DuD
Datenschutz und Datensicherheit

Verletzlichkeitsreduzierende Technikgestaltung

Volker Hammer

Um „Sicherheit" für soziale Systeme zu erreichen, müssen nicht nur Schadenswahrscheinlichkeiten verringert, sondern insbesondere Schadenspotentiale begrenzt und Beobachtungs- und Handlungsoptionen für schwere Störfälle bereitgestellt werden. Dies ist das Ziel der verletzlichkeitsreduzierenden Technikgestaltung. Der Beitrag motiviert das Konzept der technikspezifischen Störungsdynamik und stellt die sozio-technischen Kriterien für die Anforderungsanalyse zur verletzlichkeitsreduzierenden Technikgestaltung vor.[1]

Dr.-Ing.
Volker Hammer

Secorvo Security Consulting GmbH.
Arbeitsschwerpunkt: Public Key Infrastrukturen, digitale Signaturen, Anforderungsanalyse, Technikgestaltung
E-Mail: hammer@secorvo.de

Einleitung

Jedes Fachgebiet gestaltet sein „Universum", die eigene Sicht und das Verständnis der Welt durch (Fach-) Begriffe. In diesem begrifflichen Universum verstecken sich zumeist aber auch ganz spezielle Sichtweisen. Nicht anders in der IT-Sicherheit: So heben die „klassischen" anwendungsorientierten und relativierenden IT-Sicherheitsbegriffe darauf ab, dass die trotz Sicherungsmaßnahmen verbleibenden Risiken tragbar sein sollen.[2] Welche Risiken aber sind tragbar? Und: unterstützen die methodischen Instrumente der IT-Sicherheit, dass die Techniksysteme entsprechend der identifizierten Risikopräferenzen gestaltet oder eingesetzt werden können?

Der Beitrag zeigt, dass herkömmliche Ansätze der IT-Sicherheit um die Zielsetzung erweitert werden müssen, Schadenspotentiale gering zu halten (verletzlichkeitsreduzierende Technikgestaltung). Dazu sind die Zusammenhänge zwischen Störungsverlauf und Schadenspotential zu berücksichtigen (Störungsdynamik). Die verletzlichkeitsreduzierende Technikgestaltung kann schließlich durch ein Kriteriensystem für die Anforderungsanalyse methodisch unterstützt werden. Drei Beispiele deuten die Anwendung der Kriterien an.

1 Ausgangspunkte

Die Bewertung von „Risiko" wird durch (mindestens) zwei Dimensionen bestimmt: die Schadenswahrscheinlichkeit und das Schadenspotential. In der technischen Risikoformel werden diese beiden Faktoren linear verknüpft. Sicherheitsmaßnahmen werden insofern als gleichwertig angesehen, als sie eine der beiden Dimensionen im gleichen Umfang günstig beeinflussen. Die Ausgangspunkte der verletzlichkeitsreduzierenden Technikgestaltung werden dagegen aus sozialen Ansätzen zur Bewertung von Risiken gewonnen. Dabei zeigt sich, dass das Schadenspotential im Unterschied zur klassischen Risikoformel überproportional in die Bewertung eingeht und weitere Vorgaben für die Technikgestaltung berücksichtigt werden sollten.[3]

1.1 Soziale Bewertung von Risiken

Intuitive Risikokonzepte aus der Psychologie zeigen Faktoren auf, die mit einer „hohen" Risikobewertung durch Individuen korrelieren.[4] Risiken werden danach als „hoch" bewertet, wenn sie ein Katastrophenpotential beinhalten, unfreiwillig eingegangen werden müssen oder noch unbekannt sind.

Technikanwendungen sollen mit den *Zielen des Grundgesetzes* verträglich sein oder diese sogar fördern (Verfassungsverträglichkeit).[5] Dürfen sich hohe Schadenspotentiale jedoch unter keinen Umständen realisieren, können Technikbetreiber und Gesellschaft zu sozialen Sicherungsmaßnahmen gezwungen sein. Sicherheitsüberprüfungen, Kontroll- und Überwachungsmaßnahmen oder die Beobachtung des sozialen Umfeldes führen jedoch zu Einschränkungen der Realisierungsbedingungen von individuellen Freiheitsrechten. Mittelbar können auch die Voraussetzungen der demokratischen Willensbildung beeinträchtigt werden. Können Störungen weitreichende Auswirkungen auf die Versorgung der Bevölkerung mit lebensnotwendigen Gütern und Leistungen haben, kann die staatliche Pflicht zur Daseinsvorsorge vernachlässigt sein. Schließlich trifft den Staat als demokratisch legitimiertes und verpflichtetes Organ des All-

[1] Der Aufsatz ist eine überarbeitete Fassung eines Beitrags zur Tagung „VIS '99" (Hammer 1999b). Er gibt einen Überblick über Ergebnisse aus Hammer 1999a.

[2] So Z. B. in BSI 1997, Kap. 1-5, oder in Amann/Atzmüller, DuD 1992, 287.

[3] Vgl. zum folgenden Abschnitt auch das Gateway „Risiko" in diesem Heft. und ausführliche Hammer 1999a mwN.

[4] Z. B. Jungermann / Slovic 1993, 167 ff.; Rudinger / Espey / Holte / Neuf 1996, 128 ff.

[5] Vgl. zu diesem Absatz z. B. Roßnagel / Wedde / Hammer / Pordesch 1990a und Roßnagel / Wedde / Hammer / Pordesch 1990b, 171 ff.; Roßnagel 1995, 56 ff.; sowie Fuhrmann in diesem Heft.

gemeininteresses auch eine Schutzpflicht für Leben und Gesundheit des Einzelnen und zur Vermeidung von Katastrophen gesellschaftlichen Ausmaßes.

Vertreter aus der Soziologie, Politologie, Fehlerpsychologie und anderen Disziplinen weisen zudem darauf hin,[6] dass im Falle von hohen Schadenspotentialen die *Überlebens- und Lernfähigkeit* sozialer Systeme verschlechtert wird. Lernfähigkeit meint in diesem Zusammenhang, dass das soziale System Kenntnisse und Fähigkeiten im Umgang mit dem technischen System erwerben und sich, falls erforderlich, durch Anpassung auf neue Bedingungen einstellen kann. Dies verbessert auch seine Überlebensfähigkeit. Niedrige Schäden verbessern zudem die Chance, dass Anwender aus Fehlern lernen können. Die Wahrscheinlichkeit, in Störfällen einem Human-Task Mismatch[7] mit schwerwiegenden Folgen zu entgehen, wird dadurch erhöht.

1.2 Normative Vorgaben der Technikgestaltung

Die genannten Ansätze verweisen darauf, dass es ein vordringliches Ziel der Technikgestaltung sein muss, das Schadenspotential niedrig zu halten. Gelingt es darüber hinaus, dass potentiell Betroffene mit den Risiken von IT-Systemen leicht Erfahrungen gewinnen können und selbst entscheiden können, ob und welche Risiken sie eingehen, dürfte auch die Akzeptabilität neuer Techniksysteme deutlich verbessert werden. Werden neue IT-Systeme, wie Public Key Infrastrukturen und rechtsverbindliche digitale Signaturen, nach diesen Prinzipien gestaltet, kann ihre Verbreitung gefördert und beschleunigt werden.

Die Ergebnisse der sozialen Risikobewertung werden deshalb in den folgenden vier Zielen der Technikgestaltung zusammengefasst.[8] Für sie kann erwartet werden, dass sie auf breite Zustimmung als vernünftige Vorgaben einer Technikgestaltung stoßen. Sie werden daher als *normative Vorgaben* bezeichnet.

> (V1) *Niedrige Schadenspotentiale.* Ausgangspunkt für die Bewertung des Schadenspotentials muss die künftige Abhängigkeit sozialer Funktionen vom Techniksystem sein.
> (V2) *Niedrige Schadenswahrscheinlichkeit.*
> (V3) *Autonomie:* Potentiell betroffene soziale Systeme müssen die Höhe ihres Risikos bestimmen und an veränderte Bewertungen anpassen können.
> (V4) *Erfahrungsbildung:* Risiken sollen „erfahrbar" sein. Die Technikgestaltung muss deshalb eine möglichst umfassende Erfahrungsbildung über das Systemverhalten im Normalbetrieb und in Störungssituationen erlauben.

Diese vier normativen Vorgaben sind für eine sozialverträgliche Technikgestaltung allerdings nicht gleich wichtig: Die größten Gewinne sind zu erwarten, wenn es gelingt, Schadenspotentiale niedrig zu halten, weil dadurch z. B. soziale Sicherungszwänge vermieden und die Erfahrungsbildung gefördert werden können. Dagegen wird in herkömmlichen Risikobetrachtungen häufig ohne weitere Begründung vorrangig die Schadenswahrscheinlichkeit betrachtet.

Damit sind die Grundlagen für eine bgriffliche Bestimmung von Verletzlichkeit gegeben. Unter **Verletzlichkeit** wird die Möglichkeit großer Schäden für gesellschaftliche Gruppen, Organisationen oder Individuen verstanden.[9] *Verletzlichkeitsreduzierende Technikgestaltung* ist dementsprechend primär auf die Verminderung hoher Schadenspotentiale gerichtet.

1.3 Ergänzung der „IT-Sicherheit"

„Klassische" Ansätze der IT-Sicherheit konzentrieren sich im Unterschied dazu beispielsweise auf die drei Grundbedrohungen „Schutz der Vertraulichkeit", „Schutz der Integrität" und „Schutz der Verfügbarkeit" sowie die korrespondierenden Schutzziele.[10] Die Maßnahmen, die aus diesen Schutzzielen für die Technikgestaltung abgeleitet werden, sind weitgehend an der Technik orientiert und bemühen sich vorrangig, die Wahrscheinlichkeit von Störfällen gering zu halten.[11] Ein Ansatz, der die schadenspotentialorientierte Gestaltung unterstützt, ist daher eine wichtige Ergänzung der IT-Sicherheit.

Für eine stärkere Berücksichtigung von Schadenspotentialen in der Technikgestaltung spricht auch, dass sie für künftige Systeme vergleichsweise gut abgeschätzt werden können. Dagegen liegen für die Schadenswahrscheinlichkeiten, insbesondere für neue und komplexe Systeme oder soziale Fakoren, häufig keine geeigneten Zahlen vor.[12]

Sicherungsziele sollen im praktischen Einsatz von IT-Systemen erreicht werden können. Dazu sind die entsprechenden Eigenschaften der IT-Systeme bereits in der Implementierung vorzusehen. Auch die schadenspotentialorientierten Maßnahmen müssen bereits in der Anforderungsanalyse spezifiziert werden. Ausgangspunkt einer verletzlichkeitsreduzierenden Technikgestaltung sind die vier oben genannten normativen Vorgaben.

1.4 Methodische Konzepte

Für eine konkrete Technikgestaltung sind die generalklauselartigen normativen Vorgaben allerdings nicht geeignet. Zwischen diesen und technischen Spezifikationen liegt eine Beschreibungslücke, die mit Hilfe der Methode der „normativen Anforderungsanalyse" (NORA) überwunden werden kann. Dazu wird in mehreren Konkretisierungsschritten ein Kriteriensystem mit mehreren Ebenen entwickelt.[13] Jede dieser Ebenen entspricht einem Modell, in dem die normativen Vorgaben, das zu gestaltende Technikfeld und der Anwendungskontext mit zunehmender Techniknähe konkretisiert werden (vgl. Abb. 1). Exemplarisch wird im folgenden aus diesem Kriteriensystem die

[6] Vgl. z. B. Guggenberger 1987; Wehner, BSI-Forum 1993, 49f., oder Weizsäcker / Weizsäcker 1984, 167 ff.

[7] Leveson 1995, 91-126, bezeichnet damit Situationen, in denen Operateure die Aufgabe, ein technisches System zu steuern, *nicht erfüllen können*, weil dies durch die Situation und das Techniksystem verhindert wird. Ein Grund können unzureichende oder verfälschte Informationen über Störungsursachen sein.

[8] Siehe zum folgenden Hammer 1999a, Kap. 7 und die Begründungen in Kap. 4-6 mwN.

[9] Roßnagel/Wedde/Hammer/Pordesch 1990a, 7; provet/GMD 1994, 20f. Ähnlich SARK 1979, 45.

[10] Z. B. ITSEC 1993, 427 ff.

[11] Vgl. dazu und zum folgenden die Analyse in Hammer 1999a, Kap. 4 bis 6. Siehe z. B. auch die Hinweise bei Grimm 1994, 13 ff. und 26 ff.

[12] Siehe dazu auch das Gateway „Risiko" in diesem Heft .

[13] Die normative Anforderungsanalyse ist eine methodische Weiterentwicklung der „schrittweisen Konkretisierung rechtlicher Anforderungen" (KORA). Der methodische Ansatz wurde erfolgreich für die rechtsgemäße Technikgestaltung, für psycho-soziale Vorgaben und die verletzlichkeitsreduzierende Technikgestaltung und für verschiedene Technikfelder eingesetzt. Zur Methode und Entwicklung siehe Hammer 1999a, Kap. 9 mit weiteren Nachweisen.

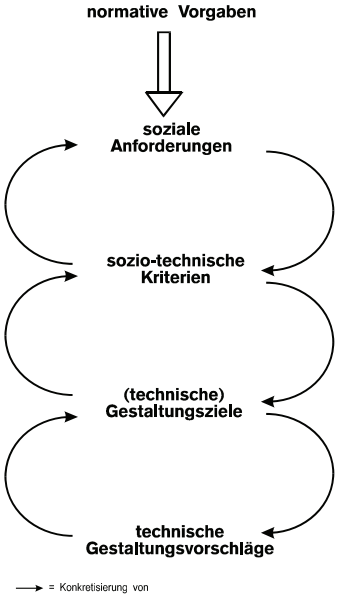

Abb. 1: Die Konkretisierungsebenen nach NORA

Ebene der sozio-technischen Kriterien vorgestellt.[14]

Vom Einsatz eines Techniksystems können verschiedene soziale Systeme betroffen sein, die unterschiedliche Interessen verfolgen. Daher wird nach NORA mit den Kriterien eine Anforderungsanalyse aus der Perspektive unterschiedlicher Rollen vorgenommen. Aus den entstehenden unterschiedlichen technischen Gestaltungszielen ist für eine konkrete Technikrealisierung eine Balancierung der Risiken anzustreben, die allen potentiell Betroffenen gerecht wird.

Schließlich wird ein Ansatz benötigt, mit dem vorlaufend hohe Schadenspotentiale identifiziert werden können. Als geeignet hat sich das Konzept der „technikspezifischen Störungsdynamik“ erwiesen, das im folgenden skizziert wird.

2 IT Beiträge zum Schadenspotential

Primär sollen Störfälle mit hohem Schadenspotential vermieden bzw. beherrscht werden. Für die verletzlichkeitsreduzierende Technikgestaltung bietet es sich daher an, technikspezifische Beiträge von IT-Systemen zu Schadenspotentialen gering zu halten oder zu vermeiden. Methodisch werden dazu Zusammenhänge zwischen dem auslösenden Ereignis und dem Schaden identifiziert.[15] Potentiell hohe Schäden können zum einen aus einem primären Störereignis entstehen, wenn ein *hoher Einzelschaden* möglich ist. Zum anderen sind hohe Schadenspotentiale möglich, wenn eine *Menge von Schäden* gemeinsam bewertet wird, weil sie auf die gleiche Störungsursache zurückzuführen sind. Hohe Schadenssummen entstehen in diesem Fall durch Störungsverläufe. Dabei darf nicht nur die Fehlerausbreitung im technischen System betrachtet werden. Gleichermaßen relevant für Störungsverläufe ist die sozio-technische Einbettung. Höhere Schäden sind nämlich auch dann zu erwarten, wenn die Störung nicht rechtzeitig erkannt werden kann oder die Handlungsmöglichkeiten nicht ausreichen, um den Störfall zu beherrschen. Die Zwangsläufigkeit, mit der sich ein primäres Störereignis ausbreitet und zu Einschränkungen für soziale Funktionen führt, wird im weiteren als *Störungsdynamik* bezeichnet. Unzureichende Beobachtungs- und Handlungsmöglichkeiten können somit zu einer hohen Störungsdynamik beitragen. Um Schadenspotentiale in Abhängigkeit vom Störungsverlauf zu charakterisieren, wird die folgende Unterscheidung von *Schadenstypen* eingeführt (vgl. Tabelle 1).

Die Ausbreitung von Störungen kann unterschiedliche Charakteristika aufweisen. Sie kann linear (Kopplungsschaden) oder als Spezialfall in der Form der automatischen Reproduktion erfolgen (Multiplikationsschaden). Viele Komponenten können auch betroffen sein, wenn sich ein primäres Störereignis über komplexe Abhängigkeiten ausbreitet (Komplexschaden). Durch die Möglichkeit zur Ereignissteuerung kann außerdem eine „außerhalb“ der IT-Systeme liegende Störbedingung zur gleichzeitigen Störung vieler ansonsten unabhängiger Komponenten führen. Die Schadenssumme eines solchen Störfalls wird als Synchronschaden eingeordnet. Prominentes Beispiel waren die als „Jahr 2000-Problem“ befürchteten Störfälle. Schließlich können Schäden, die gleiche oder ähnliche, aber durch technisch unabhängige primäre Störereignisse hervorgerufen wurden, in einem Kumulationsschaden zusammengefasst werden, wenn sie aus der Sicht eines sozialen Systems gemeinsam zu bewerten sind.

Ausbreitung des primären Störereignisses		Schadenstyp
ohne Ausbreitung	einzelnes (Teil-)System	Einzelschaden
	viele unabhängige (Teil-)Systeme durch Ereignissteuerung	Synchronschaden
mit Ausbreitung	lineare Ausbreitung	Kopplungsschaden
	automatische Reproduktion	Multiplikationsschaden
	komplexe Ausbreitung	Komplexschaden

Tabelle 1: Schadenstypen in Abhängigkeit vom Störungsverlauf

Das Konzept der Störungsdynamik wird insbesondere in den im folgenden Abschnitt vorgestellten Kriterien K1 bis K4 aufgegriffen.

3 Sozio-technische Kriterien

Nach NORA werden aus den normativen Vorgaben zunächst mit Blick auf das Anwendungs- und das Technikfeld soziale Anforderungen konkretisiert. In einem weiteren Konkretisierungsschritt werden aus diesen mit dem Schwerpunkt „Schadenspotential“ zehn sozio-technische Kriterien der verletzlichkeitsreduzierenden Technikgestaltung entwickelt (vgl. Abb. 2), die im folgenden vorgestellt werden. Diese sozio-technischen Kriterien beschreiben ein „Modell“ für das Zusammenwirken von sozialem und technischem System, mit dem die normativen Vorgaben erfüllt werden können.[16]

- (K1) *Begrenzte Schadenshöhe*: Auch unter den Bedingungen eines Technikeinsatzes sollen für ein soziales System möglichst für alle Schadenstypen Obergrenzen für die Schadenshöhe durchgesetzt werden. So sind für Kumulations- und Multiplikationsschäden Summenbegrenzungen anzustreben.
- (K2) *Transparenz*: Transparenzmechanismen sollen das Erkennen und Analysieren von Störereignissen und die Planung von Maßnahmen unterstützen. Durch beobachtungsorientierte Siche-

[14] Zur Entwicklung des Kriteriensystems siehe Hammer 1999a, Kap. 10.

[15] Vgl. Hammer 1999a, Kap. 8.

[16] Dazu und zum weiteren siehe die Entwicklung des Kriteriensystems mit den ausführlichen Konkretisierungsschritten in Hammer 1999a, Kap. 10.

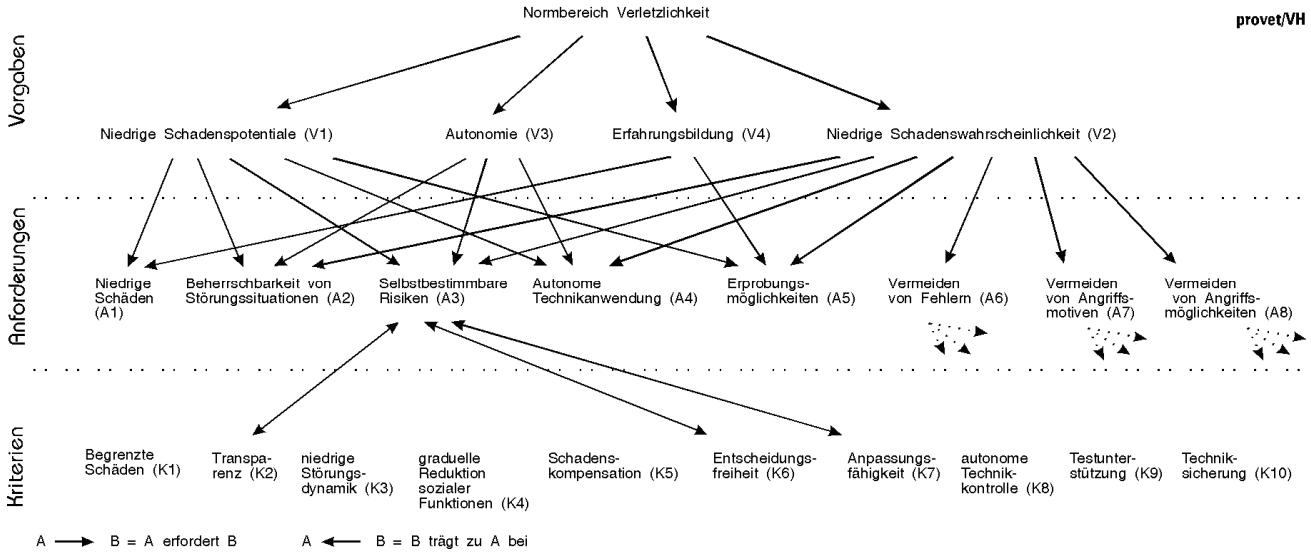

Abb. 2: Vorgaben, Anforderungen und schadenspotentialrelevante Kriterien nach NORA[17]

rungsmaßnahmen sollen soziale Systeme außerdem das sie betreffende Schadenspotential erkennen können. Transparenz kann auch durch einfache Systemstrukturen gefördert werden.

- (K3) *Niedrige Störungsdynamik*: Das Kriterium fordert eine Ausgestaltung von Techniksystemen und Einsatzkonzepten, in der sich Störungen nur schwer und nur langsam ausbreiten können. Dazu sind lose Kopplung und lineare Kopplungsstrukturen anzustreben. Außerdem sind Synchronisationsmechanismen (im oben beschriebenen Sinn) zu vermeiden. Störungsverläufe müssen unterbrochen werden können. Zur losen Kopplung tragen daher auch zeitliche Spielräume oder vorbereitete spezielle und universelle Eingriffsmöglichkeiten für die Operateure bei.
- (K4) *Graduelle Reduktion sozialer Funktionen*: Die graduelle Reduktion sozialer Funktionen ist eine besondere Form der losen Kopplung. Das Kriterium empfiehlt, Techniksysteme so zu strukturieren, dass auch beim Auftreten von Störungen wichtige soziale Kernfunktionen aufrecht erhalten werden können. Dazu können beispielsweise unabhängige Substitutionsmechanismen auf niedrigerem Leistungsniveau zur Verfügung stehen.
- (K5) Die *Unterstützung von Schadenskompensation* kann dazu beitragen, das nachlaufend Schäden ausgeglichen werden. Eingeschlossen sind Maßnahmen zur freiwilligen wie zur (rechtlich) durchsetzbaren[18] Kompensation. Da im Rahmen der verletzlichkeitsreduzierenden Technikgestaltung Schäden vermieden werden sollen, ist dieses Kriterium jedoch nachrangig.
- (K6) *Entscheidungsfreiheit*: Das Kriterium fordert Entscheidungsmöglichkeiten für soziale Systeme bei der Technikeinführung wie auch bei der Technikanwendung bezüglich aller Aspekte, die risikorelevant sind. Dies bezieht sich z. B. auf Schadensobergrenzen, aber auch auf Störungsdynamiken.
- (K7) Das Kriterium *Anpassungsfähigkeit* fordert, dass Techniksysteme in Übereinstimmung mit K6 angepasst werden können und über die Zeit an veränderte Risikobewertungen anpassbar bleiben.
- (K8) Damit soziale Systeme die Techniksysteme im Normalbetrieb selbst steuern und in Störungssituationen handeln können, ist als Option eine *autonome Technikkontrolle* zu fordern. Ob diese Option wahrgenommen wird, unterliegt der Entscheidungsfreiheit (K6).
- (K9) *Testunterstützung* soll es im Wirkbetrieb und in Störungssituationen erlauben, das Verhalten eines IT-Systems zu untersuchen. Dazu sind zum ersten Testfunktionalitäten bereitzustellen. Zum zweiten ist eine Abgrenzung des Testbetriebs notwendig, damit Tests in produktiven Anwendungen keine hohen Schäden verursachen können.
- (K10) Durch *Techniksicherung* sollen die aus den bisher genannten Kriterien abzuleitenden technischen Maßnahmen abgesichert und vor Fehlern und Angriffen geschützt werden. Dazu gehört beispielsweise auch der Schutz von verletzlichkeitsreduzierenden Maßnahmen durch eine geeignete Zugangs- und Zugriffskontrolle.

Diese sozio-technischen Kriterien werden in der Anforderungsanalyse für Techniksysteme verwendet, um Gestaltungsalternativen zu suchen oder auszuwählen.

4 Anwendung der Kriterien

4.1 Technische Gestaltungsziele

Die sozio-technischen Kriterien zur verletzlichkeitsreduzierenden Technikgestaltung konnten unabhängig von konkreten Techniksystemen und Anwendungskontexten formuliert werden. Im dritten Konkretisierungsschritt werden sie jedoch auf technische Gestaltungsobjekte angewendet, z. B. auf Komponenten von Public Key Infrastrukturen wie die Funktionalität von Trä-

[17] Die Relationen zwischen Anforderungen und Kriterien sind nur beispielhaft für A3 dargestellt. A4 bis A8 werden in den hier vorgestellten Kriterien nur in ihren schadenspotentialrelevanten Anteilen berücksichtigt.

[18] Vgl. dazu auch den Ansatz des Gleichgewichtsmodells bei Grimm 1994.

germedien für Signaturschlüssel, die Eigenschaften von Sperrkonzepten oder die Struktur einer Zertifizierungshierarchie.[19] Dazu wird gefragt, welche Eigenschaften diese Gestaltungsobjekte aufweisen müssen, damit die sozio-technischen Kriterien erfüllt werden können. In diesem Schritt müssen vier Bezüge hergestellt werden:

- zur *Größe sozialer Systeme*: Die Möglichkeiten sozialer Systeme, Störungen zu verkraften, hängen von ihrer Leistungsfähigkeit ab. Daher müssen die Eigenschaften von Gestaltungsobjekten an potentiell betroffenen sozialen Systemen ausgerichtet werden. Dies betrifft zum einen die vertretbare Schadenshöhe und zum anderen die Beobachtungs- und Handlungsoptionen, die für das soziale System zur Verfügung gestellt werden sollen. Häufig reicht es aus, Individuen, Organisationen und gesellschaftliche Gruppen als idealtypische soziale Systeme zu unterscheiden.
- zu den *Interessen sozialer Systeme*: Soziale Systeme können in unterschiedlichen Rollen agieren, z. B. als Signierender oder als Empfänger signierter Willenserklärungen. Dementsprechend werden sie an Sicherungsmaßnahmen und damit auch an Technikkomponenten unterschiedliche Erwartungen haben. Das Konzept der rollenspezifischen Gestaltungsobjekte konnte erfolgreich eingesetzt werden, um diesem Aspekt in der Anforderungsanalyse Rechnung zu tragen.[20] Dabei wird durch einen „Übertragungsmechanismus“ auch unterstützt, dass sich beispielsweise aus den Interessen des Prüfenden einer digitalen Signatur Anforderungen an die Sigierkomponente des Schlüsselinhabers ergeben.
- zu den potentiellen *Schäden*: Unterschiedlichen Schadensarten, z. B. „monetäre Verluste“ oder „Verlust der elektronischen Geschäftsfähigkeit“, wird im allgemeinen mit unterschiedlichen Maßnahmen begegnet werden. Die Konkretisierung der Kriterien ist daher nach den zu erwartenden Schadensarten zu unterscheiden.
- zu *relevanten Störfällen:* Verletzlichkeitsrelevante Störfälle werden identifiziert, indem aus der Perspektive des jeweiligen sozialen Systems nach Gestaltungsobjekten und Störungsverläufen mit hohem Schadenspotential gesucht wird. Die verschiedenen Störungsdynamiken bieten dabei Anhaltspunkte, an denen die Suche ausgerichtet werden kann, z. B. zur Identifikation zentraler Komponenten für mögliche Komplexschäden oder von Ereignissen, über die eine Synchronstörung entstehen kann.

Der Begriff „Gestaltungsobjekt“ wird dabei bewusst weit verstanden. Er schließt z. B. Einsatzkonzepte für Techniksysteme oder Strukturen ein, wie z.B. Zertifizierungsgraphen. Störfall-Szenarien, die ähnliche Eigenschaften aufweisen, können zu Klassen zusammengefasst werden. Jede Klasse von Störfällen, die vom sozialen System beherrscht werden soll, wird dann als ein *Auslegungsstörfall* betrachtet. Ein Beispiel für einen Auslegungsstörfall aus der Perspektive der Gesellschaft ist die Forderung, dass das Auslaufen eines Zertifizierungsinstanz-Zertifikats nicht zum Verlust der elektronischen Geschäftsfähigkeit vieler Teilnehmer führen darf.

4.2 Beispiele

Im folgenden werden drei Beispiele zur Identifikation von verletzlichkeitsreduzierenden Sicherungsmaßnahmen aus dem Technikfeld Public Key Infrastrukturen betrachtet. Die Darstellung muß sich auf Kriterien K1 bis K4 und K7 beschränken.[21] Die hier ausgewählten Auslegungsstörfälle sind:

- Missbrauch eines Signaturschlüssels aus der Perspektive des Inhabers, sowie
- Störfälle mit Zertifizierungsinstanz-Schlüsseln und
- Brechen von Public Key Verfahren, jeweils aus der Perspektiv einer gesellschaftlichen Gruppe.

Schadensbegrenzung für Teilnehmer
Im Signaturgesetz (SigG) wurde eine *Verwendungsbegrenzungen in Zertifikaten* vorgesehen. Im allgemeinen Fall wird sie allerdings nicht ausreichend sein, um Kumulations- oder Multiplikationsschäden durch den Missbrauch eines Signaturschlüssels für den Schlüsselinhaber zu begrenzen. Zusätzlich wäre es notwendig, durch eine entsprechende Kontrolle auf der Chipkarte oder durch einen Autorisierungsdienst nur eine limitierte Anzahl von Nutzungen pro Zeiteinheit zuzulassen, um dem Kriterium „begrenzte Schäden“ (K1) gerecht zu werden.[22] Anpassungsfähigkeit (K7) wäre erfüllt, wenn der Schlüsselinhaber die zulässige Transaktionssumme im Laufe der Zeit erhöhen, aber auch vermindern kann.

Sperrung von Zertifizierungsschlüsseln
Missbrauchsfälle bei der Verwendung *von Zertifizierungsschlüsseln* müssen beherrscht werden. Bei genauerer Betrachtung zeigt sich, dass dafür mehrere Auslegungsstörfälle unterschieden werden müssen. Zum ersten kann eine Sperrung für *künftige Verwendung* notwendig sein. Davon zu unterscheiden sind einzelne Missbrauchsfälle, die erst *nach* den Manipulationen bekannt werden. In diesen Fällen kann es notwendig sein, einzelne Zertifikate *rückwirkend zu sperren*. In eine dritte Klasse fallen Störfall-Szenarien, in denen der Missbrauch nicht abschätzbar ist oder die Ausforschung eines geheimen Schlüssels angenommen werden muss. In diesem Fall kann die *Sperrung einer Teilhierarchie* von Zertifikaten notwendig sein.

Wenn die Public Key Infrastruktur auf die unterschiedlichen Störfall-Szenarien vorbereitet sein soll, müssen sowohl die Technikkomponenten der Vertrauensinstanzen als auch die Komponenten der Teilnehmer so ausgelegt werden, dass je nach Störfall die geeigneten Maßnahmen ergriffen werden können (K2 bis K4). Nur so können einerseits z. B. monetäre Schäden begrenzt und andererseits die elektronische Geschäftsfähigkeit möglichst gut aufrecht erhalten werden. Bisherige Sperrkonzepte, z. B. nach PKIX oder SigG, decken allerdings nur einzelne Szenarien ab und differenzieren die Fälle nur unzureichend.

Schwaches Public Key-Kryptosystem
Da die Sicherheit von Signaturverfahren von den Fortschritten der Mathematik abhängt, könnten in der Zukunft ein oder

[19] Vgl. dazu Hammer 1999a, Kap. 11, und die Beispiele in Kap. 12-14. Da sich die Kriterien auf sozio-technische Systeme beziehen, können mit ihnen auch Gestaltungsziele für andere Gestaltungsobjekte, beispielsweise Rechtsregeln oder organisatorische Maßnahmen abgeleitet werden. In der Praxis werden sogar im allgemeinen Systemlösungen zu suchen sein, die sich aus einer Kombination der verschiedenen Gestaltungsziele zusammensetzen. Im Sinne einer *Technik*gestaltung sollte jedoch zunächst versucht werden, *technische* Gestaltungsobjekte gemäß der Kriterien auszuformen. Kompensationsmaßnahmen für technische Defizite durch Recht, Organisation oder soziale Anpassung sind nur Mittel der zweiten Wahl.

[20] Dadurch wird mit NORA das Ziel der mehrseitigen Sicherheit (vgl. Rannenberg / Pfitzmann / Müller 1997, 21 ff) in der Anforderungsanalyse berücksichtigt.

[21] Zu einer ausführlichen Diskussion und weiteren Beispielen siehe Hammer 1999a, Kap. 12-14.

[22] Einen entsprechenden Vorschlag macht auch Baum-Waidner 1999.

mehrere Verfahren gebrochen werden.[23] Nach K3 sind für eine solche Situation Handlungsoptionen vorzusehen. Die Schnittstellen von Anwendungssystemen sollten so gestaltet werden, dass die Verfahren kurzfristig ausgewechselt werden können. Instanzen der Public Key Infrastruktur sollten darauf vorbereitet sein, in einem solchen Fall die Versorgung der Bevölkerung mit den notwendigen Schlüsseln, Trägermedien und Zertifikaten sicherzustellen.

Eine Rückfallmöglichkeit wäre auch für den Fall vorzusehen, dass keines der verfügbaren öffentlichen Schlüsselverfahren mehr ausreichende Sicherheit aufweist. Nach dem Kriterium der „graduellen Reduktion sozialer Funktionen" (K4) könnte jedoch für bestimmte Zwecke ein Wechsel auf symmetrische Verfahren vorbereitet werden. Dadurch würden zwar Beweisvorteile aufgegeben, die durch die Angriffsmöglichkeiten aber sowieso an Gewicht verlieren. Die Teilnehmer könnten mit der Rückfallmöglichkeit jedoch entscheiden, ob sie ihre Telekooperation zumindest in Teilen gegenüber Dritten schützen. Abb. 3 skizziert ein Schalenmodell mit möglichen Ausbreitungsgrenzen nach K4.

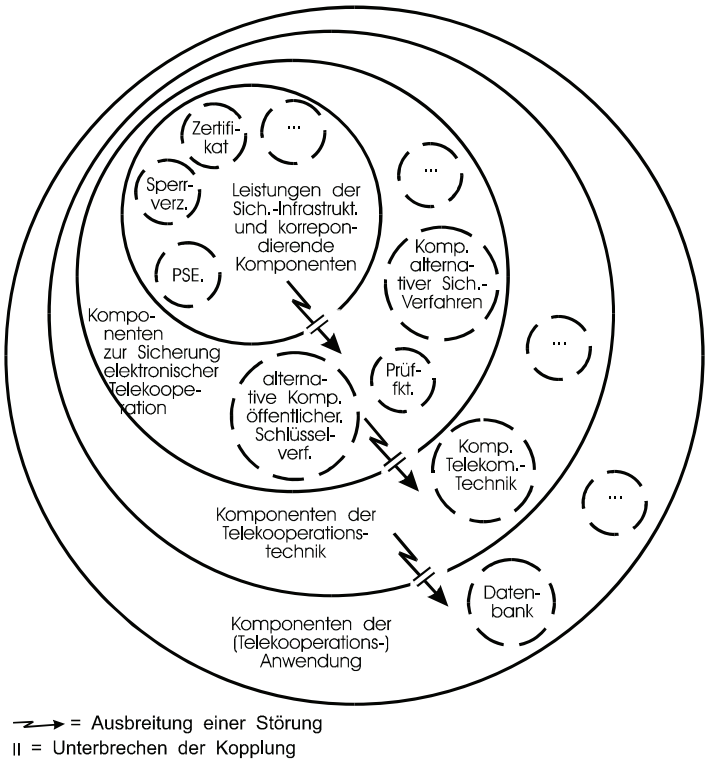

Abb. 3: Systemstruktur für eine graduelle Reduktion sozialer Funktionen

Fazit

Wie mit anderen Ansätzen der IT-Sicherheit kann auch mit der in diesem Beitrag skizzierten Methode keine vollständige Sicherheit erreicht werden. Grenzen der verletzlichkeitsreduzierenden Technikgestaltung ergeben sich unter anderem, weil auch verletzlichkeitsreduzierende Sicherungsmaßnahmen neben einem Sicherungsbeitrag einen Störungsbeitrag aufweisen. Grenzen ergeben sich auch, wenn Schadenspotentiale durch die Randbedingungen eines Systemkonzepts nicht beeinflusst werden können. Oft können auch die Zielkonflikte innerhalb und zwischen den Kriterien oder zu anderen Anforderungsbereichen nicht völlig aufgelöst, sondern nur balanciert werden. Schließlich trägt die normative Anforderungsanalyse zur verletzlichkeitsreduzierenden Technikgestaltung zwar dazu bei, dass mögliche individuelle Risikopräferenzen und die Interessenkonflikte zwischen verschiedenen Rollen aufgezeigt werden. Sie kann aber nur darauf hinweisen, dass für solche Probleme Anpassungs- und Aushandlungsmöglichkeiten in der Technik notwendig sind. Etwaige Konflikte müssen in der Realität sozial bewältigt werden.

Das skizzierte Kriteriensystem kann bereits in frühen Phasen der Anforderungsanalyse zur Gestaltung von Einsatzkonzepten und Technikkomponenten herangezogen werden. Es bietet daher die Chance zur *vorlaufenden Technikgestaltung*, auch für neue Technikfelder wie Public Key Infrastrukturen. Mit den sozio-technischen Kriterien werden Gestaltungsoptionen erschlossen, die die Schadenspotentiale von Störungen begrenzen oder Beobachtungs- und Handlungsoptionen eröffnen, um sie zu beherrschen. Die verletzlichkeitsreduzierende Technikgestaltung ergänzt damit die herkömmlichen IT-Sicherheitsansätze um eine systematische Berücksichtigung der Dimension des Schadenspotentials und berücksichtigt durchgängig eine sozio-technische Sichtweise. Sie trägt dazu bei, dass der sozialen Bewertung von Risiken und den langfristigen sozialen Folgen hoher Schadenspotentiale besser Rechnung getragen werden kann und kann dadurch auch zu einer höheren Akzeptabilität von IT-Systemen beitragen

[23] Vgl. dazu auch den Beitrag von Weis/Lucks/Geyer und die Tabelle von Lenstra und Verheul in diesem Heft.

Literatur

Amann, E. / Atzmüller, H. (1992): IT-Sicherheit – Was ist das?, DuD 6/1992, 286 ff.

Baum-Waidner, B. (1999): Ein Service zur Haftungsverteilung für kompromittierte digitale Signaturen, in: Baumgart, R. / Rannenberg, K. / Wähner, D. / Weck, G. (Hrsg.): Verlässliche Informationssysteme, Braunschweig/ Wiesbaden, 1999, 203 ff.

BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.) (1999): Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV – SigI Abschnitt A6 Gültigkeitsmodell, BSI, Bonn 1999.

CC – The Common Criteria Project Sponsering Organisations (1997): Common Criteria for Information Technology Security Evaluation, Version 2.0 Draft, 19. December 1997.

Grimm, R. (1994): Sicherheit für offene Kommunikation – Verbindliche Telekooperation, Mannheim, 1994.

Guggenberger, B. (1987): Das Menschenrecht auf Irrtum, München, Wien, 1987.

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

Hammer, V. (1999b): Verletzlichkeitsreduzierende Technikgestaltung – Methodische Grundlagen für die Anforderungsanalyse, in: Baumgart, R. / Rannenberg, K. / Wähner, D. / Weck, G. (Hrsg.): Verlässliche Informationssysteme, Braunschweig/ Wiesbaden, 1999, 187 ff.

BSI – Bundesamt für Sicherheit in der Informationstechnik (1997): IT-Grundschutzhandbuch 1997 – Maßnahmenempfehlungen für den mittleren Schutzbedarf, Köln, 1997.

ITSEC (1993): Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik – Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, in: Internationale Sicherheitskriterien – Kriterien zur Bewertung der Vertrauenswürdigkeit von IT-Systemen sowie von Entwicklungs- und Prüfumgebungen, München, 1993, 427 ff.

Jungermann, H. / Slovic, P. (1993): Die Psychologie der Kognition und Evaluation von Risiko, in: Bechmann, G. (Hrsg.): Risiko und Gesellschaft, Opladen, 1993, 167 ff.

Rannenberg, K. / Pfitzmann, A. / Müller, G. (1997): Sicherheit, insbesondere mehrseitige IT-Sicherheit, in: Müller, G. / Pfitzmann, A. (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn, 1997, 21 ff.

Leveson, N. (1995): Safeware – System Safety and Computers, Bonn, 1995.

Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U. (1990a): Die Verletzlichkeit der 'Informationsgesellschaft', Opladen, 1990.

Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U. (1990b): Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen, 1990.

Roßnagel, A. (1995): Die Verletzlichkeit der Informationsgesellschaft und rechtlicher Gestaltungsbedarf, in: Kreowski, H.-J. / Risse, T. / Spillner, A. / Streibl, R. E. / Vosseberg, K. (Hrsg.): Realität und Utopien der Informatik, Münster, 1995, 56 ff.

Rudinger, G. / Espey, J. / Holte, H. / Neuf, H. (1996): Der menschliche Umgang mit Unsicherheit, Ungewissheit und (technischen) Risiken aus psychologischer Sicht, in: BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Kulturelle Beherrschbarkeit digitaler Signaturen, Ingelheim, 1996, 128 ff.

Starr, Ch. (1969): Sozialer Nutzen versus technisches Risiko; Übersetzung von Rader, M.; Original: Science, 19/1969, 1232 ff.; übersetzt in: Bechmann, G. (Hrsg.): Risiko und Gesellschaft, Opladen, 1993, 3 ff.

Wehner, T. (1993): Zum Umgang mit Fehlern, BSI-Forum in KES 5/1993, 49f.

Weizsäcker, C. v. / Weizsäcker, E. U. v. (1984): Fehlerfreundlichkeit, in: Kornwachs, K. (Hrsg.): Offenheit – Zeitlichkeit – Komplexität. Zur Theorie der Offenen Systeme, Frankfurt a.M., 1984, 167 ff.