpläne. Wenn allerdings Business-Continunity-Strategien entwickelt werden, ist eine der zentralen Entscheidungen die räumliche Verteilung von IT-Ressourcen. Grundsätzlich kann auch angenommen werden, dass in großen Unternehmen viele geschäftskritische Anwendungen in irgendeiner Form auf den Industriestandards aufsetzen oder von ihnen abhängen. Organisatorische Diversifizierung wird wegen der schon für „einfache“ Prozesse kaum zu beherrschenden Aufwände möglichst vermieden.

27 siehe oben (4)

Gleichzeitig werden in vielen Bereichen **offene Standards** entwickelt, vor allem für Schnittstellen und Protokolle. Ein Beispiel hierfür ist XML mit den vielen darauf aufbauenden standardisierten „Fachdialekten“, wie bspw. dem Open Document Format. Diese bieten die Chance, dass unterschiedliche Applikationen die resultierenden Datenbestände weitgehend kompatibel verarbeiten können und einfachere Übergänge zwischen unterschiedlichen Applikationen möglich werden. Damit haben die Software-Hersteller eine vergleichbare Ausgangsbasis für ihre Produktentwicklung und der Anwender eine Wahlmöglichkeit zwischen alternativen Anwendungen. Anpassungen sollten beim Wechsel zwischen Applikationen mit deutlich geringerem Aufwand zu bewältigen sein. Der Trend kann Diversifikation unterstützen. Er bietet aber kaum kurzfristige Handlungsoptionen in Störfallsituationen.

Schließlich hat in den vergangenen 25 Jahren ein gewaltiger Umbruch in der **Infrastruktur für die Kommunikation** stattgefunden. Der Siegeszug des Internet, die Kommunikation über höhere offene Protokolle und die Bereitstellung von Informationen über das WWW haben die technisch unterstützte Kommunikation massiv verändert. Auch die „klassische“ Telefonie wird zunehmend durch das Internetbasierte Voice over IP abgelöst. Diese Kommunikationstechniken bedienen sich offener Standards für Schnittstellen und Funktionalität. Da sie von vielen Produkten implementiert werden, bestehen für viele Aufgaben Wahlmöglichkeiten hinsichtlich der eingesetzten Systeme. Allerdings muss auch festgehalten werden: Es findet ein Konzentrationsprozess zur TCP/IP-basierten Übertragung von Daten statt.

Neuere technische Entwicklungen setzen auf so genannte **serviceorientierte Architekturen** (SOA). Im Rahmen dieses Architekturansatzes für IT-Systeme sollen Funktionen als austauschbare Module in der IT-Landschaft bereitgestellt werden. Durch Orchestrierung der Module werden dann die gewünschten Geschäftsprozesse unterstützt. Weiter wird angenommen, dass für die Funktionen der Module Standards entstehen. Da die SOA-Infrastruktur die Module einschließlich der Schnittstellenbeschreibungen und wichtiger Sicherheitsfunktionen bereitstellen soll, wird mit dem Ansatz die Hoffnung auf wieder verwendbare und austauschbare Komponenten verknüpft. Damit wären gute Vorrausetzungen für eine Diversifizierung oder zumindest für kurzfristige Reaktionen im Störungsfall gegeben, wenn alternative Implementierungen von Modulen zur Verfügung stehen. Konkrete praktische Effekte bezüglich des Gestaltungsvorschlags können derzeit zwar noch nicht erkannt werden, entsprechende Geschäftsmodelle sind jedoch zurzeit z.B. unter den Schlagworten von ‚Software-as-a-Service’ und ‚Cloud-Computing’ bereits umgesetzt oder in der Entwicklung. Inwieweit dies tatsächlich eine Diversifizierung unterstützt, bleibt jedoch abzuwarten.

Die Miete von **Rechenleistung und Transportleistung im Web** wurde in den letzten Jahren einfacher (Cloud Computing). Mehrere Unternehmen bieten Möglichkeiten, sehr kurzfristig feste oder dynamische Kapazitäten zu mieten. Der Basisbetrieb wird vom Anbieter bereitgestellt, der Mieter kann die Maschinen nach seinen Vorstellungen mit Software ausstatten und betreiben. In anderen Angeboten wird die Kapazität von Web-Auftritten durch weltweit verteilte Kapazitäten dynamisch an der Nachfrage orientiert und ressourcensparend repliziert. Solche Dienstleistungen bieten gegebenenfalls auch Reaktionsmöglichkeiten in Störfällen. So können mit entsprechender Vorbereitung beispielsweise Web-basierte Dienste vergleichsweise einfach zu einem andern Dienstleister verlegt oder in

ihrer Leistung ausgebaut werden.[28] Ob dies allerdings auch erlaubt, monopolartige Services wie Google kurzfristig durch Alternativen zu substituieren, bliebe zu prüfen. Durch die Verlagerung von Anwendungen in die Cloud findet außerdem wieder ein Konzentrationsprozess auf wenige Stellen mit großen Ressourcen für den IT-Betrieb statt. Die Kontrollmöglichkeiten für die Auftraggeber oder Benutzer der Anwendungen sind klein. Daher werden sie auch in schweren Störfällen in der Regel von den Dienstanbietern abhängig sein.

b) Verletzlichkeitsreduzierung als Motivation:
Insgesamt zeigen die Trends keine deutlichen Vorteile unter dem Blickwinkel des Kriteriums Verletzlichkeit. Eine zeitliche, räumliche, technische und organisatorische Diversifizierung sicherzustellen, wird jedenfalls nicht systematisch verfolgt. Organisationsintern muss vielmehr ein grundsätzlicher Trend zur technischen und organisatorischen Harmonisierung angenommen werden. Räumliche Diversifikation wird von Organisationen bei entsprechender Risikobewertung im Rahmen des Aufbaus von redundanten Ressourcen gezielt angestrebt.

Organisationsübergreifend dürften für kritische Systeme überwiegend die Produkte der Marktführer zum Einsatz kommen. Eine Diversifikation kann nicht angenommen werden.

Eine gewisse gesellschaftliche Diskussion gibt es schließlich hinsichtlich der Marktmacht z.B. von Microsoft, Google und anderen weltumspannenden IT-Angeboten. Allerdings ist diese Diskussion ebenfalls ökonomisch und wirtschaftspolitisch begründet und nicht normativ aus der Verletzlichkeitsreduzierung motiviert. Eine gezielte Diversifizierung ist nicht zu erkennen und auch in der näheren Zukunft nicht zu erwarten.

(6) IuK-Systeme entkoppeln und dezentral nutzen

IuK-Systeme sind soweit wie möglich zu entkoppeln, linear aufzubauen und dezentral zu nutzen.

Je stärker entkoppelt das System und je dezentraler die Anwendung, desto geringer ist die Reichweite möglicher Schäden. Je stärker vernetzt und in seiner Anwendung zentralisiert ein IuK-System ist, desto weiter kann ein Primärschaden sich auswirken. Je komplexer das System ist, desto größer ist die Wahrscheinlichkeit, dass es zu unvorhersehbaren Interaktionen von Fehlern und Ausfällen kommt. In keinem System sind Fehler und Missbrauchsaktionen zu vermeiden. Ist das System nur lose gekoppelt, bestehen im Schadensfall - verglichen mit einem eng gekoppelten System - mehr Möglichkeiten helfend einzugreifen und Puffer, Redundanzen oder Substitutionsmöglichkeiten zu finden, um die Schadensdynamik zu begrenzen. Werden Systeme weniger komplex aufgebaut, sind sie übersichtlicher, fehlerärmer und leichter beherrschbar. Jede lineare Anordnung von Komponenten reduziert die Gefahr, dass Fehler in ihrem Zusammenwirken einen großen Schaden verursachen. Werden kleinere und selbständige organisatorische Einheiten geschaffen, vermindert sich nicht nur das größtmögliche Schadensausmaß, sondern auch der Schutzbedarf. Denn Systeme mit vermindertem Schadenspotential üben einen geringeren Anreiz aus, sie anzugreifen oder zu stören, da die Wirkung eines Missbrauchs begrenzt ist.

[28] Siehe auch oben unter These (4).

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Hinsichtlich dieses Gestaltungsprinzips lassen sich zwei verschiedene Entwicklungen beobachten:

Auf der *Infrastrukturebene* ist vielfach eine starke Vernetzung und Koppelung zu beobachten. Dabei wird IT teilweise auch (re)zentralisiert. Auf dieser Ebene wird oft auch auf die Erhaltung und Schaffung von Redundanzen geachtet.

Auf der *Anwendungsebene* ist eine immer stärkere Integration von einzelnen Geschäftsprozessen zu zunehmend sogar unternehmensübergreifenden Prozessketten zu beobachten. Puffer, Redundanzen und Substitutionsmöglichkeiten werden nach Möglichkeit zu Gunsten von höherer Effizienz und der Senkung von Kosten abgebaut. Die Triebfeder ist hierbei der ökonomische Nutzen und Gewinn aus enger Kopplung, Reduzierung der Anzahl von unterschiedlichen Anwendungssysteme und möglichst wenigen, dafür einheitlichen Datenformaten. Ob SOA-Infrastrukturen als neuer Technikansatz künftig dennoch Möglichkeiten zur Entkopplung eröffnen, bleibt abzuwarten.

Systematische Ausnahmen von diesem Trend können allenfalls da angenommen werden, wo physisch kritische Prozesse gesteuert werden. In diesen Bereichen bieten Sensoren und Mikroelektronik zur Auswertung von Messwerten die Chance, physische Prozesse wesentlich präziser zu steuern, als dies mit klassischen Techniken möglich war. Abweichungen von Soll-Werten können schneller und genauer identifiziert und Maßnahmen zur Beherrschung von Unregelmäßigkeiten eingeleitet werden.

b) Verletzlichkeitsreduzierung als Motivation:
Der Vorschlag wird nicht als Kriterium zur Gestaltung von Technikunterstützung für Geschäftsprozesse verfolgt. Nur in Bereichen der physischen Prozesssteuerung sind Maßnahmen zur Entkopplung zu erwarten.

(7) Fail-Safe-Strategien anwenden

Systeme sollten möglichst bei Fehlfunktionen oder Ausfällen von Komponenten in einen energieminimalen, schadensarmen und stabilen Zustand übergehen.

> *Als Vorbild könnten die 'fail-safe'-Schaltungen bei der Bahn dienen: Bei einem technischen Defekt, einem Bedienungsfehler oder Ausfall des Lokführers wird der Zug automatisch abgebremst. Systeme, die nach einem Defekt an wichtigen Sicherungssystemen weiterarbeiten oder gar Leistungsexkursionen ermöglichen, sind zu vermeiden. Konstruktive Vorkehrungen, die bewirken, dass sie immer nur auf die 'sichere Seite' ausfallen können, sollten auch bei Autos, medizinischen Geräten oder Anlagen zur Prozesssteuerung vorgesehen werden.*

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Technik ist zu einem immer höheren Grad von Informationstechnik durchdrungen. Sie erhöht einerseits die Komplexität und begrenzt gegebenenfalls auch die

Handlungsmöglichkeiten der Anwender bei Störfällen. Aber vielfach werden Sicherheitsmaßnahmen erst durch Informationstechnik möglich und in die Produkte integriert. Viele Prozesse werden durch ein Monitoring überwacht. Auf erkannte Fehlfunktionen kann dann – teilweise auch automatisch - reagiert werden.

Andererseits wäre für eine Vorsorge aus dem Blickwinkel der Verletzlichkeit erforderlich, dass für gesellschaftlich relevante Prozesse auch in Störfällen die notwendigen Kernfunktionen aufrechterhalten werden können.[29] Durch die zunehmende Informatisierung unserer Gesellschaft auch in nicht-physikalische Anwendungsgebiete hinein, z.B. elektronischer Zahlungsverkehr, wird es daher immer wichtiger, dass das Gestaltungsprinzip auch im übertragenen Sinne interpretiert wird. Es ist nämlich schwierig, sich vorzustellen, was ein energieminimaler Zustand für den elektronischen Zahlungsverkehr oder für das Social Web sein könnte. Unabhängig davon wären auch Substitutionsmöglichkeiten vorzuhalten, um notwendige Kernfunktionen weiterhin erfüllen zu können.

In manchen Bereichen der Technik ist tatsächlich eine solche Entwicklung zu beobachten. Z. B. haben moderne Autos, deren Türen sich eigentlich nur noch über Funkschlüssel öffnen lassen, noch einen manuellen Schlüssel als ‚Fallback'-Lösung.

Allerdings ist davon auszugehen, dass wir bei vielen komplexen IT-gesteuerten Systemen einen solchen Minimalbetrieb kaum durchführen können, sondern dass in der Tat dann für die Dauer der Störung solche Systeme ganz heruntergefahren werden müssen. Der moderne Zugverkehr beispielsweise kann beim Ausfall von Weichensteuerungssoftware höchstens noch in einem eingeschränkten Umfang erfolgen, bis die IT-Störung als solche behoben ist. Ein vollständiger Substitutionsbetrieb mit manueller Weichensteuerung ist jedoch in der Regel nicht mehr möglich.

b) Verletzlichkeitsreduzierung als Motivation:
Für diesen Gestaltungsvorschlag ist für Bereiche der Betriebs- und Funktionssicherheit zu erkennen, dass Verletzlichkeitsreduzierung tatsächlich eine Rolle gespielt haben könnte. Allerdings gilt dies nicht in vergleichbarer Weise für das gesamte Spektrum der Nutzungsformen von IuK-Techniken und IuK-Anwendungen. Teilweise ist das Fail-Safe-Prinzip oder das Prinzip der graduellen Reduktion sozialer Funktionen auch schwierig anzuwenden.

(8) Systematische Notfallplanung

Für alle die Allgemeinheit betreffenden Schadensmöglichkeiten ist eine systematische Notfallplanung zu betreiben und einzuüben.

Während bisher die Verletzlichkeit der Gesellschaft durch den Missbrauch oder ein Versagen der IuK-Technik verdrängt wurde, würden durch Notfallplanungen und -übungen das Sicherheitsbewusstsein geschärft und die notwendigsten Maßnahmen zur Schadensbegrenzung und -beseitigung eingeübt.

29 Siehe dazu auch das Gestaltungskriterium „graduelle Reduktion sozialer Funktionen" in *Hammer, V. 1999, 397.*

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:

Große Organisationen, die ein Notfall-Management aufbauen, berücksichtigen meist unterschiedliche Störfall-Szenarien. Der Fokus liegt dabei zwar in der Regel auf den schweren Störungen der eigenen Systeme und Prozesse.[30] In den Szenarien können auch Störfälle der allgemeinen Infrastruktur, wie der Stromversorgung oder bei TK-Providern enthalten sein. Allerdings sind sowohl die Vorsorge- als auch die konkreten Reaktionsmöglichkeiten aus der Perspektive der jeweiligen Organisation begrenzt. Zwar können Redundanzen vorgehalten und Notfallunterstützung bei unterschiedlichen Providern eingekauft werden. Über die Vereinbarung von Service Level Agreements können auch Anforderungen für Störfälle an die Lieferanten gestellt werden. Dadurch sollten Störfälle, die nur die Organisation betreffen, gut beherrschbar sein. Wie sich aber kumulierte Anforderungen an Externe auswirken, wenn ein schwerer Störfall viele Organisationen gleichermaßen betrifft und alle ähnliche Reaktionsmaßnahmen ergreifen, lässt sich aus der Perspektive der einzelnen Organisation kaum prüfen und bewerten.

In der Praxis scheint auch bereits ein internes betriebliches Notfall-Management eine große Herausforderung zu sein. So stellt eine Studie fest, dass „bei 50% von 253 Unternehmen, die ihren Recovery Plan aktivieren mussten, der Plan nicht mehr aktuell gewesen“ sei.[31] Eine andere Studie verspricht für Energieversorger in Deutschland keine bessere Situation.[32]

Umso schwieriger ist die übergreifende Notfallvorsorge für kritische Infrastrukturen. Ein auf der Basis der Rechtslage von 2002 und 2005 erstelltes Gutachten kommt zum Schluss: „Gesetzliche Regelungen zum Schutz kritischer Infrastrukturen sind nur vereinzelt vorhanden.“[33] Ein Bericht des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag untersucht die „Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen Ausfalls der Stromversorgung“. Er kommt zum Ergebnis: *„Die Wahrscheinlichkeit eines langandauernden und das Gebiet mehrerer Bundesländer betreffenden Stromausfalls mag gering sein. Träte dieser Fall aber ein, kämen die dadurch ausgelösten Folgen einer nationalen Katastrophe gleich. Diese wäre selbst durch eine Mobilisierung aller internen und externen Kräfte und Ressourcen nicht beherrschbar, allenfalls zu mildern.*“[34] Dafür spielen auch die Abhängigkeit von IuK-Systemen und deren komplexe Vernetzung eine wichtige Rolle.

Insbesondere für übergreifende Infrastrukturen, aber auch für viele einzelne Unternehmen besteht offenbar großer Handlungsbedarf zur Verbesserung der Notfallvorsorge. Dafür spricht auch, dass auf europäischer Ebene 2011 auf Initiative

30 In *BSI 100-4 2008* wird z. B. ein Standard zum Aufbau eines organisationsinternen Notfallmanagements bereitgestellt.

31 *http://www.bcm-news.de/2012/07/24/why-recovery-plans-fail-ergebnisse-einer-umfrage/* (Abfrage vom 26.2.2013)

32 *http://www.pwc.de/de/energiewirtschaft/pwc-studie-wie-gut-sind-deutsche-energieversorger-auf-notfaelle-vorbereitet.jhtml* und *http://www.pwc.de/de_DE/de/energiewirtschaft/assets/studie_notfallmanagement_energieversorger.pdf* (Abruf 26.2.2013)

33 *BSI 2005a*, 15.

34 TAB 2010, 26.

des DIN die CEN-CENELEC-ETSI Cyber Security Coordination Group gegründet wurde. Sie soll die Normungsarbeiten der beteiligten Organisationen in diesem Bereich koordinieren. Auch wäre die Europäischen Kommission *„in Begriff, gesetzgeberisch tätig zu werden, um Unternehmen und Behörden zu klareren Regeln und Maßnahmen zum Schutz vor Cyberattacken zu bewegen bzw. zu zwingen“.* Durch Normen soll ein Konsens über Maßnahmen erreicht werden.[35]

Im Koalitionsvertrag zwischen CDU, CSU und SPD vom Dezember 2013 heißt es: „Wir schaffen ein IT-Sicherheitsgesetz mit verbindlichen Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen und der Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle. Dafür setzen wir uns auch auf der EU-Ebene im Rahmen der europäischen Cybersicherheitsstrategie ein.“ Außerdem werden „die Bundesbehörden … verpflichtet, zehn Prozent ihrer IT-Budgets für die Sicherheit ihrer Systeme zu verwenden“.[36] Seit mehreren Jahren fördert das Bundesministerium für Bildung und Forschung spezifische Forschungsprojekte zu Verbesserung des Katastrophenmanagements im Rahmen seines Forschungsprogramms „Zivile Sicherheit“. Im Entwurf zum IT-Sicherheitsgesetz vom August 2014[37] sind Aufgaben zur Beobachtung der Sicherheitslage und zur Steuerung des Sicherheitsniveaus der IT in Kritischen Infrastrukturen vorgesehen. Der beim BSI, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), BKA und Bundesamtes für Verfassungsschutz (BfV) erwartete Personalaufwand liegt nach dem Entwurf bei insgesamt 276 Planstellen.

b. Verletzlichkeitsreduzierung als Motivation:
Für das Gestaltungsprinzip der Notfallplanung lässt sich festhalten, dass die Aufrechterhaltung der (reinen) Funktionsfähigkeit sicherlich durch die Verletzlichkeitsreduzierung motiviert ist. So umfassen z.B. die Vorgaben des BSI zum Notfallhandbuch und Vorgaben von Basel-II zum operationellen Risiko und deren Umsetzung in den MaRisk Vorschriften zur Aufrechterhaltung der Funktionsfähigkeit. Weitere Aspekte wie z.B. Integrität und Vertraulichkeit sind jedoch nicht in gleicher Weise adressiert. Die Wirkungen des geplanten neuen IT-Sicherheitsgesetzes muss die Praxis in den nächsten Jahren zeigen.

(9) Technikgestaltung im gesellschaftlichen Konsens

Die Gestaltung der Technik und der Sicherungssysteme ist an der Zustimmung der Betroffenen und der Öffentlichkeit zu orientieren.

Die Ausrichtung von Planungen am Konsens und nicht nur an Partikularinteressen verhindert nicht alle, aber einige negative Effekte der Informatisierung und ihrer Sicherung und vermeidet zumindest eine Reihe zusätzlicher Motive für einen Missbrauch der IuK-Technik. Hierzu gehört auch, die Betroffenen an den Gestaltungsentscheidungen zu beteiligen sowie die sozialunverträglichen Effekte der Informatisierung zu begrenzen und - etwa durch eine gerechte Verteilung der verbleibenden Arbeit - aufzufangen.

35 *Wischenhöfer, DuD 2013, 32.*

36 Deutschlands Zukunft gestalten, Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Legislaturperiode, 147f.

37 *http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf* (Abruf: 10.09.2014)

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Innerhalb von großen Industrieunternehmen und in öffentlichen Einrichtungen kann davon ausgegangen werden, dass die Einführung von IT-Verfahren unter Beteiligung der betrieblichen und behördlichen Interessenvertretungen im Rahmen der Vorgaben des Betriebsverfassungsgesetzes oder der Personalvertretungsgesetze erfolgt. Durch dieses Beteiligungsmodell wird in der Regel auch eine höhere Akzeptanz der Technik erreicht.

Gesamtgesellschaftlich spielt Beteiligung bei der Ausgestaltung von IT-Systemen und Infrastrukturen keine besondere Rolle. Die Endanwender können in der Regel nur in Usability-Tests mitwirken – die Entscheidungen über die De- und Re-Regulierung der TK-Wirtschaft, die Gestaltung elektronischer Pässe, der Gesundheitskarte, der Jobcard, der elektronischen Steuererklärung und vieler anderer Verfahren mit Infrastruktur-Charakter werden von den politischen Akteuren und Verwaltungen getroffen. In Bereichen mit privatisierten Dienstleistungen sind Marktprozesse die Treiber für die Gestaltung und nicht Beteiligungsprozesse. Echte Beteiligungsprozesse werden in diesem Technikfeld gesellschaftlich in der Regel nicht organisiert. Bürgerbeteiligung in begrenztem Umfang wird von den Entscheidungsträgern allenfalls dann als hilfreich angesehen, wenn die Nutzung der entstehenden Produkte freiwillig ist und durch den Beteiligungsprozess eine größere Verbreitung oder ein größerer Nutzen (für die Verwaltung) erwartet wird. Ein Beispiel für ein solches Technikprojekt mit gewisser Bürgerbeteiligung sind Bürgerportale.[38]

Allerdings bauen Vereine und Bürgerplattformen Netzwerke auf, um auf politische Projekte oder Entscheidungen Einfluss zu nehmen. Über elektronische Kampagnen können so auch für kritische Stellungnahmen zu Themen der Informationsgesellschaft viele Unterstützer gewonnen werden.[39] Diese Form von „Beteiligung“ kann IT-Projekte verhindern oder zu Anpassungen von Rahmenbedingungen führen. Sie erwächst allerdings aus Konfrontation und nicht aus einem vorausschauenden Beteiligungsansatz.

b) Verletzlichkeitsreduzierung als Motivation:
Im betrieblichen Bereich kann Beteiligung mit positiven Effekten angenommen werden – sie wird allerdings durch Mitbestimmungsverfahren ausgelöst und lässt sich nicht auf die Anwendung des Gestaltungsvorschlags zurückführen.

Soweit ersichtlich, spielt der Gestaltungsvorschlag auf gesamtgesellschaftlicher Ebene kaum eine Rolle. Vielmehr überlässt man dieses Gestaltungsprinzip weitgehend dem Markt. Systematische verletzlichkeitsreduzierende Gestaltung im Rahmen der Ordnungspolitik für den IuK-Bereich ist nicht erkennbar.

Allerdings gibt es auch Beispiele, die in die richtige Richtung weisen: Bisweilen stehen die Vorgaben zur Sicherheit allgemein im Gesetz und die Ausfüllung

38 *http://www.cio.bund.de/DE/E-Government/E-Government-Programm/Buergerportale/buergerportale_node.html*
39 Siehe z.B. *https://www.campact.de*.

durch untergesetzliche Regelungen erfolgt in einem offenen Verfahren mit Beteiligung. Solche Konsultationsprozesse fanden etwa zum BSI-Schutzprofil für Smart Meter mit Einbindung unter anderem von Datenschutzbeauftragten und Verbraucherverbänden statt. Die Bundesnetzagentur führt einen Konsultationsprozess zu Informationssicherheitsmanagementsystemen bei Energieversorgern durch.[40]

(10) Schadenspotentiale in Kosten-Nutzen-Rechnungen berücksichtigen

Auf ökonomische Vorteile und Komfortgewinn durch die IuK-Technik ist zu verzichten, wenn diese nur mit einem hohen Schadenspotential erkauft werden können.

Das Risiko von Hochgeschwindigkeitszügen ist beispielsweise durch den geringen Zeitgewinn nicht zu rechtfertigen. Ebenso wenig kann eine bessere Kapazitätsauslastung von Flughäfen oder die Bequemlichkeit und Umweltfreundlichkeit von Auto-Konvois das durch sie hervorgerufene Risiko legitimieren. Selbst wenn die computerintegrierte und zeitgenaue Produktion gegenüber weniger vernetzten und zentral gesteuerten Produktionskonzepten wirtschaftliche Vorteile bieten, ist zu fragen, ob diese das Risiko wert sein können, das mit einem Produktionsausfall verbunden ist.

Einschätzung

a) Relevanz des Gestaltungsprinzips in der IT-Entwicklung:
Die Vermeidung hoher Schadenspotentiale ist bisher kein Ziel von Unternehmen und öffentlicher Verwaltung. Noch viel weniger wird auf ökonomische Vorteile verzichtet, um hohe Schadenspotentiale zu vermeiden. Größere Flugzeuge und schnellere Züge sind Beispiele für Technikeinsatz mit größeren Schadenspotentialen. Das Instrument der Schutzbedarfsfeststellung und die Vorgaben zu einem IT-Grundschutz haben zwar vermutlich zu einer größeren Berücksichtigung von Risiken geführt. In der Praxis führt dies jedoch bisher nicht zum Verzicht auf Technologien mit hohem Schadenspotential, sondern es wird in der Regel in Maßnahmen zur Verminderung der Störfall-Wahrscheinlichkeit investiert.

b) Verletzlichkeitsreduzierung als Motivation:
Das Gestaltungsprinzip kommt in der Praxis nicht zum Tragen.

40 *http://www.bundesnetzagentur.de/cln_1412/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit_node.html*.

5 Zusammenfassung

In diesem Kapitel fassen wir die Ergebnisse aus dem Review der Thesen und der Gestaltungsvorschläge zusammen und ziehen Schlussfolgerungen bezüglich des Forschungsansatzes.

5.1 Zur Relevanz der Thesen

Die folgende Tabelle fasst die Bewertungsergebnisse aus Kapitel 3 für die Bestätigung der Thesen zusammen.

Tabelle 2: Kurzdarstellung für die Bestätigung der Thesen

These	bestätigt?
(1) Ansteigende Verletzlichkeit	teilweise
(2) Veränderte Struktur der Verletzlichkeit	weitgehend
(3) Praktische Grenzen des Sicherheitsniveaus	ja
(4) Lücken in Sicherungssystemen	ja
(5) Zunahme von Missbrauchsmotiven	nein
(6) Keine Sicherheit vor Insidern und Angriffen mit Malware	weitgehend
(7) Unbeherrschbare IT-Systeme	unsicher
(8) Höheres Schadenspotential durch IT-Einsatz	ja
(9) Zielkonflikt zwischen Sicherheit und Freiheit durch IT-Abhängigkeit	bisher nein
(10) Sicherungszwänge durch IT-Abhängigkeit für die Informationsgesellschaft	bisher nein

Aus der Übersicht ergeben sich drei zusammenfassende Ergebnisse:

- Die Thesen zur Möglichkeit großer gesellschaftlicher Schäden (Thesen 1 – 4, 6 und 8) wurden durch die Entwicklung der vergangenen 25 Jahre bestätigt.
- Das Problem der Beherrschbarkeit von IT-Systemen (These 7) scheint dabei allerdings keinen wesentlichen Einfluss zu haben. Selbst wenn komplexe IT-Systeme nicht mehr vollständig verstanden werden, weisen sie aus gesellschaftlicher Sicht eine für praktische Zwecke ausreichende Beherrschbarkeit auf.
- Die Thesen zur Entwicklung der Missbrauchsmotive (These 5) sowie zum Zielkonflikt zwischen Sicherheit und Freiheit und den resultierenden Sicherungszwängen durch IuK-Verletzlichkeit (Thesen 9 und 10) konnten hingegen nur sehr eingeschränkt oder gar nicht bestätigt werden. Wir nehmen an, dass durch wenige Missbrauchsmotive für gesellschaftlich relevante Aktionen der Sicherungsdruck gering war. Auslöser für die Erwartungen in Thesen 9 und 10 ist allerdings der gesellschaftliche Sicherungsdruck. Insofern scheint das Bild konsistent.

5.2 Zur Relevanz der Gestaltungsvorschläge

In der folgenden Tabelle wird die Relevanz der Gestaltungsvorschläge aus Kapitel 4 zusammengefasst. Zur Erinnerung: Es wird nur die die praktische Relevanz für schwere Störfälle in Organisationen und auf gesamtgesellschaftlicher Ebene betrachtet.

Tabelle 3: Kurzdarstellung der Umsetzung der Gestaltungsvorschläge

Gestaltungsvorschlag	Organisationen	Gesellschaft
(1) Reduzierung von Schadensfolgen	teilweise	offen
(2) Begrenzung von Automatisierung	nein	nein
(3) Substitutionsmöglichkeiten erhalten	nein	kaum
(4) Redundanzen schaffen	teilweise	nein
(5) Diversifizierung anstreben	nein	nein
(6) IuK-Systeme entkoppeln und dezentral nutzen	nein	nein
(7) Fail-Safe-Strategien anwenden	kritische Prozesse mit physischen Wirkungen	nein
(8) Systematische Notfallplanung	teilweise	offen
(9) Technikgestaltung im gesellschaftlichen Konsens	begrenzt	nein
(10) Schadenspotentiale in Kosten-Nutzen-Rechnungen berücksichtigen	nein	nein

Die Übersicht zeigt, dass **Organisationen** teilweise Maßnahmen realisieren, die fünf der Gestaltungsvorschläge entsprechen. Sie dienen dazu, die Auswirkungen technischer Störungen, z. B. im RZ-Betrieb, zu begrenzen. Als Ziel stehen die Interessen der jeweiligen Organisation im Vordergrund.

Für die Gestaltungsvorschläge 2, 3, 5 und 6 nehmen die Autoren dagegen an, dass sich der IT-Einsatz der vergangenen 25 Jahre in die gegenteilige Richtung entwickelt hat. Hier dürfte der Einfluss der Ökonomisierung weiter Lebensbereiche eine große Rolle gespielt haben.

Auf **gesamtgesellschaftlicher Ebene** kommen Maßnahmen, die den vor 25 Jahren entwickelten Gestaltungsvorschlägen entsprechen, dagegen nur in geringem Umfang zum Tragen. In der politischen Diskussion um die Verminderung der Verletzlichkeit der Informationsgesellschaft insgesamt haben sie wohl kaum eine Rolle gespielt.

5.3 Gesamteinschätzung

Insgesamt ergibt sich ein differenziertes Bild der Relevanz von Thesen und Gestaltungsvorschlägen aus der Studie von 1988.

- Die Thesen zur Erhöhung der Verletzlichkeit durch den Einsatz von IuK-Technik waren wohl zutreffend. Diese Entwicklung zu einer höheren Verletzlichkeit ist auch eingetreten, weil die Gestaltungsvorschläge auf gesellschaftlicher Ebene nicht aufgegriffen und umgesetzt wurden.

Bislang sind aber große gesellschaftliche Schäden durch IT-Störungen im Sinne der Verletzlichkeit noch nicht eingetreten. Gründe dafür können sein:

- Die Motivlage für Aktionen gegen die IuK-Technik ist niedriger, als dies in der Studie erwartet wurde.
- „Einfache“ Angriffsformen, die zu schweren Schäden führen, werden in vielen Fällen durch die Sicherheitsmaßnahmen der Organisationen abgewehrt.
- Weitreichende Angriffe sind möglicherweise schwieriger, als dies in der Studie erwartete wurde. Die Kompetenz, die für erfolgreiche Angriffe mit weit reichenden Schäden notwendig ist, könnte daher so hoch sein, dass sie nur wenigen Angreifern zur Verfügung steht.
- Die Störfälle durch Schadsoftware haben gezeigt, dass in vielen Fällen schnelle Reaktionen möglich sind und Schäden dadurch begrenzt werden.
- Zwar ist die gesellschaftliche Informatisierung sehr stark fortgeschritten, jedoch sind zugleich zumindest im Bereich der *IuK-Infrastrukturen* vielfach auch Redundanzen eingebaut worden, so z.B. im Bereich von Backup-Rechenzentren und dem dezentralen Aufbau des Internet. Dies reduziert die Wahrscheinlichkeit von Totalausfällen.

Vielleicht sind auch die Schadenspotentiale aber noch nicht so hoch, wie dies in der Studie erwartet wurde. Gründe hierfür könnten sein:

- IT-Systeme werden so betrieben, dass sie im alltäglichen Gebrauch noch beherrscht werden. Dazu müssen sie nicht verstanden werden.
- Angriffe und Störungen, an deren Ursachen der Einsatz von IuK-Technik wesentlich beteiligt ist, haben aus gesellschaftlicher Perspektive in den meisten Fällen nur relativ kleine Schäden zur Folge. Angreifer mit monetären Interessen „sammeln“ ihre Gewinne oft über viele kleine Aktionen ein – die Schäden treffen primär Individuen und Organisationen.
- Wo Organisationen relevante Risiken sehen, versuchen sie teilweise, sie zu verlagern oder auch mit Hilfe von IT zu vermeiden oder zu begrenzen.

Auch der erwartete Zielkonflikt zwischen Sicherheit und Freiheit ist nicht durch die Verwundbarkeit von IT-Systemen, sondern durch klassischen Terrorismus verursacht.

5.4 Tragfähigkeit des Forschungsansatzes

Gesellschaftliche Randbedingungen haben sich in unerwarteter Weise verändert. In vielen Fällen verlief die technische Entwicklung anders, als dies vor 25 Jahren angenommen wurde. Dennoch weisen die Thesen nicht ins Leere. Auch wenn manche der Erwartungen nicht eingetroffen sind, scheinen die Thesen für die heutige Situation relevant zu sein.

IT wird trotz teilweise abweichender technischer Entwicklungen heute mindestens so intensiv genutzt, wie dies 1988 angenommen wurde. Aus dieser abstrakten Perspektive lässt sich deshalb festhalten:

- Trotz der Abweichungen in der technischen Entwicklung und der Verwendung der IT sind die erwarteten Abhängigkeiten entstanden.
- Derzeit sind Sicherungszwänge durch die Verwundbarkeit der IuK-Technik nicht eingetreten. Das ‚Potential' zu solchen Sicherungszwängen scheint angesichts der sehr hohen Abhängigkeit aber dennoch gegeben.

Die Methode der konditionalen Prognose war daher für die Fragestellung des damaligen Projekts ein zielführender Forschungsansatz.

Durch die Retrospektive werden auch die Veränderungen in den politischen Steuerungsmöglichkeiten deutlich. Durch die Privatisierung mit der gewollten starken Konkurrenz in verschiedenen Technik- und Anwendungsfeldern ist eine verletzlichkeitsreduzierende Steuerung heute noch ungleich schwerer als vor 25 Jahren. Allerdings kann die Verletzlichkeit unter günstigen Umständen durch das Auftreten verschiedener neuer Anbieter im Markt im Vergleich zu einem Monopolisten auch sinken. Umso mehr scheint es geboten, die Chancen der Dezentralisierung im Bereich der Energieversorgung zu nutzen. Das Ende der Informatisierung ist nicht absehbar. Die Abhängigkeit von der Stromversorgung wird daher ebenfalls weiter wachsen. Eine Stromversorgung mit teilautarken Inseln könnte die Verletzlichkeit der Gesellschaft zumindest für diesen Teil der Infrastruktur reduzieren.

Die Retrospektive erlaubt aber zugleich auch eine kritische Reflektion über die in der Studie von 1988 gewählte Methode. Aus dem oben Beschriebenen lässt sich die Schnittmenge und die Abweichung zwischen Prognose und heutiger Wirklichkeit erkennen. Die Abweichungen wiederum geben einen ersten Eindruck von den Chancen und Grenzen einer Forschungsperspektive von 20 Jahren, die der damalige Fokus waren. Im Rückblick zeigen sich – wie zu erwarten –

- die Zeitbedingtheit der damaligen Aussagen,
- die Grenzen einer konditionalen Prognose bezüglich der Technikentwicklung und -nutzung, die von den angenommenen Randbedingungen und den erwarteten Entwicklungstrends abhängt, und
- die Wechselwirkungen zwischen Technologie-Entwicklung (objektive Ebene) und der realen gesellschaftlichen Aneignung und Bewertung.

Für die Anwendbarkeit der konditionalen Prognose heißt dies: Da die Entwicklung von Techniksystemen und Anwendungsformen heute noch dynamischer ist als damals, dürfte ein Szenario und seine Implikationen heute umso schwerer abzuschätzen sein. Als Konsequenz für die Methode könnten z. B. der Zeithorizont der Prognose verkürzt und im Abstand von wenigen Jahren die Szenarios und abgeleiteten Ergebnissen überprüft werden.

5.5 IT als Überwachungsinfrastruktur

Wir kommen zum Schluss, dass trotz großer Abhängigkeit der Gesellschaft von der Informationstechnik genau diese Abhängigkeit noch nicht wesentlich zu Überwachungsmaßnahmen geführt hat. Dies ist das Ergebnis des vorliegenden Aufsatzes, der „Überprüfung von Gestaltungsvorschlägen und Thesen von

1988“. Die Fragestellung wurde damals aus der Perspektive auf die „alte“ Bundesrepublik bearbeitet. Diese Perspektive setzt daher auch den Rahmen der Überprüfung und der Bewertung des methodischen Vorgehens.

Um aber keinen falschen Eindruck zu erwecken: Wir sehen sehr wohl, dass Informationstechnik massiv zur umfassenden und allgegenwärtigen Überwachung eingesetzt wird. Wer es nicht schon vermutet hatte, kann es nach Snowden nicht mehr abstreiten. Informationstechnik hat unter diesem Blickwinkel eine andere Rolle: Sie schafft überhaupt erst die Möglichkeiten für die entgrenzte Überwachung. Dies gilt – wie die anlass- und grenzenlosen Überwachungspraktiken der NSA mit Hilfe von Prism, Tempora und XKeyscore zeigen – potenziell für jeden Menschen auf der Welt, der IuK-Techniken nutzt.

Die primäre Motivation für eine allumfassende Überwachung vieler Sicherheitsbehörden ist aber nicht die Verletzlichkeit der Gesellschaft durch Informationstechnik. Die Notwendigkeit der Überwachung wird vielfach mit allgegenwärtigem Terrorismus oder schweren Straftaten begründet. Zu befürchten ist aber, dass andere Gründe mindestens genauso wichtig sind – beispielsweise Industriespionage und politische Einflussnahme. Im Verständnis der Dienste wird Überwachung zum Selbstzweck. Kontrolle über die Dienste wird abgewehrt oder umgangen.

Im eingangs beschrieben Projekt war neben der Verletzlichkeit auch die Frage der Verfassungsverträglichkeit der Informationsgesellschaft für viele Gesellschaftsbereiche untersucht worden.[41] Mit Blick auf die Realisierungsbedingungen der Grundrechte war in diesem Teil des Projekts erwartet worden, dass für die Sicherheitsbehörden ein erheblicher Druck entsteht, IT für ihre Zwecke einzusetzen, unter anderem durch Profilbildung und präventive Aufklärungsstrategien.[42] Als Folge wurde mit einer Machtverschiebung zwischen Sicherheitsbehörden und Bürgern und einem Transparenzverlust gerechnet. Die Erwartung aus diesem Teil der Studie wurde insbesondere im Bereich der Geheimdienste voll bestätigt. Die internationalen Akteure, die damals so nicht im Fokus standen, haben sie auf nicht vorstellbare Weise übertroffen.

6 Ausblick

In diesem Beitrag haben wir unsere Einschätzungen zur Gültigkeit der damaligen konditionalen Prognosen und zur Relevanz der damaligen Gestaltungsvorschläge zur Verletzlichkeit der Informationsgesellschaft wiedergegeben. Wie eingangs geschrieben, erheben die schlaglichtartigen Einschätzungen nicht den Anspruch umfassender und tiefgehender Forschungsergebnisse.

Die Retrospektive über 25 Jahre bietet Einblicke in die Zeitgeschichte bezüglich der sozialen Bewertung von Techniknutzung. Trotz der größeren Durchdringung und sehr hohen Selbstverständlichkeit der überall verfügbaren IuK-Dienste scheint das Bewusstsein für die Abhängigkeit von der Technik in der Breite der Gesellschaft heute nur geringfügig höher als vor 25 Jahren. Die Einschätzungen

41 *Roßnagel/Wedde/Hammer/Pordesch 1990a.*

42 *Roßnagel/Wedde/Hammer/Pordesch 1990a, 138 ff.*

oben zeigen aber, dass das Bewertungs- und Gestaltungskriterium „Verletzlichkeit“ für die Informationsgesellschaft immer noch hohe Relevanz besitzt. Weitere wissenschaftliche Analysen wären deshalb lohnend. Nachfolgend werden einige Forschungsfragen skizziert, die die heutige Lage für eine Diskussion in Politik und Gesellschaft aufbereiten würden.

1. Self-destroying Prophecy (analog zum Jahr-2000-Problem)?

Die Ereignisse, die in den vergangenen 25 Jahren große Schäden für Gesellschaften ausgelöst haben, waren nicht von Effekten aus IT-Störungen bestimmt. Vielmehr haben die Terroranschläge und die „innovativen Produkte“ der Finanzindustrie zu Verwerfungen der Finanzmärkte geführt, die weltweit nur schwer zu beherrschen waren. Auch einige Umweltkatastrophen waren für die betroffenen Staaten schwerwiegender als die schwersten IT-Störungen. Insofern muss festgestellt werden, dass die Veränderungen der Schadenspotentiale durch den wachsenden IT-Einsatz bisher noch nicht in Störfällen mit gesellschaftlich hohen Schäden zum Tragen kamen.

Forschungsfragen: Ist die Verletzlichkeit nicht in dem Maße gestiegen, wie dies in der Studie erwartet wurde? Liegen die Gründe darin, dass die Aufgabe sowohl von Organisationen wie von staatlicher Seite angegangen wurde? Welchen Anteil an der Verletzlichkeit nehmen angesichts der weiten Durchdringung der IuK-Technik heute die Infrastruktur und die Anwendungsebene ein? Welchen Anteil an den weltweit wahrgenommenen und umgesetzten Überwachungszwängen hat die steigende Abhängigkeit von IuK-Systemen? Wie werden sich diese Anteile an einem allgemeinen Sicherungszwang weiter entwickeln, beispielsweise im Kontext der (Anti-)Cyberwar-Aktivitäten?

2. In welchem Umfang führen gesellschaftliche Gewöhnungseffekte zu einem Sicherheitsparadox?

Die Gesellschaft hat sich an die Verfügbarkeit gewöhnt und vergisst allmählich die Risiken. Je länger es gut geht, umso mehr verliert das Thema an öffentlicher Wahrnehmung.

Forschungsfragen: Wenn in der Zukunft schwere Störungen für die Gesellschaft virulent werden, könnten sie dafür umso wirkungsmächtiger sein. Wie stark ist dieser Effekt? Wie kann ggf. die Notwendigkeit von verletzlichkeitsreduzierender Technikgestaltung im gesellschaftlichen Bewusstsein wachgehalten werden?

3. Ist die „bedingte Beherrschbarkeit“ von IuK-Systemen langfristig ausreichend?

Wie oben ausgeführt, sind viele IT-Systemen für praktische Zwecke ausreichend beherrscht oder beherrschbar. Oft bestehen gar nicht (mehr) der Anspruch und die Möglichkeit, die IT-Systeme vollständig zu verstehen.

Forschungsfragen: Inwieweit kann eine bedingte Beherrschbarkeit als Ergebnis der Technikentwicklung, betrieblicher Einsatzstrategien und gesellschaftlicher Lernprozess im Umgang mit Informationssystemen gesehen werden? Ist dies

langfristig ausreichend, um das das gesellschaftliche Leben basierend auf IT-Systemen erfolgreich zu organisieren? Welche Auswirkungen hat das auf die Verletzlichkeit? Sollten durch Regulierung für bestimmte Anwendungsbereiche Beherrschbarkeitsvorgaben gemacht werden.

4. Welche Möglichkeiten zur verletzlichkeitsreduzierenden Technikgestaltung bestehen heute?

In den vergangenen 25 Jahren wurden für die Politik die Möglichkeiten zur Steuerung des Technikeinsatzes sehr weit reduziert. Kommt eine neue Untersuchung zum Ergebnis, dass die Verletzlichkeit der Gesellschaft hoch ist, dann ergibt sich daraus die politische Notwenigkeit zu Technikgestaltung. Denn: Alleine Maßnahmen zur Verringerung der Störfallwahrscheinlichkeit sind nicht adäquat. Angesichts der veränderten IuK-Technologien ergeben sich im Konkreten vermutlich veränderte Handlungsbedarfe und Gestaltungsmöglichkeiten.

Forschungsfragen: Welche Gestaltungsmöglichkeiten sind unter den heutigen Einsatzszenarien von IuK-Systemen effektiv und adäquat? Wie können unter den heutigen Rahmenbedingungen die Akteure motiviert werden, IuK-Systeme verletzlichkeitsreduzierend einzusetzen? Welche Steuerungsmöglichkeiten können die nationalen und internationalen politischen Gremien zur verletzlichkeitsreduzierenden Technikgestaltung nutzen?

Die Ergebnisse zu diesen und weiteren Forschungsfragen würden die Verantwortlichen in Politik und Gesellschaft über die Notwendigkeit und die Möglichkeit einer Steuerung der IuK-Entwicklung informieren. Für die Entscheidungsträger in Politik und in Unternehmen sollten sich Hinweise für die Ausrichtung der IuK-Strategie ergeben.

Referenzen

BMI a: Umsetzungsplan KRITIS des Nationaler Plans zum Schutz der Informationsinfrastrukturen (ohne Veröffentlichungsdatum)

BMI 2005: Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI), Berlin 2005.

BMI 2009: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Juni 2009.

BSI 100-4 - Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 Notfallmanagement, Version 1.0, Bonn 2008; http://www.bsi.bund.de/gshb.

BSI 2005a: Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen - Zusammenfassung.

BSI 2008: Internationale Aktivitäten zum Schutz Kritischer Infrastrukturen, 2004 und 2008.

Hammer, V. (1999): Die 2. Dimension der IT-Sicherheit - Verletzlichkeitsreduzierende Technikgestaltung am Beispiel von Public Key Infrastrukturen, Braunschweig/Wiesbaden, 1999.

Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U. (1990a): Digitalisierung der Grundrechte?, Opladen, 1990a.

Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U. (1990b): Die Verletzlichkeit der 'Informationsgesellschaft', Opladen, 1990.
Elektronisch verfügbar über den Resolving-Dienst der Deutschen Nationalbibliothek, unter *http://nbn-resolving.de/urn:nbn:de:hebis:34-2009103030803* oder von: *www.provet.org/* → Publikationen > 1990.

SARK (1979): Bericht des Verwundbarkeitskomitees "Datenverarbeitung und die Verwundbarkeit der Gesellschaft", Stockholm 1979 (Deutsche Übersetzung).

TAB (Hrsg.) - Petermann, T. / Bradke, H. / Lüllmann, A. / Poetzsch, M. / Riehm, U. (2010): Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen Ausfalls der Stromversorgung, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag; Berlin, 2010; http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab141.pdf (Abruf am 26.02.2013).

Wischenhöfer, C. (2013): Koordinierung der IT-Sicherheitsnormung - Initiativen des DIN, DuD 1/2013, 30 ff.

Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
KRITIS	Kritische Infrastrukturen; Programm von Bundesregierung und Behörden zum Schutz derselben
IuK-Technik	Informations- und Kommunikationstechnik
MaRisk	Mindestanforderungen an das Risikomanagement an Unternehmen in der Finanzwirtschaft; verschiedene verbindliche Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
provet	Projektgruppe verfassungsverträgliche Technikgestaltung
BMI	Bundesministerium des Innern

Autoren

Prof. Dr. Urs Andelfinger promovierte 1995 zur diskursiven Anforderungsanalyse an der TH Darmstadt, wo er auch wissenschaftlicher Mitarbeiter am Zentrum für Interdisziplinäre Technikforschung (ZIT) war**.** Danach war er mehrere Jahre als Softwareingenieur in der Industrie tätig. Seit 2004 unterrichtet er Wirtschaftsinformatik, Softwaretechnik und ‚Informatik und Gesellschaft' an der Hochschule Darmstadt.

Dr. Volker Hammer war von 1986 bis 1998 Mitarbeiter der Projektgruppe verfassungsverträgliche Technikgestaltung - provet e. V. 1998 promovierte er zur „verletzlichkeitsreduzierenden Technikgestaltung am Beispiel von Public Key Infrastrukturen" an der TH Darmstadt. Seit 1998 ist er Mitarbeiter der Secorvo Security Consulting GmbH mit Arbeitsschwerpunkten u. a. in den Bereichen PKI, Verletzlichkeit und Datenschutz.

Dr. Ulrich Pordesch war nach seinem Informatikstudium zunächst bei der Projektgruppe verfassungsverträgliche Technikgestaltung (provet e.V.) und dann auch bei der Gesellschaft für Mathematik und Datenverarbeitung (GMD) in der interdisziplinären Forschung zwischen Informatik und Recht tätig. 2002 promovierte zum Thema "Die elektronische Form und das Präsentationsproblem". Seit 2004 ist er IT-Sicherheitskoordinator der Fraunhofer Gesellschaft e.V.

Prof. Dr. Alexander Roßnagel ist Universitätsprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel. Wissenschaftlicher Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel, Promotion 1981, Habilitation 1991, Forschungspreis der Alcatel Lucent-Stiftung 1993, Fellow der Gesellschaft für Informatik 2007, von 2003 bis 2011 Vizepräsident der Universität Kassel.

Dr. Roland Steidle ist Fachanwalt für Informationstechnologierecht und Partner in der Kanzlei SWM Rechtsanwälte. Von 2002 bis 2003 war er wissenschaftlicher Mitarbeiter von Prof. Roßnagel an der Universität Kassel in den Projekten „Multimedia Arbeitsplatz der Zukunft" (MAP21) und der elektronischen Langzeitarchivierung (ArchiSig) und promovierte 2005 im Multimedia- und Datenschutzrecht. Er ist spezialisiert auf IT-Recht und berät schwerpunktmäßig in den Bereichen Datenschutz, Outsourcing, IT-Vertrags- und Lizenzrecht, intentionalem Markenrecht, E-Commerce und Social Media.