Informationssicherheit und Recht – Verantwortung von IT-Anbietern und Anwendern für sichere Informationsverarbeitung, Tagung vom 4.6.2003

Ausservertragliche Haftung von IT-Anbietern in der Schweiz

Dr. Wolfgang Straub, LL.M.
Deutsch Wyss & Partner
Effingerstrasse 17/Postfach 5860
3001 Bern

Inhalt

1 Allgemeines 4

2 Unerlaubte Handlung 6

2.1 Überblick 6

2.2 Schaden 7

2.3 Widerrechtlichkeit 8

2.4 Verschulden 10

2.5 Adäquate Kausalität 11

3 Geschäftsherrenhaftung 13

4 Produktehaftung 17

4.1 Überblick über die Haftungsvoraussetzungen 17

4.2 Schaden 18

4.3 Produkt 19

4.4 Fehler 20

4.5 Hersteller 22

4.6 Kausalität 24

4.7 Entlastungsgründe 25

4.7.1 Fehlendes Inverkehrbringen 26

4.7.2 Nachträglich entstandene Produktefehler 26

4.7.3 Entlastungsbeweis des Teilherstellers 27

4.7.4 Einhaltung zwingender Normen 27

4.7.5 Entwicklungsrisiken 27

4.7.6 Nichtkommerzielle Tätigkeit 29

4.8 Verjährung und Verwirkung 29

4.9 Produkteinformation und Rückruf 30

5 Schadensverhütung und Schadensminderung 31

6 Konkurrenz von Haftpflichtigen..... 32

7 Haftungsbeschränkungen 32

8 Ergebnisse..... 33

Hinweise auf weiterführende Literatur 35

1 Allgemeines

Die Frage nach einer Haftung von IT-Dienstleistern und Herstellern stellt sich erst, wenn ein konkreter Schaden vorliegt. Ungenügende Informationssicherheit kann insbesondere dazu führen, dass Daten unrichtig verarbeitet bzw. gelöscht werden oder Unbefugte Zugriff auf Daten oder Prozesse haben. Dies kann insbesondere folgende Konsequenzen haben:

- **Produktionsausfälle**. Diese führen z.B. zu Einnahmenverlust, Schadenersatzansprüche von Vertragspartnern, weitere indirekte Schäden
- **gefährliche Prozesse geraten ausser Kontrolle.** Dadurch entstehen z. B. Körperverletzungen und Sachschäden bei Fehlsteuerung von Fertigungsrobotern oder bei Ausfall von Temperatursteuerungen
- **Imageverluste**
- **Persönlichkeits- und Datenschutzverletzungen** durch den Zugriff Unbefugter auf Daten und Informationen.

Die wirtschaftlichen Folgen solcher Vorfälle müssen immer entweder vom Geschädigten oder von einem oder mehreren Schädigern getragen werden. Die Rechtsordnung versucht durch die Regeln der vertraglichen und ausservertraglichen Haftung einen möglichst gerechten **Ausgleich zwischen den Interessen aller Beteiligten** zu finden. Man kann sich das Vertrags- und Haftpflichtrecht wie verschiedene übereinander liegende Lochkarten vorstellen. Jede dieser Ebenen führt in einer Reihe von Situationen zur Verantwortlichkeit des Verursachers, enthält jedoch Löcher für andere Konstellationen. Die ‚Lücken' sind grundsätzlich ebenso wie der abgedeckte Bereich auf Entscheidungen des Gesetzgebers zurückzuführen und daher grundsätzlich nicht als Unvollkommenheiten des Systems zu betrachten.

Das nachfolgende Schema gibt einen Überblick über die typischen Haftungsarten bei Störungen von Informationssystemen.

Geschädigte Verantwortliche	**Anwender**	**Betreiber/Eigentümer des IT-Systems**	**Vertragspartner der Betroffenen**	**geschädigte Dritte**
Angreifer	D	D	D	D
Hersteller und IT-Dienstleister	D/P/G	V/D/P/G	D/G	D/G/P
Arbeitnehmer und Hilfspersonen	D	V/D	D	D
Geschäftsleitung, Verwaltungsräte und Revisoren	G	V/G	G	G

Art des Anspruchs:

D Deliktshaftung
G Geschäftsherrenhaftung
P Produktehaftung
G gesellschaftsrechtliche Verantwortlichkeit
V Vertrag

Die **ausservertragliche Haftung** ist sowohl in jenen Fällen von Bedeutung, in welchen Schädiger und Geschädigter in keinem Vertragsverhältnis zueinander stehen, als auch in jenen, in welchen die vertraglichen Ansprüche erloschen sind (z. B. durch Verjährung). Ob die kurzen Verjährungsbestimmungen des Kauf- und Werkvertragsrechts auch für ausservertragliche Haftungsarten gelten, ist umstritten. Die in der Schweiz wohl herrschende Meinung verneint dies jedoch.

Es gibt drei Haupttypen ausservertraglicher Haftung, welche für Schäden durch IT-Produkte von Bedeutung sind: die allgemeine ausservertragliche Haftung (Art. 41 OR, **Deliktshaftung**), die ausservertragliche Haftung für das Verhalten von Mitarbeitern (Art. 55 OR, **Geschäftsherrenhaftung**) und die Haftung für fehlerhafte Produkte nach dem **Produktehaftungsge-**

setz (PrHG). Daneben bestehen besondere Regelungen für Schäden, welche durch Eisenbahnen, Atomanlagen etc. verursacht wurden.

2 Unerlaubte Handlung

2.1 Überblick

Vorliegend wird deshalb zuerst auf die Deliktshaftung eingegangen, weil die anderen Haftungstypen historisch und logisch bis zu einem gewissen Grad auf ihr aufbauen. Werden Schäden in arbeitsteiligen Prozessen durch Hilfspersonen wie **Mitarbeiter** eines IT-Dienstleisters oder Herstellers verursacht, haftet das betreffende Unternehmen nach den besonderen Grundsätzen der Geschäftsherrenhaftung dafür (vgl. dazu Kap. 3). Soweit Ansprüche aus Produktehaftungsgesetz bestehen, verdrängen sie die allgemeine Deliktshaftung (vgl. dazu Kap. 4). Diese kann aber in folgenden Konstellationen durchaus noch praktische **Bedeutung** haben:

- Ansprüche gegenüber den einen Schaden konkret verursachenden **natürlichen Personen** (z.B. Hacker, schadensverursachende Mitarbeiter eines IT-Unternehmens)
- Sicherheitsverletzungen, welche im Rahmen von **IT-Dienstleistungen** durch selbständigerwerbende natürliche Personen verursacht wurden.
- Sofern **Organe einer Gesellschaft** (z.B. Direktoren, Verwaltungsräte) im Rahmen der Ausübung ihrer Aufgaben einen Schaden verursachen, haftet das Unternehmen für deren Handlungen ebenfalls nach Art. 41 OR (Zurechnung via Art. 55 ZGB).

Eine Schadenersatzpflicht nach Art. 41 OR setzt voraus, dass der Geschädigte folgende **Voraussetzungen** beweisen kann:

- Vorhandensein eines **Schadens**
- Absichtliche oder fahrlässige Verursachung des Schadens (**Verschulden des Schädigers**)

- **Adäquate Kausalität** zwischen schädigender Handlung und Schadenseintritt
- **Widerrechtlichkeit** der Schadensverursachung

2.2 Schaden

Schäden im rechtlichen Sinn setzen stets eine **Vermögensverminderung** voraus. Daher führen z.B. Datenchutzverletzungen nicht automatisch zu einer Haftung. Der Schaden liegt in der Differenz zwischen dem Vermögensstand des Betroffenen nach der Schädigung gegenüber jenem (hypothetischen) Vermögensstand, welcher ohne die schädigende Handlung bestehen würde (vgl. dazu BGE 127 III 75 E. 4a, 126 III 393, E. 11a). Generell wird unterschieden zwischen:

- **Tod und Köperverletzung:** Diese führen einerseits zu quantifizierbaren Schäden (insbesondere Heilungskosten, Arbeitsausfall, Wegfall der Unterstützung durch einen Angehörigen), andererseits aber auch zu physischem und psychischem Leiden. Obwohl dieses nicht in Geld messbar ist, können die Betroffenen dafür **Genugtuungsleistungen** in Geld erhalten, sofern die übrigen Voraussetzungen einer ausservertraglichen Haftung gegeben sind (Art. 47 und 49 OR; vgl. zur Abgrenzung zwischen Schaden und immaterieller Unbill BGE 123 IV 147 E. 4b/bb). Die in der Schweiz in diesen Fällen zugesprochenen Beträge liegen indessen weit unter denjenigen, welche aus den USA bekannt sind (vgl. dazu die Übersicht über die Rechtsprechung in BGE 112 II 131 E. 2/3).
- **Sachschäden:** Diese bestehen im Verlust oder der Wertverminderung von körperlichen Gegenständen. Inwieweit auch Datenverlust einen Sachschaden darstellt, ist in der Schweiz bisher noch ungeklärt (vgl. dazu auch Kap. 2.3 und 4.2).
- **Reine Vermögensschäden**: Diese Kategorie umfasst alle übrigen finanziell bezifferbaren Vermögensbeeinträchtigungen (z. B. entgangener Gewinn, Produktivitätsausfall, Schadenersatzpflichten des Geschädigten gegenüber Dritten). Der Schaden kann grundsätzlich auch in einem **entgangenen Gewinn** liegen (z. B. weil die Nachfrage nach

einem bestimmten Produkt aufgrund eines softwarebedingten Produktionsausfalls nicht rechtzeitig befriedigt werden konnte).

Diese Unterscheidung ist von grosser praktischer Bedeutung, da die Voraussetzungen der Ersatzpflicht für die einzelnen Schadensarten unterschiedlich sind (vgl. Kap. 2.3.).

Oft führen Schäden zu weiteren Schäden (**mittelbaren Schäden**), z. B. verursacht ein Softwarefehler in der Steuerung einer Maschine deren Überhitzung, was die Zerstörung der Maschine selbst sowie einen Brand im betreffenden Fabrikationsgebäude auslöst, welcher das Warenlager vernichtet und einen Produktionsausfall verursacht. Unmittelbare und mittelbare Schäden werden im Haftpflichtrecht grundsätzlich gleich behandelt (vgl. demgegenüber Art. 208 Abs. 3 OR im Kaufrecht).

2.3 Widerrechtlichkeit

Die allgemeine Deliktshaftung wird auch als ‚Haftung aus unerlaubter Handlung' bezeichnet. Sie setzt nämlich voraus, dass der Schaden durch eine rechtswidrige Handlung entstanden ist, d. h. unter Verletzung einer rechtlichen Norm.

Leben, körperliche Integrität und Eigentum an Sachen sind von der Rechtsordnung umfassend geschützt, so dass deren Verletzung immer widerrechtlich ist (Verletzung absolut geschützter Rechtsgüter). Blosse **Vermögensschäden** (z. B. Arbeitsausfall, Ansprüche von Kunden des Geschädigten wegen Lieferverzögerung und Imageverluste) sind hingegen nur dann zu ersetzen, wenn bei der Verursachung eine gesetzliche Bestimmung verletzt wurde, welche dem Schutz des Vermögens gegen Schädigungen dieser Art dient (vgl. zur Bedeutung solcher Normen auch BGE 125 III 86, E. 3b und 119 II 128 E. 3). Technische Normen (z.B. ISO/BS) sind keine Vermögensschutznormen. Da solche spezifische Schutznormen selten sind, bestehen für Vermögensschäden durch IT-Produkte und -Dienstleistungen nur selten Schadenersatzansprüche aus unerlaubter Handlung.

Hingegen ziehen **strafrechtlich relevante Angriffe** gegen Informationssysteme oder IT-Infrastruktur eine zivilrechtliche Haftung des Angreifers nach sich (z.B. unbefugtes Eindringen in Datenverarbeitungsanlagen, Art. 143bis StGB oder Störung des Telefonverkehrs, Art. 239 StGB). In diesem Zusammenhang könnte die geplante Umsetzung von Art 12 Abs. 2 der Cybercrime-Convention des Europarats, welcher Arbeitgeber bis zu einem gewissen Grad verpflichtet, Computerdelikte ihrer Mitarbeiter zu verhindern, auch zivilrechtliche Auswirkungen haben.

Ob das **Löschen oder Verändern von Daten** auf einem Datenträger (z.B. Harddisk) *per se* eine widerrechtliche Eigentumsverletzung darstellt oder ob sie zu blossen Vermögensschäden führt, wird international kontrovers diskutiert. Da ungenügende Informationssicherheit oft zu Datenverlust oder zur Verfälschung von Informationen führt, hat diese Frage erhebliche praktische Bedeutung wurde bisher aber noch kaum gerichtlich entschieden. Bei wiederbeschreibbaren Medien wird der Datenträger durch den Löschvorgang nicht selbst beeinträchtigt (Substanzbeeinträchtigungstheorie). Allerdings liegt der wirtschaftliche und betriebliche Wert meist mehr in den Daten als im Speichermedium. Zumindest der Verlust von lauffähiger Software wird daher in der internationalen Diskussion zunehmend als Eigentumsverletzung betrachtet (Funktionsbeeinträchtigungstheorie).

Die **Zerstörung von Datenträgern** und das Unlesbarmachen von nur einmal beschreibbaren Medien (z.B. CD-ROM) stellen zwar ohne weiteres Sachbeschädigungen dar. Allerdings fragt sich auch hier, inwieweit die verlorenen Daten bei der Berechnung des Sachschadens zu berücksichtigen sind. Jedenfalls sind durch Datenverlust verursachte Arbeitsausfälle und Mehraufwände grundsätzlich reine Vermögensschäden und somit nur dann zu ersetzen, wenn eine Vermögensschutznorm verletzt wurde.

In Zusammenhang mit umfangreichen Datenschäden stellt sich stets die Frage, inwieweit der Geschädigte zur **Datensicherung** verpflichtet gewesen wäre (vgl. dazu Kap. 5).

Datenlöschung bzw. -veränderung kann zu **Fehlfunktionen eines Informationssystems** führen, welche ihrerseits Sach- und Personenschäden auslösen.

Schliesslich haftet auch, wer einen Schaden **in ‚sittenwidriger Weise' absichtlich** verursacht (Art. 41 Abs. 2 OR; vgl. dazu auch BGE 124 III 297 E. 5e). Eine Schädigung kann insbesondere dann sittenwidrig sein, wenn zwischen Schädiger und Geschädigtem ein besonderes Vertrauensverhältnis besteht (z. B. aufgrund eine Vertrages). Gibt z. B. der Hersteller eines IT-Systems wider besseres Wissen eine Zusicherung über dessen sicherheitsrelevante Eigenschaften ab, kann er für dadurch entstandene Vermögensschäden auch noch nach Ablauf der Gewährleistungsfristen haften.

Bei Schäden, welche in Zusammenhang mit dem **Unterlassen von Sicherheitsmassnahmen** entstanden sind, muss differenziert werden:

- Wären sie nicht entstanden, wenn die betreffende Leistung gar nicht erbracht worden wäre, liegt nicht eine Schädigung durch Unterlassen sondern durch **aktives Handeln** vor (z.B. Schädigungen beim Einbau einer neuen IT-Komponente, weil bei der Installation Sicherheitsvorkehrungen unterlassen wurden).
- Erfolgte die Schädigung hingegen durch externe Ursachen, stellt sich die Frage, ob das Unterlassen der Sicherheitsvorkehren gegen eine vertragliche oder gesetzliche **Garantenstellung** verstossen hat (vgl. dazu BGE 115 II 15), z.B. eine Pflicht zum Schutz vor bestimmten Angriffen Dritter im Rahmen von *Managed Security Service* Verträgen.

2.4 Verschulden

Die Deliktshaftung setzt voraus, dass der Schaden schuldhaft, d. h. **absichtlich oder fahrlässig** verursacht wurde. Das Verschulden des Schädigers muss sowohl nach objektiven als nach personenbezogenen Kriterien beurteilt werden. Bei Schäden durch Softwarefehler ist etwa zu prüfen, ob sich der Verursacher so verhalten hat, wie man es von einem Informatiker mit dem betreffenden Ausbildungsstand erwarten durfte und ob sein Verhalten in der konkreten Situation vorwerfbar war.

Letztlich geht es darum, ob der Schadensverursacher jenes **Mass an Sorgfalt** aufgewendet hat, welches von ihm objektiv erwartet werden durfte. In

diesem Zusammenhang ist es wichtig, dokumentieren zu können, ob die branchenüblichen Standards eingehalten wurden. Dazu kann z.B. gehören:

- Einhalten der in der betreffenden Branche gängigen **Sicherheitsstandards** (z.B. ISO/IEC 17799 soweit diese IT-Hersteller und Dienstleister mitbetreffen).
- Massnahmen zur **Qualitätssicherung**
- **Produktemonitoring** nach Inverkehrbringen/nachträgliche Produkteinformation

2.5 Adäquate Kausalität

Eine Haftung besteht nur dann, wenn der Schaden eindeutig auf ein vorwerfbares Verhalten des Schädigers zurückgeführt werden kann. Nicht jeder noch so unwahrscheinliche Kausalzusammenhang lässt es als gerechtfertigt erscheinen, alle Personen für einen eingetretenen Schaden haften zu lassen, welche zu seiner Entstehung irgend einen Beitrag geleistet haben. Es ist sozusagen eine qualifizierte (**adäquate**) **Kausalität** notwendig. Nach der ‚Adäquanzformel' des schweizerischen Bundesgerichts ist der Kausalzusammenhang dann adäquat, ‚wenn die betreffende Ursache nach dem gewöhnlichen Lauf der Dinge und der allgemeinen Lebenserfahrung geeignet war, den eingetretenen Erfolg zu bewirken, so dass der Eintritt des Erfolges als durch die fragliche Tatsache allgemein begünstigt erscheint' (vgl. BGE 123 III 110 E. 3a und 102 II 232 E. 2 mit weiteren Hinweisen). Allerdings wird diese Formel vom Bundesgericht sehr weit interpretiert, so dass es an der Adäquanz nur in seltenen Ausnahmefällen fehlen dürfte.

Im Bereich der Informationssicherheit werden Schäden durch IT-Hersteller und -Dienstleister typischerweise dadurch mitverursacht, dass sie schadensverhütende Massnahmen **unterlassen** (z.B. Verzicht auf Einbau von Schutzmechanismen in Produkte, Nichteinspielen von Softwareupdates, unsachgemässe Konfiguration von Firewalls). IT-Hersteller und -Dienstleister können auch dann zu Haftung gezogen werden, wenn der Schaden zwar primär durch Zufall oder Drittverhalten (z.B. Angriffe von

Hackern) ausgelöst worden ist, sie aber pflichtwidrig Massnahmen unterlassen haben, welche den Schadenseintritt verhütet hätten.

Das Verhalten des Geschädigten oder eines Dritten vermag im Normalfall den adäquaten Kausalzusammenhang nicht zu beseitigen (BGE 112 II 141 E. 3a). Erscheint eine Ursache im Verhältnis zu den andern Gründen der Schadensentstehung allerdings als von völlig untergeordneter Bedeutung, gilt der adäquate **Kausalzusammenhang** als **unterbrochen** und kann daher keine Haftung mehr auslösen (vgl. dazu BGE 116 II 519 E. 4b). Obwohl beispielsweise das Verschulden eines *Crackers* für einen Schaden sehr viel schwerer wiegt als das fahrlässige Offenlassen von Sicherheitslücken durch einen IT-Dienstleister führt es grundsätzlich nicht zu einer Unterbrechung des Kausalzusammenhangs. Hingegen ist dem unterschiedlich grossen Verschulden im Rahmen der internen Schadensverteilung zwischen den Verursachern Rechnung zu tragen soweit der Angreifer überhaupt ins Recht gefasst werden kann (vgl. dazu Kap. 6).

3 Geschäftsherrenhaftung

Schädigungen durch mangelhafte IT-Produkte oder -Dienstleistungen werden letztlich meistens durch **Mitarbeiter** eines Unternehmens verursacht. Für den Geschädigten ist in der Regel unzweckmässig, gegen denjenigen Arbeitnehmer zu klagen, welcher den Schaden verschuldet hat. Einerseits ist es für Aussenstehende mitunter kaum möglich zu eruieren, wer den Schaden verursacht hat. Andererseits verfügen Arbeitnehmer oft nicht über genügend Mittel bzw. eigene Versicherungsdeckung zum Ersatz grosser Schäden.

Aufgrund der spezifischen Geschäftsherrenhaftung von Art. 55 OR kann der Geschädigte den Arbeitgeber bzw. die Arbeitgeberfirma des Schadensstifters ins Recht fassen. Ein Unternehmen haftet als ‚Geschäftsherr', für das Verhalten seiner Arbeitnehmer oder sonstigen Hilfspersonen, wenn folgende **Voraussetzungen** gegeben sind:

- Der Schaden muss durch eine **Hilfsperson** verursacht worden sein. Das setzt nicht zwingend einen gültigen Arbeitsvertrag zwischen dem Unternehmen und dem Schadensverursacher voraus. Massgebend ist, ob ein **Unterordnungsverhältnis** zum ‚Geschäftsherrn' besteht, d. h. ob die Hilfsperson unter Aufsicht steht und Weisungen befolgen musste. Sofern ein faktisches Unterordnungsverhältnis besteht, kann die Geschäftsherrenhaftung auch für *Freelancer* gegeben sein. Hingegen sind Subakkordanten und Zulieferer grundsätzlich keine Hilfspersonen.

- Die Schadensverursachung muss **in Ausübung der geschäftlichen Verrichtungen** stattgefunden haben. Das ist auch dann der Fall, wenn der Arbeitnehmer sich bei der Ausführung der Arbeit über Weisungen des Geschäftsherrn hinwegsetzte (z. B. Sicherungsmassnahmen unterlässt). Hingegen haftet der Arbeitgeber grundsätzlich nicht für privat motivierte Sabotageakte der Arbeitnehmer (z. B. *Hacking*), auch wenn sie bei Gelegenheit der Arbeit erfolgen.

- Die Schädigung muss **widerrechtlich** erfolgt sein (vgl. dazu Kap. 2.3).

- Zwischen schädigender Handlung und Schaden muss ein **adäquater Kausalzusammenhang** bestehen (vgl. Kap. 2.5).

Der ‚Geschäftsherr' kann sich **von der Haftung befreien**, wenn er beweist, dass er die nötige Sorgfalt in folgenden Bereichen walten liess:

- **Auswahl** der schadensverursachenden Hilfsperson. Diese musste insbesondere über die notwendige berufliche Qualifikation für die betreffende Aufgabe verfügen.

- Korrekte und ausreichende **Instruktion** der Hilfsperson. Der Umfang der notwendigen Anleitung hängt ebenfalls von der Qualifikation der betreffenden Person ab.

- Ausreichende **Überwachung und Kontrolle** der Hilfsperson. Da in grösseren Unternehmen nicht alle Mitarbeiter von Verwaltungsrat und Direktion persönlich überwacht werden können, hat die Implementierung von Controlling- und Qualitätssicherungsverfahren hier besondere Bedeutung.

- Schliesslich muss der Geschäftsherr beweisen, dass alle objektiv gebotenen Massnahmen zur Vermeidung von Schäden der betreffenden Art durch zweckmässige **Organisation** des Arbeitsprozesses getroffen wurden. Dazu gehört auch das Bereitstellen der nötigen personellen Ressourcen für eine bestimmte Aufgabe und eine realistische Zeitplanung. Softwareentwicklung erfolgt häufig unter extremem Zeitdruck. Führt eine unzweckmässiger Projektplanung durch den Geschäftsherrn zu Schäden wegen Übermüdungseffekten, kann der Entlastungsbeweis scheitern.

  Nach der Rechtsprechung des Bundesgerichtes muss der Geschäftsherr insbesondere wirksame **Qualitätskontrollen** der von ihm hergestellten Produkte durchführen. Falls dies nicht möglich ist, muss ein Herstellungsprozess gewählt werden, welcher Schädigungen mit hoher Wahrscheinlichkeit ausschliesst (vgl. BGE 110 II 456 E. 3a/b). Bei komplexen IT-Produkten ist angesichts des Problems der praktischen Unvermeidbarkeit von Fehlern im Sinn der Technik entscheidend, wie weit die Testmassnahmen gehen müssen (vgl. zu Entwicklungsrisiken auch Kap. 4.7.5). Der notwendige Umfang von Tests hängt insbesondere vom Schädigungspotential des betreffenden Produkts ab. Besonders hohe Anforderungen gelten z. B. für medizinaltechnische Systeme.

Vereinzelte **Ausreisser innerhalb einer Produktionsserie**, welche auch durch sorgfältige Tests nicht erkannt werden konnten, führen nicht zur Geschäftsherrenhaftung des Herstellers. Dies ist aber praktisch nur für Hardware von Bedeutung, da Fehler in Standardsoftware grundsätzlich alle Exemplare des betreffenden Releases umfassen. Ausnahmen sind immerhin für Beeinträchtigungen durch Fehler der Datenträgern denkbar.

Der Geschäftsherr haftet nur, wenn eine Verletzung seiner Sorgfaltspflichten für die Entstehung des Schadens tatsächlich **kausal** war. Allerdings dürfte nur in seltenen Fällen der Beweis gelingen, dass der Schaden auch bei Aufwendung der nötigen Sorgfalt eingetreten wäre.

Soweit der Schaden durch ein fehlerhaftes Produkt verursacht wurde, kommt neben der Geschäftsherrenhaftung die Anwendung des **Produktehaftungsrechts** in Betracht. In welchem Verhältnis diese beiden Haftungsarten zu einander stehen, ist in der Schweiz noch nicht abschliessend geklärt. Es ist aber davon auszugehen, dass die Geschäftsherrenhaftung anwendbar ist, wenn die besonderen Voraussetzungen des Produktehaftungsrechts nicht gegeben sind (insbesondere, wenn kein Schaden im Sinn des Produktehaftungsgesetzes vorliegt). Die Produktehaftung des Geschäftsherrn hat somit vor allem noch Bedeutung für Sachschäden an kommerziell genutzten Gegenständen (z.B. Beschädigung von Produktionsanlagen durch Softwarefehler, Brände).

Inwieweit zu den Sorgfaltspflichten des Herstellers auch die **Beobachtung von bereits in Verkehr gebrachten Produkten** gehört (Produktemonitoring), bzw. ob er bei erst nachträglich erkennbarer Gefährlichkeit der Produkte zur Information bzw. zum Rückruf verpflichtet ist, wird international kontrovers diskutiert. Diese Frage ist im IT-Bereich vor allem für Sicherheitsprodukte relevant, welche gegen sich verändernde Gefährdungen keinen Schutz mehr bieten.

4 Produktehaftung

Ziel des Produktehaftungsrechts ist primär der Schutz der **Konsumenten und zufälligerweise geschädigter Dritter** *(innocent bystanders)* vor gefährlichen Produkten. 1985 hat die EU eine Richtlinie zur Vereinheitlichung der Vorschriften zur Haftung für fehlerhafte Produkte (PrHRL) erlassen, welche die Mitgliedstaaten dazu verpflichtet, ein der Richtlinie entsprechendes Produktehaftungsrecht einzuführen.

Unter das **EU-Produktehaftungsrecht** fallen auch schweizerische Hersteller, wenn deren Produkte in die EU exportiert werden und dort Schäden verursachen. Umgekehrt können ausländische Hersteller für in der Schweiz eingetretene Schäden hier ins Recht gefasst werden (vgl. zum anwendbaren Recht Art. 135 IPRG und zu Zuständigkeit und Vollstreckbarkeit Art. 5 Ziff. 3 LugÜ).

In der **Schweiz** hat die PrHRL zwar keine direkte Geltung. Aus der Entstehungsgeschichte des schweizerischen Produktehaftungsgesetzes (PrHG) ergibt sich aber das Bestreben einer engen Anlehnung an die PrHRL. Diese ist daher bei seiner Auslegung mit zu berücksichtigen.

Obwohl unsichere Informationssysteme zahlreich sind, gibt es bisher weder in der Schweiz noch in der EU Gerichtsentscheide zu Produktehaftung für **IT-Produkte**. Dies hängt vor allem damit zusammen, dass das Produktehaftungsrecht nicht alle Arten von Schäden umfasst: Bei Schäden an privat genutzten Gegenständen steht das Prozessrisiko meist in einem zu ungünstigen Verhältnis zum erreichbaren Schadenersatz, so dass solche Fälle in Europa praktisch nie gerichtlich ausgetragen werden.

4.1 Überblick über die Haftungsvoraussetzungen

Ein **Hersteller** haftet nach dem PrHG bzw. der PrHRL unter folgenden **Voraussetzungen**:

- Nachweis eines **Schadens** durch Tod, Körperverletzung oder an einem Gegenstand, welcher dem Privatgebrauch diente (Art. 1 PrHG/Art. 9 PrHRL),
- Verursachung durch ein **fehlerhaftes Produkt** (Art. 4 und 5 PrHG/Art. 6 PrHRL)
- **adäquate Kausalität** zwischen Schaden und Produktefehler.

Unter bestimmten Voraussetzungen kann sich der Hersteller von der Produktehaftung **entlasten** (vgl. dazu im einzelnen Kap. 4.7).

4.2 Schaden

Nur Schäden durch **Tod**, **Körperverletzung** oder an **Gegenständen, welche dem Privatgebrauch** dienen, sind vom Produktehaftungsrecht erfasst (vgl. zum Umfang der einzelnen Schadensarten Kap. 2.2). Schäden an kommerziell nutzbaren Objekten und sonstige Vermögensschäden liegen somit ausserhalb des Anwendungsbereiches des PrHG.

Mangelhafte Computerprogramme führen häufig zu **Datenverlust** und unerwünschter Datenveränderung. Nach der hier vertretenen Auffassung fallen diese nicht unter die vom Produktehaftungsrecht erfassten Schäden, da Daten anders als Computerprogramme auch nicht als ‚Produkt' im Sinn des PrHG bzw. der PrHRL zu qualifizieren sind. Die Frage wird allerdings international kontrovers diskutiert.

Schäden am fehlerhaften Produkt selbst sind vom Produktehaftungsrecht ebenfalls nicht erfasst. Dies kann mitunter zu schwierigen Abgrenzungsfragen zwischen Gesamtprodukt und Produktebestandteilen führen.

Das Produktehaftungsrecht hat somit nur für jene IT-Produkte oder Systeme **praktische Bedeutung**, welche zu Personenschäden führen können. Das ist bei Computerprogrammen zum Glück relativ selten der Fall. Allerdings haben Computerprogramme zur Temperaturüberwachung bereits zu Bränden geführt und Fehler in der Steuerungssoftware von Benzinpumpen und Verkehrsampeln schon schwere Verkehrsunfälle verursacht.

4.3 Produkt

Das Produktehaftungsrecht geht von körperlichen Sachen aus. Ob **Software** darunter fällt, ist in der Schweiz noch teilweise umstritten. Es zeichnet sich jedoch international eine klare Tendenz ab, diese Frage zu bejahen, unabhängig davon, ob die Software in ein anderes Produkt integriert oder als eigenständiges Gut vermarktet wird. Es spielt auch keine Rolle, ob ein Computerprogramm *online* übertragen oder auf einem physischen Datenträger geliefert wird.

Nach der hier vertretenen Auffassung besteht keine Produktehaftung für **reine Daten**, (z. B. fehlerhafte Informationen in Datenbanken) da diese keine produktetypische Funktionalität aufweisen und Schäden im Sinn des Produktehaftungsrechts erst durch die Umsetzung der Information entstehen. Die Frage der Produktehaftung für Informationen (z. B. fehlerhafte Angaben in Bücher, Flugkarten etc.) ist allerdings international kontrovers.

Obwohl die Produktehaftung vor allem auf industriell gefertigte Gegenstände zugeschnitten ist, umfasst sie auch **individuell hergestellte Produkte** (z. B. Individualsoftware und integrierte IT-Systeme).

Hingegen ist das Produktehaftungsrecht **nicht auf Dienstleistungen anwendbar**. Der Versuch, eine besondere ausservertragliche Dienstleistungshaftung einzuführen, ist in der EU vorläufig gescheitert. Allerdings können sich insbesondere bei Entwicklungs-, Wartungs- und Outsourcingleistungen schwierige Abgrenzungsfragen zwischen Produkten und Dienstleistungen stellen. Nach der hier vertretenen Auffassung ist entscheidend, ob solche Leistungen direkt ein funktionsfähiges Produkt erzeugen (z. B. lauffähiges Computerprogramm, nicht aber ein blosses Programmkonzept).

Reparatur und Wartung führen bei Computerprogrammen im Gegensatz zu Produkten, welche nur in den ursprünglichen Zustand bei Inverkehrbringen zurückversetzt werden, in der Regel zu einem veränderten Produkt. Damit unterliegen solche Leistungen grundsätzlich der Produktehaftung. Es erscheint jedoch bei nur einzelne Module erfassenden Änderungen nicht unbedingt sinnvoll, das modifizierte Programm als völlig neues Produkt zu betrachten und damit die Zehnjahresfrist seit Inver-

kehrbringen für das ganze Programm oder gar das ganze IT-System erneut auszulösen. Hingegen kann das geänderte Modul selbst als neues Produkt begriffen werden sofern es eigene produktetypische Gefährdungen mit sich bringt.

Outsourcingunternehmer, *Application Service Provider* und ähnliche Dienstleister haften grundsätzlich nur für das Zurverfügungstellen von selbst hergestellten Programmen als Produktehersteller, nicht aber für Verfügbarkeitsunterbrüche und dergleichen. Für Fremdprogramme kann allerdings eine Haftung als Importeur oder Lieferant bestehen (vgl. dazu Kap. 4.5).

4.4 Fehler

Ein durch ein Produkt verursachter Schaden führt nur dann zu einer Haftung des Herstellers, wenn es als fehlerhaft zu qualifizieren ist. Ob ihn ein Verschulden an der Fehlerhaftigkeit trifft, spielt hingegen keine Rolle. Der **Fehlerbegriff** des Produktehaftungsrechts ist weder mit dem Fehlerbegriff der Technik noch mit dem Mangelbegriff des Vertragsrechts identisch.

Ein Produkt ist dann fehlerhaft im Sinn des Produktehaftungsrechts, wenn es **berechtigte Sicherheitserwartungen** enttäuscht. Dies ist insbesondere anhand folgender Kriterien zu prüfen:

- **Produktepräsentation** (z. B. Werbung, Benutzerhandbücher und grafische Benutzeroberfläche)
- vernünftigerweise **zu erwartender Gebrauch**
- **Einsatzgebiet** (z. B. Steuerung von Operationsgeräten oder blosses Schreibprogramm)
- **Anwenderkreis** (z. B. professionelle, technisch versierte Anwender oder Laien)
- **Produktepreis**. Allerdings besteht auch bei günstigen Produkten ein Anspruch auf sichere Mindestfunktionalität.

Die relevanten Sicherheitserwartungen an ein Produkt beziehen sich auf die Schädigungsgefahr und nicht auf dessen technische Eigenschaften. Die Benutzer brauchen sich grundsätzlich keine konkreten Vorstellungen über die in einem Produkt enthaltenen Sicherheitsmechanismen zu machen, sondern sie dürfen davon ausgehen, dass es bei richtiger Anwendung keine Schäden an Leib und Leben oder privaten Gegenständen verursacht. Sicherheit besteht nach der hier vertretenen Auffassung immer nur im Hinblick auf einen bestimmten Gebrauch, so dass die Sicherheitserwartungen die zu erwartende **Bandbreite sicheren Gebrauchs** umfassen.

Diese Bandbreite des sicheren Gebrauchs muss neben dem Normalgebrauch auch vorhersehbare **Fehlgebrauchsarten** umfassen. Für IT-Produkte ist insbesondere an die Möglichkeit von Fehlmanipulationen durch falsche oder zufällige Eingaben zu denken, hingegen wohl nicht an Programmänderungen seitens des Benutzers. Wenn damit gerechnet werden muss, dass durch Fehleingaben produktehaftungsrelevante Schäden entstehen könnten, sind zumindest geeignete Rückfragen via Bildschirm einzubauen.

Unter Umständen muss ein Produkt auch **Sicherheit gegenüber äusseren Einflüssen** bieten (z. B. keine unnötige Gefährlichkeit im Fall von ‚Systemabstürzen'). Einzelne IT-Produkte wie Firewalls und Antivirenprogramme dienen ausschliesslich der Sicherheit und sollen Schutz vor gängigen Angriffstechniken garantieren. Betriebssysteme oder Programme, welche Zugang zum Internet verschaffen, erfüllen zwar primär einen anderen Zweck, stellen aber neuralgische Punkte innerhalb einer Sicherheitsarchitektur dar und können daher ebenfalls besondere Schutzerwartungen wecken. Für sicherheitsrelevante Produkte muss die Bandbreite der zu erwartenden Störungen ermittelt werden, welche vom Produkt kompensiert werden soll.

Das Produktehaftungsrecht stellt nicht auf die Einhaltung **technischer Normen** sondern auf die Enttäuschung berechtigter Sicherheitserwartungen ab. Immerhin kann die Verletzung einschlägiger Sicherheitsnormen ein Indiz für die Fehlerhaftigkeit des Produkts bilden.

Die Fehlerfreiheit eines Produkts kann grundsätzlich nicht an später in Verkehr gebrachten Produkten gemessen werden (Art. 4 Abs. 2 PrHG). Bei Serienprodukten, welche über längere Zeit hinweg hergestellt werden, ist auf die **Sicherheitserwartungen bei Inverkehrbringen** des konkret schadensstiftenden Exemplars abzustellen.

4.5 Hersteller

Nach dem PrHG haften folgende Personengruppen für die Schäden durch die Fehlerhaftigkeit der von ihnen in Verkehr gebrachten Produkte:

- **Hersteller des Endprodukts**
- Hersteller fehlerhafter **Produktebestandteile**
- ‚**Quasihersteller'** wie Zwischenhändler und Lizenzgeber, welche den Anschein erwecken, das Produkt selbst hergestellt zu haben.
- **Importeure**
- subsidiär **Lieferanten**

IT-Produkte durchlaufen meist Herstellungsschritte auf verschiedenen Marktstufen. Z. B. besteht ein integriertes IT-System aus Hard- und Softwarekomponenten einer Vielzahl von Herstellern. Im Sinn einer immer breiter werdenden ‚Haftungskaskade' haftet jeder Beteiligte für die Fehlerhaftigkeit seiner eigenen Leistung und derjenigen seiner ‚Vorhersteller', nicht aber für derjenigen der ‚Nachhersteller'. Als ‚Hersteller' werden vom Produktehaftungsrecht praktisch alle Beteiligten erfasst, welche **Verantwortung für die Qualität eines Produktes oder für dessen Inverkehrbringen** wahrnehmen können.

Voraussetzung für eine Haftung als Teilhersteller ist stets, dass ein **Arbeitsergebnis mit eigener produktetypischer Schädigungsgefahr** geschaffen wird (z. B. lauffähiges Unterprogramm, nicht aber blosse Mitarbeit, etwa durch Entwurf der Programmstruktur).

Wenn Lieferanten bzw. ***Assembler*** integrierte IT-Systeme aus Standardkomponenten zusammenstellen und installieren, fragt sich, ob sie als Gesamtproduktehersteller haften. Ein Produkt im Sinn des Produktehaftungsrechts ist mehr als die Summe seiner Bestandteile. Nach der hier vertretenen Auffassung ist entscheidend, ob der Assembler selbst produktetypische Risiken schafft, etwa durch Auswahl von Komponenten, Installation und Konfiguration.

Die rechtliche Einordnung von ***Freelancern,*** welche fehlerhafte Bestandteile entwickeln, hängt davon ab, inwieweit sie in die Arbeitsorganisation des Gesamtproduktehersteller eingebunden sind, insbesondere, ob sie faktisch an seine Weisungen gebunden sind. Sie sind nur dann als Teilhersteller zu betrachten, wenn dies nicht der Fall ist.

Für die Geschädigten ist es unter Umständen schwierig, Ansprüche gegenüber Herstellern durchzusetzen, welche ihren Sitz im Ausland haben (vgl. für die Mitgliedstaaten des EWR immerhin Art. 5 Ziff. 3 LugÜ). Die EU-Produktehaftungsrichtlinie sieht für Produkte, welche ausserhalb der EU bzw. des EWR-Raums hergestellt wurden daher eine Haftung des **Importeurs** vor. Eine analoge Haftung kennt das schweizerische PrHG für Produkte, welche nicht aus der Schweiz oder Liechtenstein stammen (Art. 2 Abs. 1 lit. c PrHG). Da Produktehaftungsansprüche gegenüber den Geschädigten nicht ausgeschlossen werden können, ist es für Importeure entsprechender Produkte wichtig, dass ihnen der Hersteller vertraglich zusichert, im Haftungsfall Ersatz zu leisten (Freistellung von der Haftung).

Schadenersatzansprüche stossen auch dann auf praktische Schwierigkeiten, wenn der Geschädigte nicht feststellen kann, wer das Produkt hergestellt bzw. importiert hat. Für diesen Fall sieht das Produktehaftungsrecht vor, dass auf den **Lieferanten** zurückgegriffen werden kann (Art. 2 Abs. 2 und 3 PrHG). Dieser kann sich allerdings durch die Bekanntgabe des Herstellers bzw. seines Lieferanten von der Haftung befreien.

Computerprogramme werden mitunter **via Internet** direkt vertrieben. Die eigentliche Importhandlung wird zwar durch den Erwerber ausgelöst, welcher das Programm auf dem fremden Server abruft und damit sozusagen

selbst einführt. Der *Online-Anbieter* kann jedoch als Importeur haften, wenn der Einspeisungsort im Ausland liegt.

Lizenzgeber, OEM-Partner etc. unterliegen dann der Produktehaftung, wenn sie den Eindruck erwecken, die Produkte selbst hergestellt zu haben bzw. die inhaltliche Verantwortlichkeit dafür zu tragen (Haftung als **Quasihersteller** nach Art. 2 Abs. 1 lit. b PrHG).

Für jeden Hersteller gilt die Weitergabe an die nächste Marktstufe als **Zeitpunkt des Inverkehrbringens.** Insbesondere Sicherheitsprodukte, welche im Zeitpunkt des Inverkehrbringens durch einen (Teil-)hersteller fehlerfrei waren, können bei der Weiterveräusserung durch den Gesamthersteller oder Importeur unter Umständen fehlerhaft sein, weil inzwischen neue Angriffstechniken aufgekommen sind, gegen welche es wirkungslos ist.

4.6 Kausalität

Schäden sind nur dann produktehaftungsrechtlich relevant, wenn ihre Verursachung einem fehlerhaften Produkt **adäquat kausal** zugeordnet werden kann (vgl. dazu Kap. 2.5).

Bei IT-Systemen mit Hard- und Softwarekomponenten verschiedener Hersteller und Lieferanten ist oft schwer festzustellen, welches Element nicht korrekt funktionierte und wer daher als Hersteller ins Recht gefasst werden könnte. Besondere Beweisschwierigkeiten bringen insbesondere **nicht reproduzierbare Fehler** mit sich. Gelingt es dem Geschädigten nicht, das Gericht davon zu überzeugen, dass der Schaden durch einen Fehler in einem bestimmten Produkt entstanden ist, muss er ihn selbst tragen.

Die Adäquanz der Schadensverursachung kann auch dann problematisch sein, wenn ein IT-System eine **falsche Information** generiert (z.B. unrichtige Berechnung medizinischer Analysedaten), aber erst deren unkritische Umsetzung durch eine Person zu einem Schaden führt. Ob die Erzeugung gefährlicher Fehlinformationen überhaupt einen Produktefehler darstellen kann, wird allerdings international kontrovers diskutiert.

Bei **wirkungslosen Sicherheitsprodukten** (z. B. Firewalls, Virenschutzprogramme), welche einen Schaden hätten verhindern sollen, ist zunächst zu prüfen, ob überhaupt berechtigte Sicherheitserwartungen hinsichtlich der Resistenz gegenüber den betreffenden Störungen bzw. Angriffen bestehen. Die Schädigung ist kausal, wenn sich belegen lässt, dass der Schaden nicht eingetreten wäre, wenn bei Kenntnis der Wirkungslosigkeit des betreffenden Produkts ein anderes, wirkungsvolles eingesetzt worden wäre oder der Geschädigte sich anders verhalten hätte.

4.7 Entlastungsgründe

Sowohl das PrHG als auch die PrHRL enthalten eine abschliessende Aufzählung von sechs Entlastungsgründen. Teilweise handelt es sich um echte Ausnahmen von der Haftung, teilweise um Konstellationen, in welchen im Grunde die Haftungsvoraussetzungen fehlen (durch deren Einordnung unter die Entlastungsgründe soll die Beweislast aber dem Hersteller auferlegt werden):

- Der Hersteller hat das fehlerhafte Produkte **nicht selbst in Verkehr gebracht**.
- Der **Produktefehler ist erst nach dem Inverkehrbringen** entstanden.
- Der **Hersteller eines Teilprodukts** haftet nicht, wenn der Fehler auf Anweisungen des Gesamtproduktehersteller oder Eigenschaften des Endproduktes zurückzuführen ist.
- Der Fehler beruht auf der **Einhaltung zwingender rechtlicher Normen**.
- Der Fehler war nach dem Stand der Wissenschaft und Technik **im Zeitpunkt des Inverkehrbringens nicht erkennbar**.
- Das Produkte wurde **nicht im Rahmen einer kommerziellen Tätigkeit** hergestellt bzw. vertrieben.

4.7.1 Fehlendes Inverkehrbringen

Nach der gängigen Definition gilt ein Produkt als in Verkehr gebracht, sobald der Hersteller es willentlich aus seinem Herrschaftsbereich entlassen hat (**Werktorprinzip**). Auf die Eigentumsverhältnisse kommt es dabei nicht an, so dass auch bloss befristet lizenzierte Software als in Verkehr gebracht gilt. Entscheidend ist, dass das Produkt dem Erwerber zugänglich gemacht wurde. Computerprogramme dürften *online* in Verkehr gebracht sein, sobald sie von den Benutzern ordnungsgemäss heruntergeladen werden können.

Selbst hergestellte Produkte, welche **bei der Erbringung einer Dienstleistung** verwendet werden, gelten auch als in Verkehr gebracht (vgl. dazu den Entscheid des EuGH vom 10.5.2001 in der Rechtssache C-203/99, Veedfald/Arhus Amtskommune, Slg. 2001 I 3569).

Raubkopien lösen keine Produktehaftung des Originalherstellers aus, da sie nicht vom Hersteller in Verkehr gebracht wurden. Hingegen stellt die Übernutzung grundsätzlich nur ein vertragsrechtliches Problem zwischen Hersteller und Lizenznehmer dar. Allerdings können sich bei der unerlaubten Herstellung zusätzlicher Programmkopien schwierige Abgrenzungsfragen stellen.

4.7.2 Nachträglich entstandene Produktefehler

Ursprünglich korrekt funktionierende IT-Produkte können im Lauf der Zeit fehlerhaft werden (z. B. durch Alterung von Datenträgern). Dies führt allerdings nicht in jedem Fall zu einer Entlastung des Herstellers: Fehlte es im Zeitpunkt des Inverkehrbringens an der **Sicherheit für die zu erwartende Gebrauchsdauer**, war der Fehler bereits latent vorhanden.

IT-Sicherheitsprodukte wie Firewalls und Antivirenprogramme werden nicht dadurch fehlerhaft, dass nach ihrem Inverkehrbringen **neuartige Angriffstechniken** auftauchen (vgl. zur Produktebeobachtung allerdings Kap. 3). Waren bestimmte Angriffsmethoden hingegen damals bereits bekannt oder naheliegend, ist zu prüfen, ob die Nutzer damit rechnen durften, dass das Produkt Sicherheit dagegen biete.

4.7.3 Entlastungsbeweis des Teilherstellers

Das Gefahrenpotential bestimmter Teilprodukten entsteht erst in Verbindung mit anderen Elementen bzw. dem Gesamtprodukt. Sicherheit von Informationssystemen ist in gewissen Bereichen nur durch eine kohärente IT-Sicherheitsarchitektur zu erreichen. Wenn eine Komponente in einer bestimmten IT-Umgebung nicht sicher funktioniert, kann dies darauf zurückzuführen sein, dass sie nicht den typischerweise an solche Teilprodukte gestellten **Anforderungen** entspricht. Es kann aber auch sein, dass ihre Auswahl oder Integration in das Gesamtprodukt nicht fachgerecht erfolgt ist. Im letzteren Fall wird der Teilhersteller entlastet, da die Auswahl geeigneter Komponenten und deren Integration in den Verantwortungsbereich des Gesamtherstellers fällt.

Der Teilhersteller haftet auch dann nicht, wenn der Fehler auf **Vorgaben des Gesamtherstellers** beruht. Diese können sowohl die Spezifikationen des Teilprodukts als auch unrichtige Angaben über den Verwendungszweck betreffen. Der Teilhersteller wird allerdings wohl nur entlastet, wenn er die Fehlerhaftigkeit der Anleitung weder erkannt hat noch hätte erkennen müssen.

4.7.4 Einhaltung zwingender Normen

Der Hersteller haftet nicht für Fehler, welche durch die **Einhaltung verbindlicher, hoheitlich erlassener Vorschriften** (nicht aber privater Standards wie ISO-Normen!) verursacht wurden. Eine Befreiung von der Haftung setzt allerdings voraus, dass keine Konstruktionsvariante möglich ist, welche sowohl der Norm entspricht als auch den Fehler vermeidet. Dieser Entlastungsgrund hat daher nur in Ausnahmefällen praktische Bedeutung.

4.7.5 Entwicklungsrisiken

Computerprogramme bestehen oft aus Hunderttausenden oder gar Millionen von Zeilen mit einzelnen Befehlen, Hardwarechips aus Millionen elektrischer Schalter. Statistische Untersuchungen gehen davon aus, dass ungefähr jede 66. Programmzeile einen **technischen Fehler** enthält. Davon

wird durchschnittlich etwa die Hälfte beim Testen noch entdeckt. Innerhalb eines grösseren Computerprogramms ist zudem die Anzahl möglicher Verknüpfungen beim Programmablauf vom menschlichen Vorstellungsvermögen nicht mehr fassbar. Ähnliches gilt für Hardware. Beträgt beispielsweise die Ausfallwahrscheinlichkeit pro Transistor 1:1'000'000 pro Stunde, ist davon auszugehen, dass innerhalb eines Mikroprozessors mit 10 Mio. Transistoren durchschnittlich ca. 10 Transistoren pro Stunde ausfallen. Ab einer gewissen Komplexität ist bei IT-Produkten eine Fehlerhaftigkeit im Sinn der Informatik somit unvermeidbar. Daraus resultiert eine erhöhte Gefahr von produktehaftungsrechtlich relevanten Fehlfunktionen. Währenddem die völlige Elimination aller Fehler statistisch gesehen praktisch ausgeschlossen ist, wäre jeder dieser Fehler einzeln ohne weiteres erkennbar und damit auch vermeidbar gewesen.

Eine Haftungsbefreiung ist nur dann möglich, wenn der Produktefehler im Zeitpunkt des Inverkehrbringens weder nach dem Stand der Wissenschaft noch nach demjenigen der Technik hätte erkannt werden können. Bei solchen Fehlern handelt sich sog. **Entwicklungsrisiken**. (Vgl. dazu auch den Entscheid des EuGH vom 29. Mai 1997 in der Rechtssache C-300/95 Kommission gegen Grossbritannien und Nordirland, Slg. 1997 I 2649, der festhält, dass der Hersteller beweisen muss, dass der Fehler nach dem objektiv höchsten, publizierten Stand der Wissenschaft und Technik nicht erkannt werden konnte). Der Hersteller haftet daher immer, wenn die Entdeckung des konkret schadensverursachenden Mangels möglich gewesen wäre. Er kann somit keine generelle Entlastung aus der Tatsache ableiten, dass komplexe IT-Produkte nie fehlerfrei im Sinn der Technik sind. Entwicklungsrisiken könnten immerhin für Sicherheitsprodukte von praktischer Bedeutung sein, welche sich gegenüber neuen und nicht ohne weiteres nahe liegenden Angriffstechniken als unwirksam erweisen (z. B. Antivirenprogramme).

Die Problematik der **statistischen Unvermeidbarkeit von IT-Fehlern** ist in der Informatik allgemein bekannt und kann unter Umständen die Erwartungen an die Bandbreite sicherer Anwendungen beeinflussen. Die Verwendung der Produkte im Rahmen des Haupteinsatzzwecks muss aber in jedem Fall sicher sein. Beispielsweise stellen Softwarefehler in chirurgi-

schen Operationsgeräten, welche zu einem Schädigungsrisiko für die Patienten führen, generell Fehler im Sinn des Produktehaftungsrechts dar.

4.7.6 Nichtkommerzielle Tätigkeit

Währenddem der **private Import** überhaupt nicht unter das Produktehaftungsrecht fällt, ist für die **private Herstellung und** den **privaten Vertrieb** nur dann eine Entlastung möglich, wenn sie keinen wirtschaftlichen Zweck verfolgen.

Die kommerzielle ‚**Gratisbeigabe'** von Software zu anderen Produkten fällt ohne weiteres unter das Produktehaftungsrecht, da sie Teil der Gegenleistung für ein Gesamtentgelt ist und somit eigentlich gar nicht gratis erfolgt.

Heikel ist die Einordnung von ***Open Source*** Software (z.B. Programme und Programmbibliotheken, welche unter der GNU General Public License stehen). Hier ist zwischen verschiedenen Konstellationen zu differenzieren: Unter das Produktehaftungsrecht fallen grundsätzlich der kommerzielle Vertrieb von Datenträgern mit an sich freier Software sowie die Entwicklung von Gratissoftware im Rahmen eines Geschäftsmodells, welches darauf abzielt, softwarebezogene Dienstleistungen zu verkaufen. Hingegen ist die rein private Arbeit für Open Source Projekte von der Haftung ausgenommen.

4.8 Verjährung und Verwirkung

Ansprüche aus Produktehaftungsrecht müssen innert **drei Jahren nach Eintritt des Schadens**, spätestens jedoch innert **zehn Jahren seit dem Inverkehrbringen des Produkts** geltend gemacht werden (Art. 9 und 10 PrHG).

4.9 Produkteinformation und Rückruf

Produkterisiken lassen sich bis zu einem gewissen Grad durch geeignete **Information** (Bedienungsanleitung, Warnhinweise auf dem Produkt etc.) vermeiden. Vollständige Information über Restrisiken verhindert die Entstehung ungerechtfertigter Sicherheitserwartungen (vgl. dazu auch Kap. 4.4). Hingegen sind pauschale Hinweise auf die softwaretypische Fehlerinhärenz nicht relevant, da sie den Benutzern keine Anhaltspunkte für ein risikogerechtes Verhalten liefern.

Obwohl weder das PrHG noch die PrHRL den Rückruf von Produkten nach deren Inverkehrbringen regeln, kann sich für den Hersteller **nachträgliche Produkteinformation** oder ein **Produkterückruf** aus verschiedenen Gründen aufdrängen:

- Solche Massnahmen dienen zunächst einmal der **Vermeidung von Schädigungen** und damit von Haftungsansprüchen und Imageverlusten. Der Hersteller kann sich allerdings durch Rückruf bzw. Austausch fehlerhafter Produkte nur gegenüber den von einer solchen Aktion konkret Erreichten von einer Schadenersatzpflicht befreien.

- Falls das Produkt Leib und Leben von Personen gefährdet (z. B. fehlerhafte medizinische Geräte), kann die Untätigkeit des Herstellers zu einer **strafrechtlichen Verantwortlichkeit** führen (vgl. dazu BGE 121 IV 15 E. 3a).

- Erkennt der Hersteller nachträglich die Gefährlichkeit seines Produkts, könnte sich auch im schweizerischen Recht eine Informations- oder Rückrufpflicht aus **nachvertraglichen Nebenpflichten** oder aus der **Geschäftsherrenhaftung** von Art. 55 OR ergeben.

- Versicherungspolicen sehen regelmässig Schadensverhinderungspflichten vor, bei deren Nichtbefolgung die **Versicherungsansprüche erlöschen**.

- Die **EU-Produktesicherheitsrichtlinie 2001/95/EG** verpflichtet den Hersteller zur Beobachtung und eventuell zum Rückruf von in der EU in Verkehr gebrachten gefährlichen Produkten (vgl. Art. 5 Abs. 1 PrSRL).

5 Schadensverhütung und Schadensminderung

Sind die Benutzer über Sicherheitslücken eines Informationssystems informiert, so haben sie sich nach den Grundsätzen der Schadensverhütung und der Schadensminderung zu verhalten und müssen es anpassen, soweit sonst mit der Verursachung von Schäden zu rechnen ist. Andernfalls kann die Schadenersatzpflicht wegen Selbstverschulden herabgesetzt oder aufgehoben werden (Art. 44 OR).

Wenn das Selbstverschulden die Bedeutung der sonstigen Schadensursachen verblassen lässt, kann es ausnahmsweise sogar deren **adäquaten Kausalzusammenhang unterbrechen**, so dass die Schadenersatzpflicht prinzipiell entfällt (vgl. dazu Kap. 2.5).

Ein hohes Mass an Informationssicherheit kann nur durch **Zusammenwirken von IT-Herstellern/Dienstleister und Anwender** erreicht werden. Vernachlässigt der Anwender diejenigen Sicherheitsmassnahmen, welche von ihm objektiv erwartet werden können, muss er eine Kürzung bzw. im Extremfall sogar den Wegfall seiner Schadenersatzansprüche in Kauf nehmen.

Soweit das Löschen bzw. Verändern von Daten überhaupt zu einer ausservertraglichen Haftung führt (vgl. dazu Kap. 2.3), stellt sich die Frage, inwieweit **Datensicherung** zu den Schadensverhütungspflichten der Anwender gehört. Währenddem zumindest bei Unternehmen das Vorhandensein einer Datensicherung heute generell vorausgesetzt werden kann, lässt sich die vorauszusetzende Häufigkeit und Art kaum generell bestimmen (z.B. bloss tägliche Bandsicherung von Daten oder zeitnahe Spiegelung laufender Systeme).

Die Schadenshöhe bei IT-Ausfällen hängt oft in erheblichem Mass davon ab, ob der Betroffene auf eine entsprechende Situation vorbereitet war oder nicht (z.B. ob organisatorische und technische Vorkehren zu einem Wiederanlauf der Produktion getroffen wurden). In welchem Mass ein **Disaster Recovery Planning** heute allgemein vorausgesetzt werden kann, hängt ebenfalls von Art und Grösse des Unternehmens ab. Es handelt sich dabei sozusagen um präventive Schadensminderungspflichten.

Um zu belegen, dass alle sich aufdrängenden Schadensverhütungs- und Schadensminderungsmassnahmen getroffen wurden, bzw. dass kein Selbstverschulden vorliegt, kann für den Betreiber eines Informationssystems der Nachweis eines aktuellen **Sicherheitskonzepts** und die periodische Überprüfung seiner Einhaltung wichtig sein.

6 Konkurrenz von Haftpflichtigen

Haben mehrere Personen an Konzeption, Produktion, Installation, Verkauf und Wartung eines fehlerhaften IT-Systems oder an der Erbringung einer schädigenden IT-Dienstleistung mitgewirkt, ist zu prüfen, wer welche Verantwortung an der Schadensentstehung trägt. **Gegenüber dem Geschädigten** haften alle Verursacher gemeinsam (solidarisch). Ein allfälliges Selbstverschulden des Geschädigten kann jedoch zu einer Reduktion des Gesamtbetrages führen. Jeder Schadensverursacher kann sich jedoch auf allfällige eigene Entlastungsgründe und auf die für ihn geltenden Verjährungsfristen berufen (Art. 144 ff. OR).

Bei der Bestimmung der Höhe von **Regressansprüchen** gegenüber Mitverursachern hat der Richter letztlich Wertungen über den Grad der Verantwortung der beteiligten IT-Herstellern und -Dienstleistern vorzunehmen (vgl. dazu aber auch Art. 51 OR).

7 Haftungsbeschränkungen

Ausservertragliche Ansprüche unterliegen grundsätzlich der **Vertragsfreiheit** so dass der potentiell Geschädigten zum voraus auf sie verzichten kann. Allerdings gilt es dabei verschiedene **Einschränkungen** zu beachten:

- Ein zum voraus getroffener Haftungsausschluss für rechtswidrige **Absicht** oder **grobe Fahrlässigkeit** ist nichtig (Art. 100 OR). Hingegen kann die Haftung für Hilfspersonen vollständig wegbedungen werden (Art. 101 Abs. 2 OR). In Ausnahmefällen kann aber ein schwerwiegendes Verschulden des Geschäftsherrn hinsichtlich Auswahl, Instruktion und Überwachung der Hilfsperson zu einer Haftung aus unerlaubter Handlung führen.

- Auch ein zum voraus erklärter Verzicht auf Haftung für leichtes Verschulden kann nach Ermessen des Richters als nichtig betrachtet werden, wenn die Verantwortlichkeit aus dem Betrieb eines ‚**obrigkeitlich konzessionierten Gewerbes'** folgt (Art. 100 Abs. 2 OR). Im IT-Bereich können insbesondere Telekommunikationsleistungen auf obrigkeitliche Konzessionen basieren.

- In Ausnahmefällen kann ein Haftungsverzicht als **sittenwidrig** erscheinen und aus diesem Grund ebenfalls als nichtig betrachtet werden. Nach der wohl herrschenden Lehre kann insbesondere das Ausnützen einer Monopolstellung zur Durchsetzung von Haftungsfreizeichnungen unzulässig sein. Allerdings gibt es bisher noch kaum Gerichtsentscheide zu dieser Frage.

- Eine Beschränkung von Ansprüchen aus dem **Produktehaftungsgesetz** ist nichtig (Art. 8 PrHG).

Nach Schadenseintritt kann der Geschädigte in jedem Fall auf die Geltendmachung seiner Haftungsansprüchen verzichten.

Indirekt kann die Durchsetzung von Haftungsansprüchen auch über vertragliche **Regeln zur Beweislastverteilung und Schadensberechnung** beeinflusst werden.

Umfassen generelle Haftungsausschlüsse (Freizeichnungsklauseln) in IT-Verträgen auch ausservertragliche Ansprüche? Dies ist letztlich durch Auslegung des konkreten Vertrages zu ermitteln. Im Zweifel ist wohl davon auszugehen, dass ausservertragliche Ansprüche – soweit gesetzlich überhaupt zulässig – von einem Haftungsausschluss mit umfasst werden (vgl. dazu BGE 107 II 161, E. 8, offen gelassen allerdings in BGE 111 II 471).

8 Ergebnisse

Bisher gibt es in der Schweiz keine Gerichtsentscheidungen zur ausservertraglichen Haftung von IT-Anbietern in Zusammenhang mit ungenügender Sicherheit ihrer Produkte und Dienstleistungen. Trotzdem gibt es Konstel-

lationen, in welchen solche Ansprüche praktische Bedeutung erlangen können. Zu denken ist insbesondere an **Sach- und Personenschäden** durch Fehlfunktion von softwaregesteuerten Geräten und Anlagen. Bisher ungeklärt ist hingegen die Frage, in welchem Mass Datenverlust zu ausservertraglichen Ansprüchen führt (Verletzung eigentumsähnlicher Rechte oder blosse Vermögensschäden?).

Ausservertragliche Ansprüche sind vor allem relevant, wenn zwischen IT-Anbieter und Geschädigtem kein Vertragsverhältnis bestehet oder **vertragliche Ansprüche** durch Verzicht, Verjährung oder Verwirkung **untergegangen** sind. Zudem sind vertragliche Haftungsbeschränkungen gegenüber ausservertraglichen Ansprüchen nur innerhalb gewisser Grenzen möglich (z.B. kein Ausschluss von Produktehaftungsansprüchen).

Die informatiktypische Unvermeidbarkeit von Fehlern in Sinn der Technik führt nicht zu einer Befreiung des Herstellers von der Produktehaftung. Wenn fehlerhafte IT-Produkte zu Personenschäden führen, wird die Haftung aus unerlaubter Handlung/Geschäftsherrenhaftung daher weitgehend durch das **Produktehaftungsrecht** verdrängt. Es ist allerdings denkbar, dass aus den generellen Sorgfaltspflichten von Art. 55 OR in Zukunft auch in der Schweiz eine Pflicht zur Beobachtung und zum Rückruf bereits in Verkehr gebrachter Produkte, welche sich nachträglich als gefährlich erweisen, abgeleitet werden könnte.

Bisher ungeklärt ist die Frage, ob **Informationssysteme, welche falsche Informationen generieren** (z.B. unrichtige medizinische Daten) unter die Produktehaftung fallen. Bei spezifischen **IT-Sicherheitsprodukten** wie *Firewalls* muss im Einzelfall geprüft werden, gegenüber welchen Angriffstechniken von ihnen Sicherheit erwartet werden darf und inwieweit sie Lücken in den übrigen Teilen der Sicherheitsarchitektur eines Informationssystems kompensieren müssen.

Hinweise auf weiterführende Literatur

SCHWEIZ

BREHM ROLAND, Die Entstehung durch unerlaubte Handlungen, Kommentar zu Art. 41-61 OR, in: Berner Kommentar zum schweizerischen Privatrecht, Teilband VI/1/3/1, Bern 1998; **BÜHLER ROLAND**, Produktehaftung für Software, in: Software-Schutz Software-Haftung, Zürich 1992, S. 92 ff., und ***ders.***, Definition des Produktfehlers im Produktehaftpflichtgesetz, AJP 1993, S. 1425 ff.; **DESCHENAUX HENRI/TERCIER PIERRE**, La responsabilité civile, 2. A., Bern 1982; **FELLMANN WALTER**, Kommentar zum Produktehaftpflichtgesetz, in: Kommentar zum schweizerischen Privatrecht, Obligationenrecht I, 2. A., Basel/Frankfurt a. M. 1996; **FELLMANN WALTER/VON BÜREN-VON MOOS GABRIELLE**, Grundriss der Produkte-Haftpflicht, Bern 1993; **HESS HANS-JOACHIM**, Kommentar zum Produktehaftpflichtgesetz, 2. A., Bern 1996; **HILTY RETO M.**, Produktehaftpflicht und Lizenzverträge, JKR 2000, S. 74 ff.; **HOLLIGER-HAGMANN EUGÉNIE**, Management der Produkthaftpflicht, Zürich 2001; **OFTINGER KARL/STARK EMIL W.**, Schweizerisches Haftpflichtrecht, Band I, 5. A., Zürich 1995, Band II/1, 4. A., Zürich 1987; **HONSELL HEINRICH**, Schweizerisches Haftpflichtrecht, 2. A., Zürich 1996; **KELLER ALFRED**, Haftpflicht im Privatrecht, Band I, 6. A., Bern 2001, Band II, 2. A. 1998; **MORSCHER LUKAS**, Software-Überlassung nach Schweizer Recht; Urheberrecht, Gewährleistungspflichten, Produkthaftung, CR 1999, S. 262; **ROBERTO VITO**, Produktehaftpflicht und Software, JKR 2000, S. 56 ff.; ***ders.***, Schweizerisches Haftpflichtrecht, Zürich 2002; **STOESSEL GERHARD**, Haftung des Lizenzgebers nach Produktehaftpflichtrecht, SVZ 1999, S. 70 ff.; **SCHNYDER ANTON K.**, Art. 51-59 OR, in: Kommentar zum schweizerischen Privatrecht, Obligationenrecht I, 2. A., Basel/Frankfurt a. M. 1996; **STRAUB WOLFGANG**, Produktehaftung für Informationstechnologiefehler, Zürich 2002; **WEBER ROLF H.**, Informatik und Jahr 2000, Risiken und Vorsorgemöglichkeiten aus rechtlicher Sicht, Zürich 1998

EUROPÄISCHE UNION

BARTSCH MICHAEL, Computerviren und Produkthaftung, CR 2000, S. 721 ff.; **BAUER AXEL**, Produkthaftung für Software nach geltendem und künftigem deutschen Recht, PHI 1992, S. 38 ff. und 98 ff.; **CAHN ANDREAS**, Produkthaftung für verkörperte geistige Leistungen, NJW 1996, S. 2899 ff., ***ders.***; Münchner Kommentar zum Bürgerlichen Gesetzbuch, Band 5, 3. A., München 1997; **GÜNTHER ANDREAS**, Produkthaftung für Informationsgüter; Verlagserzeugnisse, Software und Multimedia im deutschen und US-amerikanischen Produkthaftungsrecht, Köln 2001, zugl. Diss. München 2000; **HEYMANN THOMAS**, Haftung des Softwareimporteurs, CR 1990, S. 176 ff.; **HOEREN THOMAS**, Produkthaftung für Software – zugleich eine kritische Erwiderung auf Bauer,

PHI 1989, S. 138 ff.; **KARDASIADOU ZOI**, Die Produkthaftung für fehlerhafte medizinische Expertensysteme, Baden-Baden 1998; **KORT MICHAEL**, Produkteigenschaft medizinischer Software, Einordnung im deutschen und US-amerikanischen Produkthaftungsrecht, CR 1990, S. 171 ff.; **KULLMANN HANS JOSEF/PFISTER BERNHARD**, Produzentenhaftung, Loseblattsammlung, Berlin 1980 ff.; **KURBOS RAINER**, Computerausfall – wer zahlt? Wien/Frankfurt 1999; **LEHMANN MICHAEL**, Produzenten- und Produkthaftung für Soft- und Hardware, in: Michael Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, 2. A., Köln 1993, S. 999 ff.; ***ders.***, Produkt- und Produzentenhaftung für Software, NJW 1992, S. 1721 ff.; **LLOYD IAN J.**, Information Technology Law, 3. A., London/Edinburgh/Dublin 2000; **MEIER KLAUS/ANDREAS WEHLAU**, Produzentenhaftung des Softwareherstellers, § 823 Abs. 1 BGB und das Produkthaftungsgesetz, CR 1990, S. 95 ff.; **MUSULAS GIORGOS**, Die Haftung des Softwareherstellers im Hinblick auf das ProdHaftG, Diss. Berlin 1990; **OECHSLER JÜRGEN**, Produktehaftungsgesetz, in: J. von Staudingers Kommentar zum bürgerlichen Gesetzbuch mit Einführungsgesetzen und Nebengesetzen, 13. Bearbeitung, Berlin 1998; **ROLLAND WALTER**, Produkthaftungsrecht, Kommentar, Köln 1990; **SCHMIDT-SALZER JOACHIM**, Kommentar EG-Richtlinie Produkthaftung, Band 1, 2. A., Heidelberg 1988; **SPINDLER GERALD**, Haftungsrecht, in: Thomas Hoeren/Ulrich Sieber (Hrsg.), Handbuch des Multimediarechts (Loseblatt), München 1999, Teil 29; **TASCHNER HANS CLAUDIUS/FRIETSCH EDWIN**, Produkthaftungsgesetz und EG-Produkthaftungsrichtlinie, 2. A., München 1990; **TAEGER JÜRGEN**, Ausservertragliche Haftung für fehlerhafte Computerprogramme, Tübingen 1995; ***ders.***, Produkt- und Produzentenhaftung bei Schäden durch fehlerhafte Computerprogramme, CR 1996, S. 257 ff.; **THÖMEL JENS-ARNE**, Datenbankverträge: Rechtsnatur und Haftung für fehlerhafte Information, Frankfurt a. M. 2002, zugl. Diss Frankfurt a. M. 2001; **VON WESTPHALEN FRIEDRICH**, Produkthaftungshandbuch Band 2, 2. A., München 1999.