IT-Dienstleistungen im Spannungsfeld zwischen Vertragsgestaltung, Risiko und Versicherbarkeit

Tagung des Schweizer Forum für Kommunikationsrecht (SF•), der swiss interactive media and software association (simsa) und des Zentrum für Informations- und Kommunikationsrecht der Universität Zürich (ZIK) vom 1. Oktober 2003

JEAN-PHILIPPE KLEIN*

Das Schweizer Forum für Kommunikationsrecht (SF•FS), die swiss interactive media and software association (simsa) und das Zentrum für Informations- und Kommunikationsrecht der Universität Zürich (ZIK) haben im Rahmen der Veranstaltungsreihe ICT: Rechtspraxis[1] eine weitere Veranstaltung zu Fragen im IT-Bereich durchgeführt[2]. Die Tagung wandte sich dem weiten Bereich der IT-Dienstleistung zu und sollte insbesondere deren Risikofaktoren und deren Optimierung, aber auch deren Versicherbarkeit aufzeigen.

Als Referenten zu den einzelnen Themenbereichen waren ausgewiesene Experten geladen: Zu den rechtlichen Grundlagen der Haftung für IT-Dienstleistungen sprach Prof. Dr. Ernst A. Kramer (Universität Basel). Dr. Robert G. Briner (Rechtsanwalt, Zürich) erläuterte die Möglichkeiten der Risikooptimierung durch angemessene Vertragsgestaltung. Die Verbesserungsmöglichkeiten durch Einhaltung von Standards wurden von Prof. Dr. Rolf H. Weber (Universität Zürich) aufgezeigt, die konkrete Vorgehensweise beim Risk Assessment erläuterte Kristian Bader (Arthur D. Little, Zürich). Peter Duschinger (Oberhänsli & Partner AG, Thalwil) und Dr. Helmut Steigele (Cascade IT, Zürich) stellten die Probleme bei der Versicherbarkeit der mit IT-Dienstleistungen verbundenen Risiken dar. Die Veranstaltung leitete Dr. Mathis Berger (Rechtsanwalt, Zürich).

I. Einleitung

IT–Dienstleistungen sind aus dem modernen Alltag nicht mehr wegzudenken; bald jedes Unternehmen ist heute von Informationstechnologie in irgendeiner Form abhängig, Ausfälle von Systemen ziehen deshalb regelmässig schwerwiegende Konsequenzen mit sich. Man denke etwa an den Ausfall eines Broker-Systems eine halbe Stunde vor Börsenschluss. Dieses «Horror-Szenario» wünschen sich weder der Dienstleistungsanbieter noch der Kunde. Möglicherweise hätte es aber nicht soweit kommen müssen. Besonders wichtig sind deshalb vorbeugende Massnahmen zur Optimierung von Informationssicherheit, etwa im Verfahren eines Risk Assessments (dazu u. III/1). Der Dienstleistungserbringer kann sich auch nach einer der bestehenden internationalen Qualitätsnormen (Standards) zertifizieren lassen; damit kontrolliert sich der Anbieter selbst und kann dem Kunden darlegen, dass Vertraulichkeit, Sicherheit und Verfügbarkeit seiner Dienstleistung stets gewährleistet sind (dazu u. III/3).

Ist der Schaden jedoch eingetreten, stellt sich die Frage nach der Haftung. Wofür hat der Anbieter einzustehen? Hier zeigt sich, ob die Parteien bei Vertragsschluss die jeweiligen Pflichten präzise genug festgelegt haben (dazu u. III/2). Hat der Dienstleister seine Haftung nicht gültig eingeschränkt (dazu u. II/2), wird für ihn die Frage brisant, ob er über eine ausreichende Versicherungsdeckung verfügt (u. III/4).

Die Ergebnisse der Tagung werden hier in Form einer Gesamtschau von Problemen und Lösungsansätzen dargestellt.

---

[1] ICT = Information and Communication Technology.

[2] Die Veranstaltung fand am 1. Oktober im Hotel Widder (Zürich) statt. Die Ergebnisse der letzten Tagung zum Thema IT-Outsourcing sind in einem vertiefenden Sammelband veröffentlicht worden: Hg. Rolf H. Weber/Mathis Berger/Rolf auf der Maur, IT-Outsourcing, ICT: Rechtspraxis I, Zürich 2003.

II. Die rechtlichen Grundlagen der Haftung für IT-Dienstleistungen

1. Innominatcharakter von IT-Dienstleistungsverträgen

Betrachtet man die Vielfalt von möglichen IT-Dienstleistungen, mag man nicht erstaunt sein, dass die Variationsbreite von IT-Vertragstypen ins Unübersichtliche angewachsen ist und dass es auch «den» IT-Dienstleistungsvertrag als solchen nicht geben kann.

Bei der Qualifikation ist zunächst zu beachten, dass nicht alle IT-Verträge Dienstleistungsverträge darstellen: so ist etwa das Zurverfügungstellen eines Speicherplatzes auf einem Server – der sog. Website-Hosting-Vertrag – als reiner Überlassungsvertrag zu qualifizieren. Zum anderen umfassen Verträge auf IT-Dienstleistungen zumeist verschiedene Leistungspflichten, neben auftragsrechtlichen und werkvertraglichen Elementen kommen etwa auch kaufvertragliche oder gesellschaftsrechtliche Elemente zu stehen. Als Beispiel eines solchen komplexen Vertrags sei der sog. Systemintegra-tionsvertrag erwähnt: Er umfasst die Planung, Realisierung und Einführung eines Informatiksystems. Der Generalunternehmer übernimmt dabei gegen Bezahlung Leistungen wie Lieferung von Hardware, Lizenzierung, Erstellung, Installation und Integration von Software, aber auch Einführung des Systems und Schulung[3]. Solche Verträge lassen sich in aller Regel nicht auf den Nenner eines im Gesetz vorgesehenen Vertrags beziehen, zumeist wird es sich beim IT-Dienstleistungsvertrag daher um einen sog. Innominatvertrag handeln.

2. Die Haftungsnormen insbesondere

Bei Innominatverträgen kommt dem durch die Parteien vorgesehenen Haftungsregime, dem sog. Risk Management, naturgemäss eine besondere Bedeutung zu. Prof. E. A. Kramer sprach in diesem Zusammenhang von eigentlichen «Sicherheitsarchitekturen» im Hinblick auf vertragsrelevante Schadens- und Haftungsrisiken.

Solches Risk Management steht aber nicht im rechtsfreien Raum. Ist das Haftungsregime lückenhaft oder erscheint es kontrollbedürftig, sind allenfalls Bestimmungen des besonderen Teils analog heranzuziehen. Vor allem aber sind die Haftungsbestimmungen des Allgemeinen Teils des OR auch auf Innominatkontrakte anwendbar, was insbesondere im Hinblick auf die Grenzen der Haftungsfreizeichnung von grösster praktischer Bedeutung ist.

Aber nicht nur die Freizeichnung wirft Fragen auf: Haftung setzt regelmässig eine Pflichtverletzung voraus. Wann eine solche anzunehmen ist, lässt sich indes angesichts der Komplexität der Leistungspflichten oft nicht leicht beantworten. Zentrale Funktion kommt hier einerseits dem konkreten Vertrag zu (u. III/2), hilfreich können andererseits auch privatautonom entwickelte Industrie-Standards (dazu u. III/3) sein. Das sicherste Instrument bleibt aber für die Parteien, in ihrem Vertrag ein eigentliches Pflichtenheft – sowohl für den Leistungsanbieter wie für den Kunden (!), etwa zur Datensicherung beim Outsourcing – vorzusehen. Solche Service Level Agreements regeln dann etwa Fragen zur Verfügbarkeit von IT-Systemen, das Vorgehen bei Störungen (z.B. die Einrichtung eines Help Desk-Diensts) oder maximale Reparaturzeiten. Im Übrigen gilt die objektivierte redliche Publikumserwartung als Massstab. Gegebenenfalls hat der Dienstleister auch Spezialisten beizuziehen.

Verletzt der Anbieter eine Vertragspflicht, haftet er grundsätzlich für den daraus resultierenden Schaden, sofern er sich nicht exkulpieren kann (Art. 97 OR). Andererseits ist der Kunde oftmals nicht in der Lage, einen konkreten Schaden nachzuweisen: hier empfiehlt sich für die Parteien die Vereinbarung einer Konventionalstrafe oder eines Bonus-Malus-Systems.

Will sich der Anbieter durch eine Haftungsfreizeichnung oder -beschränkung vor Ansprüchen seines Kunden schützen, so kann er dies nur für leichte Fahrlässigkeit tun: hier gelten die Grenzen von Art. 100 Abs. 1 OR. Die völlige Freizeichnung von der Haftung für Hilfspersonen ist zwar nach Art. 100 Abs. 2 zulässig, ist aber bei pauschalem Haftungsausschluss, jedenfalls bei AGB, nach der «Unklarheitenregel» nicht zu vermuten. Prof. Kramer verwies hier auf die Haftungsbestimmung des

[3] Präambel des SWICO/SVD-Systemintegrations-Mustervertrags, dazu sogleich Fn. 4 und 5.

SWICO/SVD-Systemintegrations-Mustervertrags[4]. Enthält der Vertrag Garantiezusagen, sind Haftungsfreizeichnungen im zugesicherten Bereich nicht gültig.

Zu Diskussion Anlass gab die für die Dienstleistungserbringer zentrale Frage, ob eine vertragliche Beschränkung der Verfügbarkeit von Systemleistungen – häufig findet sich etwa eine Beschränkung auf 99,97% – nicht zugleich ein (verkappter) pauschaler Haftungsausschluss im Umfang von 0,03% darstellt, der den Grenzen von Art. 100 OR unterliegen würde. Dies hätte die Konsequenz, dass jedenfalls bei grober Fahrlässigkeit der Dienstleistungserbringer auch für einen Systemausfall im besagten Umfang einzustehen hätte.

Wohl ist hier zu differenzieren: Haben die Parteien eine Verfügbarkeits-Toleranzgrenze ausdrücklich vereinbart, sollte von einer Einschränkung der Leistungspflicht ausgegangen werden. Wurde die Beschränkung hingegen einseitig aufgestellt, ist sie anhand der für den Einbezug von AGB entwickelten Kriterien zu überprüfen; hier wird alles davon abhängen, ob eine Einschränkung der Verfügbarkeit vom Kunden überhaupt und gegebenenfalls in welchem Umfang vernünftigerweise hingenommen werden muss. Es wurde in der Diskussion darauf hingewiesen, dass kein System immer verfügbar ist und dass mit minimalen Ausfällen jedenfalls zu rechnen sei. Ist generell mit Ausfällen in minimalem Ausmass zu rechnen, wird man eine solche Klausel nicht allgemein als ungewöhnlich bezeichnen können. Es stellt sich aber weiterhin die Frage, wie der Kunde die Klausel verstehen durfte und musste: als Einschränkung der Leistungspflicht oder als Freizeichnung? Ist die Formulierung nicht eindeutig als Leistungsbeschränkung zu verstehen, wird man nach der Regel «in dubio contra stipulatorem» von einer Freizeichnung ausgehen, da diese für den Kunden günstiger ist. Die so verstandene Klausel unterliegt dann nämlich den Grenzen von Art. 100/101 OR (sog. Inhaltskontrolle).

In allen Fällen dürfte die Grenze der Leistungspflichtbeschränkung jedoch bei einer vertragstypenwidrigen Einschränkung (etwa Beschränkung der Verfügbarkeit der Systemleistung auf 60%) liegen, denn sorgfältige Leistungserbringung ist auf jeden Fall geschuldet. Wird die Leistungspflicht über das vertragstypische hinaus eingeschränkt, liegt darin eine Umgehung der (zwingenden) Haftungsbestimmungen.

Angesichts dieser doch starken Unsicherheit einerseits im Pflichtenumfang der Parteien, andererseits im Ausmass der Konsequenzen bei Fehlleistungen, lohnt es sich, beim Abschluss von IT-Dienstleistungsverträgen über Massnahmen zur Schadensverhinderung oder zumindest deren Begrenzung nachzudenken.

III. Verbesserungs- bzw. Lösungsansätze

Eine wirksame Prävention verhindert nicht nur konkreten Schaden, sondern auch Imageverlust, der sich in mangelnden künftigen Einnahmen niederschlägt, die den Anbieter auf lange Zeit hinaus gegenüber seinen Konkurrenten benachteiligen können.

1. Risk Assessment

Eine wirksame Präventionsmöglichkeit bietet das Risk Assessment, sofern nicht erst im Katastrophenfall eingeschritten wird (sog. «Herdplatten-Effekt»). Ziel eines solchen Risikoprofils ist es, die Schwachstellen des Dienstleisters (sog. Risk Areas), die in den unterschiedlichsten Bereichen liegen können – etwa Ausgestaltung der Verträge mit Kunden und anderen Dienstleistern, Kompetenzfragen auf Führungsebene, Schutz der für die Dienstleistung zentralen Einrichtungen, elektrische Versorgung – aufzudecken, diese zu analysieren und geeignete Strategien zu deren Ausschaltung oder zumindest Verminderung zu entwickeln. Mit dem Risk Assessment wird ein eigentliches «Röntgenbild» des Unternehmens erstellt.

Kristian Bader präsentierte anhand eines konkreten Falls das Vorgehen beim Erstellen eines solchen Risikoprofils. Die Erstellung des Assessments kann sich über Monate erstrecken. In zahlreichen Fällen lassen sich aber einzelne Risiken leicht erkennen und praktisch zeitgleich vermindern (sog. Quick Wins). Andere Risiken bedürfen eines aufwändigeren Massnahmenkonzepts: Im referierten Beispiel

[4] SWICO = Schweizerischer Wirtschaftsverband der Informations-, Kommunikations- und Organisationstechnik; SVD = Schweizerische Vereinigung für Datenverarbeitung. Die Bestimmung (Teil IV, P.3) lautet: «Die Haftung für leichte Fahrlässigkeit wird ausdrücklich wegbedungen. Für Leistungen von Erfüllungsgehilfen haften beide Vertragspartner wie für eigene.» Die Haftung des Kunden bezieht sich dabei in erster Linie auf eine etwaige Verletzung von Mitwirkungspflichten.

wurde in der Endphase ein Implementierungsplan erstellt, dessen Realisierung fast zwei Jahre beanspruchte.

Betont wurde besonders der Faktor Kommunikation. Sowohl die Projektleitung wie auch der «Kunde» müssen gegenseitiges Vertrauen aufbringen und zum Gelingen des Assessments die nötigen Informationen zur Verfügung stellen. In komplexen Fällen werden externe Experten beigezogen, im referierten Fall Tochtergesellschaften und Partner, dies mit doppelter Wirkung: Einerseits wird dadurch die Professionalität der Untersuchung gewährleistet, andererseits wird es für den Kunden schwieriger, allenfalls durch Desinformation auf die Resultate des Assessments einzuwirken.

2. Angemessene Vertragsgestaltung

Wie eben zum Risk Assessment erwähnt wurde, liegt ein wesentlicher Aspekt der Beziehung zwischen Dienstleistungserbringer und Kunde in der sorgfältigen Vertragsausarbeitung. Angesichts der grundsätzlichen Vertragsinhaltsfreiheit lohnt es sich, die Spielräume des dispositiven Gesetzesrechts vollständig auszuloten. Die analog anwendbaren Regelungen des Werkvertrags – etwa bei Erstellung von Individualsoftware – oder auch des Auftragsrechts sind ungenügend und entsprechen auch nicht immer den Parteiinteressen[5]: Der Kunde will im Problemfall nicht «Geld statt Software» und ist möglicherweise auch bereit, für eine mängelfreie Dienstleistung mehr zu bezahlen als ursprünglich vorgesehen. Der Projektleiter seinerseits fürchtet sich vor Imageverlusten infolge gescheiterter Projekte und wird alles daran setzen, seinen Kunden zufrieden zu stellen. Umso wichtiger ist es für die Parteien, etwa bezüglich der Mängelbehebung oder der Entlöhnung, besondere Regelungen vorzu-sehen. In diese Richtung weisen auch Vereinbarungen zur Streitbeilegung. Die relative Seltenheit der Gerichtsentscheide im IT-Dienstleistungsbereich erklärt sich aus dem Interesse beider Parteien an einer raschen und diskreten Klärung von Differenzen, aber wohl auch aus den Anforderungen, die in solchen Fällen an die Gerichte gestellt werden.

Dr. Briner wies besonders auf typische IT-Risikobereiche hin, die jedenfalls eine angemessene Regelung erfahren sollten: Projektleiter müssen ausgewechselt werden können; allzu oft treten während eines Projekts personelle Inkompatibilitäten zu Tage. Die Mitwirkungspflichten auch des Kunden müssen detailliert spezifiziert werden. In aller Regel wird sich der Anbieter ein Wartungsrecht ausbedingen. Umgekehrt müssen die Parteien vorsehen, inwiefern der Kunde zur Abnahme von Updates verpflichtet ist und wie lange der Dienstleister noch ältere Versionen zu warten hat (Release-Zwang). Besonders wichtig sind das Change Management (Vorkehrungen zur Abänderung des Vertrags bei neuen Gegebenheiten) und die periodische Qualitätsüberprüfung. Zu erwähnen ist schliesslich die Bedeutung einer vollständigen Dokumentation im Streitfall.

3. Einhaltung von Standards und Zertifizierung von Informationssicherheit

Standards sind privatautonom angelegte Regelwerke, die in unternehmerische Abläufe derart integriert werden sollen, dass der Anbieter die für den reibungslosen Betrieb erforderliche Informationssicherheit gewährleisten und auch messen kann (Qualitätsnormen). Dabei werden zwei Arten von Standards unterschieden: solche, die nur Verhaltensregeln aufzeigen (Code of Practice) und solche, die eigentliche Kontrollen vorschreiben, die Unternehmen im Rahmen der effektiven Sicherheitsverwaltung der Information durchführen müssen. Die Zertifizierung, dass der Unternehmer diesen Anforderungen genügt, bringt im Wesentlichen drei Vorteile: Zum einen ermöglicht die Zertifizierung dem Anbieter eine effektive Selbstkontrolle, die sich präventiv auszahlt. Zum anderen wird damit das Vertrauen des Kunden in das Unternehmen gestärkt und drittens ermöglicht die Implementierung dieser Standards eine internationale Vergleichbarkeit der Sicherheitsniveaus von Unternehmen.

---

[5] Anschaulich z.B. der Hinweis im oben (II/1 und 2) erwähnten Mustervertrag: «Bei komplexen Systemintegrations-Vorhaben bestehen zwar zu Beginn seitens beider Vertragspartner gewisse Vorstellungen und Vorarbeiten, in der Regel auch eine Umschreibung des geplanten Informatiksystems. Aber der Umfang und Ablauf des Projektes, die Kosten und Termine, sowie die Realisierung und Einführung im Einzelnen sind noch in vielen Bereichen offen. Statt dem Abschluss eines Werkvertrags mit festen Terminen und Preisen oder eines Auftrags mit reiner Vergütung nach Zeitaufwand, was in solchen Situationen für beide Vertragspartner unvernünftige Risiken mit sich bringt, empfiehlt sich der Abschluss eines Systemintegrationsvertrags …»

Als Beispiel eines solchen Standard-Werks seien die ISO/IEC 17799: 2000[6] angeführt: Diese Standards bezwecken allgemein die Gewährleistung von Informationssicherheit. In den insgesamt über hundert Sicherheitsanforderungen im ersten Teil wird festgelegt, wie ein Unternehmen vorgehen sollte, um ein Maximum an Sicherheit für seine Information zu gewährleisten (Code of Practice). Dies betrifft nicht nur den Schutz vor Informationsverlusten, etwa durch Eingriffe Unbefugter, sondern genauso die reibungslose Gestaltung der Betriebsabläufe (Festsetzung der Verantwortlichkeiten, Sicherheitskopien wichtiger Daten) oder auch noch die Kontinuitätsplanung im Verlustfall. Im zweiten Teil werden ebensoviele Kontrollen festgelegt, die das Unternehmen im Rahmen der effektiven

Sicherheitsverwaltung einführen muss. Dazu gehören etwa Eingangskontrollen, Firewalls (Zugangsschutzsysteme im elektronischen Datenverkehr) und Antivirus-Programme, Dokumentationspflichten, aber auch die Einführung einer innerbetrieblichen Disziplinarordnung. Die Betriebe werden zusätzlich verpflichtet, alle zwei Jahre eine Betriebsprüfung durchzuführen. Auf der Basis dieser zwingend einzuhaltenden Schritte kann dann ein entsprechendes Sicherheitszertifikat («Gütesiegel») ausgestellt werden. Dabei wird, wie Prof. Weber betonte, kaum ein Unternehmen auf Anhieb diesen sehr strengen Anforderungen genügen können.

Die Standards haben keine unmittelbar rechtliche Geltung. Sie sind Teil des sog. soft-law und dienen vorerst der Selbstregulierung von Unternehmen. Je mehr Unternehmen sich aber diesen Standards unterwerfen, desto grösser wird der Druck auf die übrigen Diensteanbieter. Diese faktische Bindungswirkung ist aber umso wichtiger, als fehlbaren Unternehmen kaum mehr rechtliche Konsequenzen drohen als der Verlust des Zertifikats. Immerhin werden diese Qualitätsnormen je länger je mehr Auswirkungen auf das Mass der zu erwartenden Sorgfalt bei der Vertragserfüllung haben und auch bei der Konkretisierung der Pflichten des Verwaltungsrats (Art. 717, 754 OR) im IT-Bereich von Bedeutung sein.

In diesem Zusammenhang wird auch der vom Ausschuss für Bankenaufsicht erarbeitete Entwurf zur neuen Eigenkapitalvereinbarung für Kreditinstitute (Basel II) von Bedeutung sein[7].

Basel II verlangt von den Finanzinstituten für Kredite eine vom eingegangenen Risiko abhängige Eigenkapitalunterlegung. Die Banken werden daher mittels klar definierter Ratings ihre Kunden bewerten und die Kreditkonditionen entsprechend ausgestalten; dadurch erhöht sich der Druck auf die Kreditnehmer, auch im Gebiete der IT-Dienstleistung optimale Voraussetzungen zu schaffen, was ebenfalls eine Konsolidierung der angesprochenen Standards zur Folge haben dürfte.

4. Die Versicherbarkeit von Risiken im IT-Dienstleistungsbereich

Die verschiedensten Risiken, wie sie eben erläutert wurden, führen insgesamt zu einer kostenbezogenen Gefahr, nämlich zum Haftungsrisiko.

XSP (als Bezeichung für einen beliebigen Internet Service Provider)[8] müssen sich, dies leuchtet ohne weiteres ein, für den Fall der Haftung versichern. Während der Dienstleister in der Regel der Meinung ist, gut versichert zu sein, ergibt ein Blick in die einzelnen Versicherungspolicen, dass die Versicherer sehr oft ihre Leistung in zentralen Bereichen in vom Kunden ungeahntem – und oft gesetzlich nicht zulässigem – Umfang zu beschränken versuchen. Diese Feststellung betrifft die Deckung des Unternehmerrisikos, aber auch die Deckung bei Verletzungen von fremden Patenten, Persönlichkeitsrechten und Schäden durch unbefugten Zugriff – alles für den Anbieter zentrale Risikobereiche. Die Deckungsgrade variieren je nach Versicherung beträchtlich, was einerseits grosse Unsicherheit

[6] ISO = International Organization for Standardization; IEC = International Electrotechnical Commission. ISO ist eine nicht staatliche Dachorganisation der nationalen Standardisierungsbehörden, die sich v.a. um die Angleichung nationaler Normen bemüht. Daneben wären als andere Standards etwa zu nennen: ITIL = IT Infrastructure Library und CobiT = Control Objectives for Information and related Technology. CobiT kombiniert 41 nationale und internationale Standards. Während ITIL sich mehr noch den Prozessabläufen zuwendet, wird CobiT besonders als Standard für die Revision und Kontrolle im IT-Bereich beigezogen. Beachte dazu auch die Links am Ende des Beitrags.

[7] Der Basler Ausschuss für Bankenaufsicht ist der Bank für Internationalen Zahlungsausgleich (BIZ) angeschlossen und erarbeitet weltweit verbindliche Richtlinien für Kreditinstitute und Finanz-dienstleister. Basel II soll das seit 1988 geltende Abkommen Basel I ablösen. Die Verordnung bezweckt eine grössere Sicherheit im Weltfinanzsystem und soll bis 2006 in über 100 Ländern in natio-nales Recht umgesetzt werden. Die Umsetzung wird in der Schweiz durch die Eidgenössische Bankenkommission (EBK) erfolgen.

[8] XSP steht für die Beliebigkeit der erbrachten Dienstleistung. Im Rahmen der XSP wird zumeist unterschieden zwischen dem ISP (Internet Service Provider), der den Zugang zum Internet und even-tuelle Zusatzdienste vermittelt, und dem ASP (Application Service Provider), der Leistungen eines rückwärtigen Computers online zur Verfügung stellt.

auf Seiten der Versicherer verrät, v.a. aber auch ein beträchtliches Risiko für den Kunden darstellt. Die Situation lässt sich daher allgemein als unbefriedigend bezeichnen.

Dabei lassen sich die Risiken im IT-Bereich, wie es das Beispiel des Risk Assessments gezeigt hat, durchaus bis zu einem gewissen Grad quantifizieren. Die Vermeidung solcher Unsicherheitsfaktoren bezwecken auch die eben erwähnten Standards.

Die von Peter Duschinger und Dr. H. Steigele vorgestellte Studie befasste sich insbesondere mit der Verwendbarkeit von Audits (Unternehmensbeurteilungen) auf Basis ebendieser Qualitätsnormen für die von den Versicherungen verwendeten Fragebögen. Dabei wurden sowohl auf Seiten der Kunden wie auch der Versicherungen recherchiert. Das Ergebnis ist laut Studie ernüchternd.

Die meisten der befragten Versicherungsunternehmen bezeichnen die Standards zwar als gangbaren Weg, ohne diesen jedoch einzuschlagen. Selbst erfolgte Audits werden nur in seltenen Fällen wahrgenommen. Untersucht man dabei die Begründung, so liegt diese einerseits in der mangelnden Verbreitung dieser Standards, aber auch an allzu stark gewinnorientiertem Denken jedenfalls der Versicherungskunden: Wie bereits oben ausgeführt wurde, ist die Unterstellung unter Qualitätsnormen ein aufwändiges, kostenintensives Unterfangen. Die Unternehmen versprechen sich damit keinen unmittelbaren Gewinn und werden deshalb, obwohl sie von der Existenz der Standards wissen, oft erst im Rahmen des besagten «Herdplatten-Effekts» tätig.

Diese Realität dient indessen weder den Kunden noch den Versicherern. Ob Audits nämlich wirklich keinen Mehrwert bringen, kann mit guten Gründen bezweifelt werden: Solche Bewertungen bezwecken den Nachweis der Betriebssicherheit und bilden daher ein wichtiges Verkaufsargument für den Dienstleister. Aus präventiver Sicht wäre es für die Versicherer durchaus von Interesse, ihre Kunden auf rationeller Basis bewerten zu können, denn die Verwendung von Standards erhöht Transparenz und Sicherheit. Dabei würden sich etwa ISO 17799 oder COBIT nach Meinung der Gutachter als Auditgrundlage für die Versicherung durchaus anbieten.

Nach Ansicht der Untersuchenden erbringt die IT-Branche Dienstleistungen wie ein Bauingenieur, doch fehlen die SIA-Normen. Würde man hier die Verwendung von Standards unterstützen, liessen sich IT-Risiken letztlich genauso quantifizieren wie das Risiko eines Bauingenieurs, was eine Versicherbarkeit auf standardisiertem Level durchaus ermöglichen würde. Damit könnten die starken Deckungsunterschiede zwischen den einzelnen Versicherungsanbietern vermindert, wenn nicht gänzlich eingeebnet werden.

IV. Schlussbemerkung

Im Bereich der IT-Dienstleistung lauern viele Risiken, die aber durch geeignete Massnahmen auf ein annehmbares Mass reduziert werden können. Dabei braucht es die konstruktive Mitarbeit aller Beteiligten, sowohl des Dienstleisters als auch des Versicherers und des Kunden. Deshalb ist es wichtig, Verträge sorgfältig zu redigieren und die darin stipulierten Pflichten einzuhalten. Im Sinne der Schadensvermeidung bieten sich Risk Assessment und Einhaltung von Standards an. Diese Massnahmen sind zwar teuer, dürften aber auf Dauer den besseren Weg darstellen. Die Standards sollten auch von den Versicherern beachtet werden, da dies zu einer kostengünstigeren und transparenteren Schadensdeckung beitragen würde.

Nützliche Links:

www.swico.ch (SWICO/SVD)

www.isaca.ch (COBIT)

www.iso.org (ISO)

www.bis.org (Basel II)

* lic. iur., Wissenschaftlicher Assistent an der Universität Basel.