DuD
Datenschutz und Datensicherheit

Risiko

Volker Hammer

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

„Risiko" ist einer der zentralen Begriffe in Diskussionen um und über (IT-)Sicherheit.[1] Er wird in verschiedenen Kontexten unterschiedlich belegt, beispielsweise in der Ökonomie, der Soziologie, der Psychologie, der Technikbewertung oder im Projektmanagement von Software-Engineering-Prozessen.

Für die Gestaltung von technischen und informationstechnischen Systemen spielt der Risikobegriff dann eine große Rolle, wenn die Art und der Umfang von Sicherungsmaßnahmen bestimmt und begrenzt werden müssen. Es wird dann ein Grenzwert für Risiken gesucht, ab dem ein System als sicher gelten soll (vgl. z. B. Abb. 1). Sicherheit wird angenommen, wenn „die verbleibende Risiken tragbar" erscheinen. Die Forderung, bestimmte Risiken zu vermeiden, oder die Suche nach der Gestaltungsalternative mit dem „günstigsten" Risiko ist dann entscheidungsleitend für die Implementierung und den Einsatz von Sicherungsmaßnahmen.

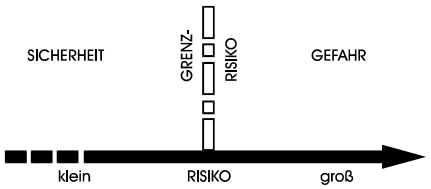

Abb. 1: Sicherheit, Grenzrisiko und Gefahr nach DIN/VDE 31000.[2]

Risiko wird in der technischen Diskussion im allgemeinen aus den beiden Komponenten *Schadenshöhe* und *Schadenswahrscheinlichkeit* bestimmt. Der probabilistische Risikobegriff basiert auf der Formel:

```
Risiko = Schadenswahrscheinlichkeit *
         Schadenspotential
```

Beide Faktoren gehen linear ein. Ein bestimmter Risikowert kann dementsprechend mit niedriger Schadenswahrscheinlichkeit bei hohem Schadenspotential oder umgekehrt bei niedrigem Schadenspotential auch bei hoher Schadenswahrscheinlichkeit unterboten werden. In der probabilistischen Sicherheitsphilosophie wird angenommen, daß Risikowerte und die zu ihrer Einhaltung erforderlichen Maßnahmen über Wahrscheinlichkeitswerte abzuleiten sind.

Dieser mathematisch-technische Ansatz stieß in der Vergangenheit jedoch vielfach auf Probleme: Er wurde in der „sozialen Wirklichkeit" nicht anerkannt. Bereits [Starr 1969, 12] stellt eine „Differenz, um mehrere Größenordnungen, zwischen der gesellschaftlichen Bereitschaft, 'freiwilliges' oder 'unfreiwilliges' Risiko zu akzeptieren" fest.

Zudem bestehen häufig bei genauerer Betrachtung bereits grundsätzliche Probleme für die Anwendung der Risikoformel. Schadenswahrscheinlichkeiten lassen sich nur unzureichend bestimmen, wenn noch unbekannte Systeme oder soziale Faktoren berücksichtigt werden müssen, wie die Stimmung oder Müdigkeit von Operateuren, die Einhaltung organisatorischer Bestimmungen oder gar soziale (gesellschaftliche) Spannungen.

Auch lassen sich verschiedene Schadensarten kaum auf *einer* numerischen Skala abbilden, weshalb die Vergleichbarkeit von Risikowerten unterschiedlicher Szenarien in Frage steht. Schließlich gibt die Risikoformel häufig die Verteilung von potentiellen Schäden und potentiellem Nutzen für unterschiedliche „Träger" nur unzureichend wider.

Technische Ansätze zur Risikobestimmung eignen sich zwar oft zum Vergleich unterschiedlicher technischer Realisierungen bei gleichem Schadenspotential. Sie geben aber für die *soziale Bewertung* von Risiken, also die Beantwortung der Frage „wie sicher ist sicher genug", im allgemeinen keine Hinweise. So verweist auch die obige Formulierung der IT-Sicherheit mit den „verbleibenden tragbaren Risiken" auf eine soziale Bewertung.

Hinweise zu sozialen Bewertungen finden sich in anderen Risikobegriffen: in intuitiven Risikokonzepten aus der Psychologie, in der rechtlichen Bewertung besonderer Risiken und in der Forderung nach Erhalt der Lern- und Überlebensfähigkeit sozialer Systeme.

In psychologischen Studien konnten *intuitive Risikokonzepte* identifiziert werden. Die Einflüsse auf die intuitive Bewertung wurden in drei Faktoren zusammengefaßt:[3]

- Über den Faktor *dread Risk* wird ein Risiko als hoch bewertet, wenn es
  - unfreiwillig eingegangen werden muss,
  - unkontrollierbar,
  - furchtbar oder tödlich erscheint,
  - zu einer ungerechten Verteilung von Vor- und Nachteilen führt oder
  - ein hohes Katastrophenpotential beinhaltet.
- Der Faktor *unknown Risk* trägt zu einer hohen Bewertung bei, wenn das Risiko
  - als nicht wahrnehmbar,
  - unbekannt oder neuartig beurteilt oder
  - seine Wirkung erst mit starker Verzögerung erwartet wird.
- Über den Faktor *exposure* wird berücksichtigt, wenn eine große Anzahl von Menschen einer Gefahr ausgesetzt wird, auch wenn der Einzelne sich nicht unmittelbar bedroht fühlt.

Im *Recht* wird der Übergang vom (polizei-)rechtlichen erfahrungsgeleiteten Gefahrenbegriff zum rechtlichen Risikobegriff in Genehmigungsverfahren für technische Systeme darauf zurückgeführt, daß es in Bereichen mit besonderen Schadenspotentialen gesellschaftlich nicht akzeptabel sei, Erfahrungen zur Gefahrenabwehr über Versuch und Irrtum zu erwerben.[4]

Zudem müssen hohe Schäden aus der Sicht des sozialen Systems unter allen Umständen ausgeschlossen werden. Hohe Schadenspotentiale erfordern es deshalb,

[1] Vgl. zum folgenden ausführlich mit weiteren Nachweisen Hammer 1999, 97 ff.

[2] Abb. aus DIN/VDE 31000 (1987), Teil 2, 3; Zitat: DIN/VDE 31000 (1987), Teil 2, 2.

[3] Vgl. Jungermann / Slovic 1993, 173 ff.

[4] Z. B. Ladeur, UPR 1993, 121 ff.

auch mögliche soziale Ursachen für Störungen auszuschließen: Sie zwingen zu sozialen Sicherungsmaßnahmen. Diese aber können die Realisierungsbedingungen von Grundrechten verschlechtern. Hohe Schadenspotentiale sind daher auch nach dem Kriterium der Verfassungsverträglichkeit in Risikobewertungen überproportional zu berücksichtigen.[5]

Schließlich werden hohe Schadenspotentiale in der Literatur abgelehnt, weil sie die *Lernfähigkeit* von sozialen Systemen verschlechtern und hohe Schäden große Anstrengungen zur Regeneration binden. Realisierte große Schäden können letztlich sogar das Überleben des sozialen Systems in Frage stellen.

Diese Ergebnisse für die soziale Bewertung von Risiken motivieren einen Risikobegriff für die Technikgestaltung, der Schadenspotentiale überproportional gewichtet und Erfahrungsbildung und Autonomie als weitere „Komponenten" neben der Schadenswahrscheinlichkeit aufgreift. Dabei muß die „Risikoskala" jeweils auf das soziale System bezogen werden, das von potentiellen Schäden betroffen ist. Die Risikopräferenzen eines sozialen Systems werden zum einen von seiner Fähigkeit abhängen, Störungen zu verkraften. Diese Fähigkeit wird wiederum von der jeweiligen Bewertung der relativen Höhe eines potentiellen Schadens durch das soziale System, aber auch von seinen Reaktionsmöglichkeiten im Störfall beeinflußt. Zum anderen wird auch seine Risikobereitschaft in die Riskobewertung eingehen. Grundsätzlich muss deshalb für ein IT-System von einer Bandbreite unterschiedlicher Risikobewertungen ausgegangen werden. Technikentwickler können dem durch Anpassbarkeit der Anwendungen Rechnung tragen.

Im Unterschied zur probabilistischen konzentriert sich die deterministische Sicherheitsphilosopie auf das Risiko bestimmter Störfälle, sogenannter Auslegungsstörfälle.[6] Nach diesem Ansatz ist sicherzustellen, dass die Auslegungsstörfälle mit den getroffenen Sicherungsmaßnahmen beherrscht werden.

Damit ist der deterministische Ansatz pragmatischer als der probabilistische. Gleichzeitig ist er stärker am Schadenspotential orientiert. Die Auswahl der Auslegungsstörfälle und die Erwartung zuverlässig arbeitender Sicherungsmaßnahmen unterliegen allerdings Annahmen. Insofern verbleiben auch im deterministischen Ansatz bewusste oder „verdeckte" Wahrscheinlichkeiten. Je weiter die Auslegungsstörfälle die möglichen Störfälle mit schweren Folgen überdecken und je kritischer Sicherungsmaßnahmen auf ihren Sicherungsbeitrag und ihre Unabhängigkeit geprüft werden, desto eher wird allerdings der deterministische Ansatz Einfluss auf das Schadenspotential von Risiken nehmen. Die Kriterien der verletzlichkeitsreduzierenden Technikgestaltung[7] fordern zum einen möglichst eine direkte Beeinflussung des Schadenspotentials. Zum zweiten nutzen sie das Konzept der gestaffelten Barrieren aus deterministischen Ansätzen. Schließlich greifen die Kriterien auch die weiteren sozialen Aspekte von Risiko auf und geben Hinweise für die Gestaltung von IT-Systemen, die die Erfahrungsbildung und die Autonomie sozialer Systeme beim Einsatz von IT-Systemen und in Störfällen fördern können.

Literatur

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

Ladeur, K.-H. (1993): *Risikobewertung und Risikomanagement im Anlagensicherheitsrecht – Zur Weiterentwicklung der Dogmatik der Störfallvorsorge*, UPR 4/1993, 121 ff.

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

Roßnagel, A. (1997): Der Nachweis von Sicherheit im Anlagenrecht – Am Beispiel von deterministischen und probabilistischen Sicherheitsnachweisen im Atomrecht, DÖV 19/1997, 801 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.

[5] Roßnagel / Wedde / Hammer / Pordesch 1990; rechtliche Argumente auch bei Fuhrmann in diesem Heft.

[6] Zu einem Vergleich der beiden Ansätze in Bezug auf das Atomrecht siehe z. B. Roßnagel, DÖV 1997 mwN.

[7] Vgl. dazu den Beitrag von Hammer in diesem Heft.