Dr. iur. Wolfgang Straub

Die Verantwortung von IT-Anbietern und Anwendern für Informationssicherheit

Bei Störungen in IT-Systemen stellt sich regelmässig die Frage, ob die Sicherheitsvorkehrungen ausreichend waren bzw. wer die Verantwortung dafür trägt. Die Fachgruppe Security der Schweizer Informatikergesellschaft hat im Rahmen einer Tagung nach Antworten zu diesen in der Schweiz bisher noch kaum diskutierten Fragen gesucht.

Ungenügende Informationssicherheit – ein Rechtsproblem?

[Rz 1] Sicherheitslücken in Informationssystemen können insbesondere Datenverlust, Leistungsausfall oder unerwünschte Systemreaktionen verursachen. Dadurch entstehen Wiederherstellungskosten, Produktionsausfall und Ansprüche wegen Lieferungsverzögerung, eventuell sogar Sach- und Personenschäden (z. B. Körperverletzungen bei Fehlsteuerung von Fertigungsrobotern oder Brände bei Ausfall von Temperatursteuerungen). Durch solche Vorfälle können verschiedene Arten von Schadenersatzansprüchen entstehen:

- **Gewährleistungs- und Schadenersatzansprüche der Betreiber** eines Informationssystems gegenüber den für Konzeption, Herstellung und Wartung verantwortlichen Unternehmen (z.B. Hard- und Softwarehersteller, Outsourcingpartner).
- **Ansprüche von Kunden der Betreiber** für mangelhafte oder verspätete Leistungserbringung (z.B. Bankkunden gegenüber Bank bei Verspätungen im E-Banking)
- **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 der Informationssicherheit.

[Rz 2] Ungenügende Sicherheit von Informationssystemen wirft zudem Fragen in **weiteren Rechtsgebieten** auf:

- **Verletzung des Datenschutzrechts,** wenn Personendaten wegen Sicherheitslücken von Unbefugten eingesehen werden können (vgl. Art. 7 Abs. 1 DSG).
- **Verletzung öffentlichrechtlicher Vorschriften**, wenn Systeme nicht den vorgeschriebenen Sicherheitsanforderungen entsprechen oder Berufsgeheimnisse nicht ausreichend geschützt werden (vgl. z.B. Art. 47 BankG).
- **Strafrechtliche Konsequenzen** gegenüber Dritten, welche unbefugt in IT-Systeme eindringen oder Störungen verursachen (vgl. Art. 143, 143bis und 144bis StGB).

Warum rechtliche Auseinandersetzungen selten sind

[Rz 3] Trotz der verschiedenen Anspruchsgrundlagen ist es in der Schweiz und der EU bisher kaum je zu Haftungsprozessen gekommen. Das hängt insbesondere mit folgenden Ursachen zusammen:

- Schäden entstehen im IT-Bereich oft durch ein komplexes Zusammenwirken verschiedener Faktoren. Dies wird etwa am Beispiel zweier unverträglicher Applikationen deutlich, welche alle paar Wochen bei einem bestimmten Backupstatus zum Absturz führen. Wer in einem derartigen Fall einen der involvierten Softwarehersteller belangen will, muss **beweisen**, dass die Schadensursache in dessen

Verantwortungsbereich lag.

- Allfällige Schadenersatzansprüche sind aufgrund vertraglicher Haftungsausschlüsse, Verjährung oder nicht rechtzeitiger Rüge der Sicherheitsmängel oft nicht mehr **durchsetzbar**.

- Bei IT-Sicherheitslücken stellt sich regelmässig die Frage nach der **Eigenverantwortung** der Betreiber des betreffenden Systems bzw. ihrer Systemadministratoren. Bei Datenschäden muss z.B. geprüft werden, ob der Geschädigte eine angemessene Datensicherung hatte, bei Produktionsausfällen, ob geeignete Massnahmen zu Disaster Recovery/Business Continuity Planning durchgeführt wurden. Ein Selbstverschulden des Geschädigten kann zum Wegfall oder zur Reduktion allfälliger Schadenersatzansprüche führen (vgl. Art. 44 Abs. 1 OR).

- Im Fall von Sicherheitslücken bei **Individualsoftware, integrierten Systemen und Outsourcingleistungen** hat der Betreiber ein besonderes Interesse an einer einvernehmlichen Lösung, weil hier oft ein faktisches Abhängigkeitsverhältnis vom IT-Anbieter besteht.

- Gerichtliche Auseinandersetzungen über IT-Sicherheitslücken können für die Geschädigten zu **Imageverlusten** führen (z.B. Publizität über Sicherheitslücken im E-Banking).

- Das Schadenersatzrecht ist über Jahrhunderte gewachsen. Die **Einordnung von informatiktypischen Sachverhalten** in dieses System wirft einige neue Fragen auf, für welche es noch keine Präjudizien gibt (z.B. ob Datenverlust einer Sachbeschädigung gleichzustellen ist).

- Komplexe technische Vorgänge sind für Richter als Nichtinformatiker schwierig zu verstehen. Das Recht verlangt auch in nuancenreichen und unsicheren Sachverhalten mitunter ‚Entweder-oder-Entscheidungen'. In welche Richtung diese ausfallen werden, ist 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.

[Rz 4] Angesichts dieser rechtlichen und tatsächlichen Unsicherheitsfaktoren verzichten die Geschädigten meist darauf, Schäden im Zusammenhang mit unzureichender IT-Sicherheit überhaupt geltend zu machen.

Warum juristische Überlegungen trotzdem nötig sind

[Rz 5] Die Tatsache, dass es bisher kaum zu gerichtlichen Auseinandersetzungen in Zusammenhang mit Störungen und Ausfällen von Informationssystemen gekommen ist, darf nicht über die potentielle **Bedeutung** dieser Fragen hinwegtäuschen (vgl. dazu Wolfgang Straub, Zur Haftung für Informationstechnologiefehler, in: Jusletter 20. August 2001). Selbst ein relativ kurzer Ausfall grösserer Informations- und Kommunikationssysteme (z.B. das Rechenzentrum einer Grossbank) könnte aufgrund der weitreichenden Vernetzung überraschende Auswirkungen haben und kaskadenartige Haftungsrisiken von gesamtwirtschaftlicher Bedeutung auslösen. Im Zusammenhang mit dem Jahr-2000-Problem wurde daher die Frage aufgeworfen, ob das geltende Recht überhaupt angemessene Antworten für solche Fälle ermöglicht.

Ergebnisse der Tagung der Fachgruppe Security vom 4.6.2003

[Rz 6] Die Fachgruppe Security der Schweizer Informatikergesellschaft befasst sich seit einiger Zeit auch mit den rechtlichen Aspekten der Informationssicherheit. In ihrem Auftrag habe ich zusammen mit Fürsprecher Beat Lehmann (Alcan Holdings) und Prof. Dr. Bernhard Hämmerli (HTA Luzern) am 4. Juni 2003 in Zürich eine **Tagung zur Verantwortung von IT-Herstellern und Dienstleistern für Informationssicherheit** organisiert. Es handelte sich um die bisher erste Veranstaltung zu diesem Thema in der Schweiz. Die Tagungsunterlagen sind unter http://www.fgsec.ch/events/ft2003.06/ publiziert.

[Rz 7] In seinem Eröffnungsreferat stellte Prof. Dr. Rolf H. Weber (Universität Zürich) die Thematik in den breiteren Zusammenhang der **Verantwortung des Unternehmens für sichere Informationsverarbeitung**. Dabei wies er insbesondere auf die Bedeutung eines umfassenden ICT-Konzepts hin. Die Verantwortung von

IT-Dienstleistern und die Versicherbarkeit von IT-Risiken werden im Herbst an einer Tagung des Zentrum für Informations- und Kommunikationsrecht und des Schweizer Forums für Kommunikationsrecht weiter vertieft.

[Rz 8] Prof. Dr. Peter Gauch (Universität Freiburg) befasste sich zunächst mit der rechtlichen Einordnung von IT-Verträgen und mit den **vertraglichen Gewährleistungs- und Schadenersatzmodalitäten**. Er wies auf die Unterschiede zwischen dem technischen und dem vertraglichen Mängelbegriff hin und setzte sich mit dem vielschichtigen Begriff der ‚Garantie' in IT-Verträgen auseinander.

[Rz 9] In meinem eigenen Referat ging es um die **ausservertraglichen Haftung von IT-Anbietern** (Produktehaftungsgesetz, Haftung aus unerlaubter Handlung und ausservertragliche Haftung des Unternehmens). Derartige Ansprüche haben vor allem bei Sach- und Personenschäden praktische Bedeutung, wenn zwischen Schadensverursacher und Geschädigtem kein Vertragsverhältnis besteht oder die Ansprüche bereits erloschen sind (z.B. bei Fehlsteuerung von medizinischen Geräten, Verkehrssystemen oder Produktionsanlagen). Eine erweiterte Fassung dieses Referates ist unter http://www.fgsec.ch/events/ft2003.06/UnterlagenStraub.pdf verfügbar.

[Rz 10] Das Referat von Prof. Dr. Thomas Hoeren (Universität Münster) beschäftigte sich mit der **Verantwortung für Informationssicherheit in der EU**. Er stellte in prägnanter Form die verschiedenen Haftungsgrundlagen des deutschen Rechts dar und erläuterte, warum Haftungsfälle in der bisherigen Gerichtspraxis selten sind. Dies hängt insbesondere damit zusammen, dass Haftungsansprüche oft an Schadensvermeidungspflichten der Anwender scheitern (z. B. Datensicherung und Disaster Recovery Planning).

[Rz 11] Prof. Dr. Bernhard Hämmerli (HTA Luzern) setzte sich aus Ingenieursicht mit dem **Begriff der Informationssicherheit** auseinander und zeigte auf, dass die Sicherheitsanforderungen an ein Gesamtsystem umfassender sind als die Summe der Anforderungen an seine Einzelteile.

[Rz 12] Der stellvertretende Delegierte des Bundesrates für Informatikstrategie, Peter Trachsel, erläuterte den **Stellenwert der Informationssicherheit in den Projekten des Bundes** (Strategie, Organisation und Verfahren). Sein Referat machte deutlich, wie anspruchsvoll die Definition der notwendigen Sicherheitselemente bei der Ausschreibung von IT-Projekten ist.

Organisatorische und vertragliche Möglichkeiten

[Rz 13] In verschiedenen parallelen Foren diskutierten erfahrene IT-Manager und Unternehmensjuristen unter der Moderation von David Rosenthal, Dr. Peter K. Neuenschwander und mir über die **organisatorischen Möglichkeiten** zur Verringerung von Sicherheitsrisiken in IT-Projekten, die vertraglichen Instrumente der **Risikoüberwälzung** auf Vertragspartner und die **Versicherbarkeit** von Haftungsrisiken aus IT-Projekten (vgl. dazu auch die ‚pistes de réflexion' zur Haftung von IT-Herstellern unter http://www.fgsec.ch/events/ft2003.06/PistesDeReflexionForum1.pdf).

[Rz 14] Da Informationssicherheit nicht nur spezielle Sicherheitsfeatures sondern auch Verfügbarkeit und zuverlässiges Funktionieren von Informationssystemen umfasst, ist eine präzise **Definition** der zu erbringenden Leistung und der Abnahme- und Gewährleistungsmodalitäten elementar. Pflichtenhefte und Service Level Agreements sind allerdings auch bei sorgfältiger Redaktion nie vollständig und müssen bei länger dauernden Projekten immer wieder aktualisiert werden. Dem sollte durch Implementierung eines mehrstufigen **Verfahrens zur Anpassung und Konkretisierung des Vertrages** begegnet werden. Ein hohes Sicherheitsniveau kann von IT-Anbieter und Besteller nur gemeinsam erreicht werden. Die Mitwirkungs- und Informationspflichten beider Parteien sollten im Rahmen eines Claim Management Verfahrens regelmässig thematisiert werden. Die Verantwortung für Informationssicherheit von IT-Produkten und IT-Dienstleistungen Iässt sich jedenfalls erst in letzter Linie auf der Ebene von **Haftungsbeschränkungsklauseln** regeln.

[Rz 15] Im Versicherungspanel wurde deutlich, dass die **Versicherung von IT-Herstellern und Dienstleistern** in der Schweiz noch relativ wenig verbreitet ist und eine intensive Zusammenarbeit zwischen Versicherer und Versicherungsnehmer bei der Risikoanalyse erfordert.

[Rz 16] In der anschliessenden Podiumsdiskussion unter der Leitung von Prof. Dr. Fridolin Walther (Universität Bern) wurden die Ergebnisse der einzelnen Foren zusammengefasst und die Frage aufgeworfen, ob es für neue

Technologien tatsächlich **neue Haftungsgrundsätze** braucht.

Fazit

[Rz 17] Viele rechtliche Aspekte ungenügender IT-Sicherheit bleiben nach wie vor ungeklärt. So z. B. Frage, inwieweit spezielle Sicherheitsprodukte Lücken in den übrigen Komponenten eines Informationssystems kompensieren müssen, Bestand und Umfang von Produktebeobachtungs- und Informationspflichten bei nachträglichem Auftreten von Sicherheitslücken oder die Einordnung und Quantifizierung von Datenschäden. 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 auszahlen.

Dr. Wolfgang Straub, LL.M., ist Rechtsanwalt in Bern und Lehrbeauftragter am Departement Informatik der Universität Fribourg. E-Mail: wolfgang.straub@advobern.ch

Rechtsgebiet	Internet und Recht
Erschienen in	Jusletter 16. Juni 2003
Zitiervorschlag	Wolfgang Straub, Die Verantwortung von IT-Anbietern und Anwendern für Informationssicherheit, in: Jusletter 16. Juni 2003 [Rz]
Internetadresse	http://www.weblaw.ch/jusletter/Artikel.jsp?ArticleNr=2463