Rechtsanwendung

Wer haftet für Mängel in der IT-Sicherheit?

Autor
Wolfgang Straub,
Dr. iur. LL.M.,
Rechtsanwalt, Bern,
wolfgang.straub@
advobern.ch

Unter Informatiksicherheit kann Unterschiedliches verstanden werden. Nach der nachfolgend verwendeten Konzeption umfasst sie drei sich teilweise überschneidende Aspekte:

- Sicheres Funktionieren eines Informationssystems unter Normalbedingungen – das ist z.B. dann nicht der Fall, wenn Softwarefehler zu Systemausfällen oder Datenverlust führen.
- Angemessene Reaktion auf externe Einflüsse und ausserordentliche Belastungen, z.B. geordnete Beendigung von Rechenprozessen bei Ausfall von Strom, Datenübertragung oder Teilen der IT-Architektur, Verhindern des Systemabsturzes bei aussergewöhnlichen Datenmengen, und Auslösen von Warnungsmeldungen, wenn gefährliche Produktionsprozesse nicht mehr kontrolliert werden können.
- Resistenz gegenüber Angriffen Dritter, z.B. Hackerangriffe, Viren, Zugriffe nichtberechtigter Mitarbeiter.

Bereits diese Beispiele machen deutlich, dass Sicherheit stets etwas Relatives ist. Kein grösseres Informationssystem kann auf Dauer ohne Strom funktionieren oder ist gegen Fremdeinwirkungen völlig immun. Die Informationssicherheit ist insbesondere dann ungenügend, wenn konkrete Gefahr besteht, dass Daten unrichtig verarbeitet oder gelöscht werden, dass Unbefugte Zugriff auf Daten oder Prozesse haben oder dass IT-gesteuerte gefährliche Prozesse (z.B. Produktionsanlagen) ausser Kontrolle geraten.

Diese Fragen müssen laufend neu beurteilt werden. Auch in Systemen, die zum Zeitpunkt der Inbetriebnahme ausreichend sicher waren, können jederzeit neue Sicherheitslücken entstehen. Unter rechtlichen Gesichtspunkten stellt sich die Frage, wer welche Sicherheitsaspekte eines Informationssystems wann überprüfen muss und wie die Betroffenen auf erkannte Risiken reagieren müssen, z.B. sofortige Information und baldmöglichste Nachbesserung durch den Hersteller eines bestimmten Produkts, schadensverhütende Massnahmen durch Benutzer.

Sicherheitslücken

Informationssysteme sind von zahlreichen Sicherheitsmängeln betroffen, die in ähnlicher Form auch bei anderen Produkten und Anlagen vorkommen und daher keine neuartigen Rechtsfragen aufwerfen, z.B. Abhängigkeit von Infrastruktur, Verletzlichkeit gegenüber Dritteinwirkungen, Konstruktionsfehler. IT-typisch sind aber insbesondere folgende Probleme:

- Informationssysteme sind weltweit Angriffen via Internet ausgesetzt. Das erfordert besondere Sicherheitsvorkehrungen und bringt Fragen nach dem anwendbaren Recht mit sich.
- Es ist praktisch kaum möglich, ein genügend sicheres Informationssystem herzustellen. Grössere Informationssysteme enthalten auf-grund ihrer Komplexität quasi naturgemäss Sicherheitslücken. Technisch gesehen ist jeder einzelne Sicherheitsmangel vermeidbar. Informatiktypisch ist jedoch die Schwierigkeit der lückenlosen Erkennung. Die Berücksichtigung aller Interdependenzen überfordert teilweise das menschliche Denkvermögen. Die Frage der konkreten Vermeidbarkeit von Sicherheitslücken ist für alle vertraglichen und ausservertraglichen Haftungsarten[1], die ein Verschulden voraussetzen, von entscheidender Bedeutung.

Rechtsprobleme

Sicherheitslücken in Informationssystemen können insbesondere Datenverlust, Leistungsausfall oder unkontrollierte Systemreaktionen verursachen. Diese führen mitunter ihrerseits zu Sach- und Personenschäden, z.B. Körperverletzungen bei Fehlsteuerung von Fertigungsrobotern oder Brände bei Ausfall von Temperatursteuerungen. Störungen können aber auch Forderungen Dritter wegen Leistungsausfall oder Verzögerungen auslösen. Im Hinblick auf finanzielle Ansprüche sind insbesondere folgende Ebenen zu unterscheiden:

- Gewährleistungs- und Schadenersatzansprüche der Betreiber gegenüber den für

Konzeption, Herstellung und Wartung verantwortlichen Unternehmen, z.B. Hard- und Softwarehersteller, Outsourcingpartner. Da es oft an einem Vertragsverhältnis zwischen den Geschädigten und dem verantwortlichem Hersteller bzw. Dienstleister fehlt oder vertragliche Ansprüche bereits verjährt sind, haben auch ausservertragliche Haftungsnormen praktische Bedeutung. Reine Vermögensschäden sind dadurch allerdings nur ausnahmsweise gedeckt. Ob auch Datenverlust und Datenveränderung darunter fallen, ist noch kaum geklärt.

- Ansprüche von Kunden der Betreiber für mangelhafte oder verspätete Leistungserbringung.
- Ansprüche zufällig geschädigter Dritter, z.B. durch Fehlfunktion einer Produktionsanlage verletzte Mitarbeiter.
- Ansprüche der direkt oder indirekt Geschädigten gegenüber ihren Versicherungen und Rückgriffsansprüche der Versicherungen auf die Schadensverursacher.
- Verantwortlichkeitsansprüche von Aktionären gegenüber Geschäftsleitung, Verwaltungsrat und Revisoren für schwerwiegende Versäumnisse bei der Organisation und Kontrolle des Bereichs Informationssicherheit.

Ungenügende Sicherheit von Informationssystemen wirft zudem Fragen in weiteren Rechtsgebieten auf:

- Verletzung des Datenschutzrechts, wenn Personendaten wegen Sicherheits-lücken von Unbefugten eingesehen werden können[2].
- Verletzung straf- und verwaltungsrechtlicher Vorschriften, wenn Systeme nicht den Sicherheitsanforderungen entsprechen oder Berufsgeheimnisse nicht ausreichend geschützt werden[3].
- Strafrechtliche Konsequenzen gegenüber Dritten, die unbefugt in IT-Systeme eindringen oder Störungen verursachen[4].

Kaum Präzedenzfälle

Schadenersatz im Zusammenhang mit IT-Sicherheitslücken zu erlangen, ist in der Praxis mit verschiedenen Schwierigkeiten verbunden:

- Schadenersatz setzt zunächst voraus, dass eine entsprechende vertragliche oder ausservertragliche Grundlage besteht.
- Schäden entstehen im IT-Bereich oft durch ein komplexes Zusammenwirken verschiedener Faktoren. Dies wird am Beispiel eines Hackerangriffs deutlich, der nur deshalb erfolgreich war, weil eine Sicherheitslücke im Betriebssystem bestand, der Systemadministrator ein Sicherheitspatch nicht rechtzeitig installierte und die Firewall schlecht konfiguriert war. Den Hacker ausfindig zu machen, ist meist schwierig und finanziell unergiebig. Wer in einem derartigen Fall den Hersteller des Betriebssystems, den Lieferanten der Firewall oder den Systemadministrator belangen will, muss beweisen, dass der Betreffende durch sein Handeln bzw. Unterlassen einen wesentlichen Beitrag zur Schadensentstehung geleistet hat.
- Es muss stets geprüft werden, ob die Ansprüche im konkreten Fall noch durchsetzbar sind. Dem können beispielsweise vertragliche Haftungsausschlüsse, Verjährung oder nicht rechtzeitige Rüge von Sicherheitsmängeln entgegenstehen.
- Bei IT-Sicherheitslücken stellt sich regelmässig die Frage nach der Eigenverantwortung der Betreiber des betreffenden Systems bzw. ihrer Systemadministratoren. Ein Selbstverschulden kann zum Wegfall oder zur Reduktion allfälliger Schadenersatzansprüche führen[5].
- Die Hersteller von sicherheitsrelevanten IT-Produkten haben ihren Sitz oft im Ausland. Die Rechtslage wird dadurch komplizierter. Zudem ist die Durchsetzung von Ansprüchen im Ausland mit praktischen Schwierigkeiten verbunden.
- Im Fall von Mängeln an Individualsoftware hat der Betreiber ein besonderes Interesse an einer einvernehmlichen Lösung, weil aus tatsächlichen und rechtlichen Gründen oft kaum die Möglichkeit besteht, Änderungen selbst oder durch Dritte vorzunehmen[6].
- Gerichtliche Auseinandersetzungen über IT-Sicherheitslücken können für die Geschädigten zu Imageverlusten führen, z.B. Publizität über Sicherheitslücken im E-Banking.
- Komplexe technische Vorgänge sind für Richter als Nichtinformatiker nur schwer zu verstehen. Das Recht verlangt auch in nuancenreichen und unsicheren Sachverhalten mitunter «Entweder-oder-Entscheidungen». In welche Richtung diese ausfallen werden, ist in Bereichen, in de-

Kurz und bündig

Wer für Schäden haftet, die durch ungenügende IT-Sicherheit hervorgerufen werden, ist aufgrund der komplexen Herstellungs- und Verantwortlichkeitsstrukturen oft schwer zu beurteilen. Die Tatsache, dass es im In- und Ausland bisher kaum zu gerichtlichen Auseinandersetzungen gekommen ist, darf aber nicht über die potenzielle Bedeutung dieser Fragen hinwegtäuschen. Mitunter zeigen erst Systemausfälle, die zu komplizierten Reflexschäden führen, welche Abhängigkeiten von bestimmten Komponenten der IT-Infrastruktur bestehen. Um rechtliche Unsicherheiten zu minimieren, empfiehlt es sich deshalb, ein Inventar der gegenseitigen Abhängigkeiten innerhalb und ausserhalb des Unternehmens zu erstellen und das eigene Haftungspotenzial gegenüber Lieferanten und Kunden einer sorgfältigen vertraglichen Kontrolle und Planung zu unterziehen.

nen Präjudizien weitgehend fehlen, oft kaum vorhersehbar.

■ Jeder Prozess ist mit Kostenrisiken verbunden. Wird er gewonnen, erhält der Kläger bestenfalls Ersatz des Schadens und der Anwalts- und Gerichtskosten. Im Fall des Unterliegens muss er hingegen die Verteidigungskosten der Gegenpartei übernehmen.

Angesichts dieser rechtlichen und tatsächlichen Unsicherheitsfaktoren verzichten die Geschädigten meist darauf, Schäden im Zusammenhang mit unzureichender IT-Sicherheit überhaupt gerichtlich geltend zu machen. In der Schweiz gibt es daher bisher praktisch keine und in der EU nur wenige Gerichtsentscheidungen im Zusammenhang mit ungenügender IT-Sicherheit.

Handlungsbedarf

Die Tatsache, dass es bisher kaum zu gerichtlichen Auseinandersetzungen in Zusammenhang mit Störungen und Ausfällen von Informationssystemen gekommen ist, darf nicht über die potenzielle Bedeutung dieser Fragen hinwegtäuschen. Selbst ein relativ kurzer Ausfall grösserer Informations- und Kommunikationssysteme (z.B. das Rechenzentrum einer Grossbank), könnte aufgrund der umfassenden Vernetzung weitreichende Auswirkungen haben und kaskadenartig Haftungsrisiken von gesamtwirtschaftlicher Bedeutung auslösen. Im Zusammenhang mit der Jahr-2000-Problematik wurde daher erstmals die Frage aufgeworfen, ob das geltende Recht überhaupt angemessene Antworten auf solche Fragen ermöglicht.

Im schweizerischen Recht beschränkt sich die juristische Diskussion bisher weitgehend auf die vertragliche[7] und ausservertragliche[8] Haftung für Softwarefehler und die Sicherheitsanforderungen des Datenschutzrechts. In Deutschland begannen sich die Juristen bereits in der zweiten Hälfte der 80er Jahre mit der Haftung für Mängel von Computerprogrammen auseinanderzusetzen. Das Schwergewicht der Diskussion liegt auch hier auf den vertragsrechtlichen Folgen von Softwaremängeln[9] und der ausservertraglichen Haftung[10] für Körper- und Sachschäden durch mangelhafte IT-Systeme. International diskutiert wird zudem die strafrechtliche Qualifikation von Angriffen auf IT-Systeme.

Viele rechtliche Aspekte ungenügender IT-Sicherheit bleiben vorläufig ungeklärt. So beispielsweise Bestand und Umfang von Produktebeobachtungs- und Informationspflichten bei nachträglichem Auftreten von Sicherheitslücken, die Pflichten von Verwaltungsräten und Revisoren im Zusammenhang mit der Informationssicherheit oder die Frage inwieweit spezielle Sicherheitsprodukte Lücken in den übrigen Komponenten eines Informationssystems kompensieren müssen. Um die Rechtssicherheit zu erhöhen, wäre auf nationaler und internationaler Ebene eine vermehrte politische und wissenschaftliche Auseinandersetzung mit solchen Themen notwendig. Auf Unternehmensebene dürfte sich eine systematische Analyse und Planung der Haftungsrisiken in Verträgen mit Lieferanten und Kunden längerfristig in jedem Fall auszahlen. ■

Fussnoten und Links

1 Der Begriff der Haftung wird vorliegend in einem weiten Sinn verstanden, sodass er auch vertragliche Schadenersatzforderungen und gesellschaftsrechtliche Verantwortlichkeitsansprüche mit einschliesst.

2 Vgl. Art. 7 Abs. 1 DSG und Art. 21 StGB.

3 Vgl. z.B. Art. 47 BankenG.

4 Vgl. Art. 143, 143bis und 144bis StGB.

5 Vgl. Art. 44 OR.

6 Vgl. dazu WOLFGANG STRAUB, Der Sourcecode von Computerprogrammen im schweizerischen Recht und der EU-Richtlinie über den Rechtsschutz von Computerprogrammen, UFITA 2001 III, 807 ff.

7 Vgl. zur vertraglichen Haftung für mangelhafte Software URSULA WIDMER, Risikofolgeverteilung bei Informatikprojekten: Haftung für Softwaremängel bei Planung und Realisierung von Informationssystemen, Diss. Bern 1989, LUKAS MORSCHER, Gewährleistung und Haftung bei der Software-Überlassung, SZW 1999, 61 ff., HEINRICH HONSELL, Standardsoftware- und Sachmängelhaftung, in: Festschrift zum 65. Geburtstag von Mario M. Pedrazzini, Bern 1990, 313 ff. und MARKUS ZÜST, Vertragshaftung für Soft-ware, in: Software-Schutz Software-Haftung, Zürich 1992, 69 ff.

8 Vgl. zur ausservertraglichen Haftung für Mängel an IT-Produkten WOLFGANG STRAUB, Produktehaftung für Informationstechnologiefehler, Zürich 2002, und ROLAND BÜHLER, Produktehaftung für Software, in: Software-Schutz Software-Haftung, Zürich 1992, 92 ff.

9 Vgl. dazu insbesondere ROLAND BÖMER, Risikozuweisung für unvermeidbare Softwarefehler, CR 1989, 361 ff., PETER GORNY / WOLFGANG KILIAN Computer-Software und Sachmängelhaftung, Stuttgart 1985, BENNO HEUSSEN, Technische und rechtliche Besonderheiten von Mängeln bei Computerleistungen, CR 1988, 894 ff. und 986 ff., WOLFGANG KILIAN, Haftung für Mängel der Computer-Software, Heidelberg 1986, und HELMUT REDEKER, Der Rechtsbegriff des Mangels beim Erwerb von Software, CR 1993, 193 ff.

10 Vgl. zur ausservertraglichen Haftung für Softwaremängel in Deutschland insbesondere JÜRGEN TAEGER, Ausservertragliche Haftung für fehlerhafte Computerprogramme, Tübingen 1995, ANDREAS GÜNTHER, Produkthaftung für Informationsgüter; Verlagserzeugnisse, Software und Multimedia im deutschen und US-amerikanischen Produkthaftungsrecht, Köln 2001, zugl. Diss. München 2000, und MICHAEL LEHMANN, Produzenten- und Produkthaftung für Soft- und Hardware, in: Michael Lehmann (Hrsg.), Rechtsschutz und Verwertung von Computerprogrammen, 2. A., Köln 1993, 999 ff.