

Verantwortung für Sicherheit beim Outsourcing

Informationssicherheit ist beim Outsourcing von zentraler Bedeutung. Die rechtliche Seite dieses Themas erweist sich in der Praxis allerdings als vielschichtig. Was gilt es zu beachten? *Wolfgang Straub*



Dr. Wolfgang Straub
LL.M., ist Rechtsanwalt in Bern. Er ist Vorstandsmitglied der Fachgruppe Security der Schweizer Informatikergesellschaft und liest Informationstechnologierecht am Departement Informatik der Universität Freiburg i.Ü.
wolfgang.straub@advobern.ch

Unter dem Begriff Informationssicherheit wird in der Praxis Unterschiedliches verstanden. Im Zusammenhang mit Outsourcing interessieren insbesondere folgende Aspekte:

- Verfügbarkeit von Daten und Systemleistung (Rechenkapazität, Speicherplatz, Übertragungsbandbreiten) unter Normalbedingungen, im Fall ausserordentlicher Ereignisse und bei Angriffen Dritter;
- Integrität der Daten des Auftraggebers: Schutz gegen Löschung und Verfälschung;
- Vertraulichkeit der Information: Unzugänglichkeit der Daten für Personen, welchen der Auftraggeber keinen Einblick gewähren will oder darf;
- Authentizität: Informationen stammen von denjenigen Personen/Organisationen, welche als Autoren erscheinen.

Unzureichende Verfügbarkeit von Daten und Systemen oder Beeinträchtigungen der Integrität von Informationen können insbesondere zu Produktionsausfall und zur Nichteinhaltbarkeit von Verträgen mit Endkunden führen. In solchen Fällen entstehen finanziell quantifizierbare – wenn auch nicht immer leicht beweisbare und bezifferbare – Schäden. Ungenügende Vertraulichkeit von Information führt hingegen meist zu nicht in Geld messbaren Verletzungen von Datenschutzbestimmungen, Geheimhaltungspflichten und Persönlichkeitsrechten.

Vertragliche Planung der Haftung

Im Hinblick auf die vertragliche Verteilung der Haftungsrisiken sollte zunächst geklärt werden, welche gesetzlichen Normen auf das konkrete Outsourcingverhältnis überhaupt anwendbar sind. Die gesetzliche Haftung kann grundsätzlich vertraglich sowohl erweitert als auch beschränkt werden. Unzulässig sind aber etwa Haftungsausschlüsse

für grobfahrlässige oder absichtliche Schadensverursachung.

Wo mit schwer beweisbaren Schäden gerechnet werden muss, hat der Auftraggeber ein Interesse an der vertraglichen Fixierung von Konventionalstrafen, Schadenspauschalen oder einem Bonus-Malus-System. Allerdings erfordern solche Instrumente eine exakte Definition und Überprüfbarkeit der Voraussetzungen.

Mindestverfügbarkeiten müssen festgelegt werden

In Outsourcingverträgen wird regelmässig eine Mindestverfügbarkeit und Mindestperformance des Informationssystems vorgesehen. Innerhalb der versprochenen Bandbreiten hat der Auftraggeber Systemausfälle und Leistungseinschränkungen grundsätzlich hinzunehmen, auf welchen Gründen sie auch immer beruhen. Immerhin können sie zu einer Verminderung der Vergütung führen, wenn diese leistungsabhängig ausgestaltet ist.

Bei Ausfällen, welche über den zulässigen Toleranzbereich hinausgehen, kann sich der Outsourcingunternehmer in der Regel von der Haftung befreien, wenn er beweist, dass ihn kein Verschulden an der Schadensverursachung trifft, das heisst, wenn ihm keine Handlungen oder Unterlassungen vorgeworfen werden können, welche den Schaden ausgelöst oder verschlimmert haben. Der Outsourcingunternehmer haftet auch für das Verhalten Dritter, welche er beigezogen hat (z.B. für Hilfspersonen und Subunternehmer).

Beeinträchtigungen der Integrität von Kundendaten stellen grundsätzlich nur dann eine Vertragsverletzung dar, wenn dem Outsourcing-Unternehmer ein pflichtwidriges Verhalten oder Unterlassen vorgeworfen werden kann. Das ist zum Beispiel dann der Fall, wenn er angemessene Schutzmassnahmen gegenüber Zugriffen Dritter unterlas-

sen hat. Welche Sicherheitsvorkehrungen durchzuführen sind, lässt sich vertraglich kaum abschliessend definieren, da sich die Risiken laufend verändern. Was vom Outsourcing-Unternehmer konkret erwartet werden darf, hängt insbesondere von der Wahrscheinlichkeit entsprechender Übergriffe und vom erkennbaren Schadenspotenzial ab.

Leistungen müssen effizient angepasst werden können

Outsourcingverträge werden meist für einen längeren Zeitraum abgeschlossen. Die Sicherheits- und Leistungsanforderungen können sich aber schon bald nach Vertragsabschluss ändern. Es sollten daher vertragliche Mechanismen vorgesehen werden, welche eine effiziente Anpassung der Leistungen an sich verändernde Verhältnisse ermöglichen (zum Beispiel Claim Management und Change Management).

Datenschutz muss sichergestellt werden

Der Inhaber einer Datensammlung muss deren Sicherheit gewährleisten (Art. 7 DSGVO/Art. 8 VDSG). Beim Outsourcing eines Informationssystems erhält der Outsourcing-Unternehmer meist technische Zugriffsmöglichkeiten auf personenbezogene Daten. Der Auftraggeber ist in diesen Fällen für eine sorgfältige Auswahl, Instruktion und Überwachung des Outsourcing-Unternehmers verantwortlich. Im Vertrag ist zu definieren, wie die Einhaltung des Datenschutzrechts sichergestellt wird. Besondere Voraussetzungen gelten für das grenzüberschreitende Outsourcing (Art. 6 DSGVO).

Soweit der Auftraggeber gegenüber seinen Kunden vertraglich oder gesetzlich zur Geheimhaltung bestimmter Daten verpflichtet ist (zum Beispiel Revisoren, Spitäler, Anwaltskanzleien), setzt das Outsourcing grundsätzlich die Einwilligung aller Betroffenen voraus (Art. 14 DSGVO). Wenn der Outsourcing-Unternehmer ohne deren Ein-

willigung eine tatsächliche Möglichkeit zum Einblick in solche Daten erhält, liegt eine strafrechtlich relevante Geheimnisverletzung vor (Art. 321 StGB). Spezielle Massnahmen erfordern auch besonders schützenswerte Personendaten, z.B. solche über Herkunft und Religionszugehörigkeit von Mitarbeitern (Art. 3 lit. c/Art. 12 DSGVO).

Der Outsourcing-Unternehmer darf die Bearbeitung von personenbezogenen oder geheim zu haltenden Daten seinerseits nur dann an Dritte weitergeben, wenn der Auftraggeber damit einverstanden ist, die notwendigen Ermächtigungen vorliegen und Gewähr für die Einhaltung des Datenschutzrechts geboten wird.

Aktive Überprüfung der Identität insbesondere bei E-Commerce-Lösungen

Je nach Art des betreffenden Informationssystems reichen die vom Outsourcingunternehmer zu ergreifenden Massnahmen unterschiedlich weit: Er ist auf jeden Fall zu einem sorgfältigen Umgang mit Informationen über die Herkunft von Daten verpflichtet und muss sicherstellen, dass Datenbankanwendungen korrekte Zuordnungen vornehmen. Zudem muss er adäquate Schutzmassnahmen gegenüber Manipulationen Dritter vorsehen. Das folgt bereits aus dem Schutz der Integrität der Daten. Aus Art und Zweck des betriebenen Informationssystems kann sich darüber hinaus eine Pflicht zur aktiven Überprüfung der Identität von Kommunikationspartnern ergeben (etwa bei E-Commerce-Anwendungen). Die Verletzung entsprechender Pflichten macht den Outsourcing-Unternehmer grundsätzlich schadenersatzpflichtig.

Auftraggeber muss zur Vertragserfüllung aktiv beitragen

Outsourcing erfordert eine relativ intensive Zusammenarbeit zwischen den Parteien. Der Auftraggeber muss aktiv bei der Vertragserfüllung mitwirken. Der Umfang seiner Unterstützungs- und Informationspflichten sollte vertraglich so weit als möglich definiert werden und ein Verfahren zur Konkretisierung und Umsetzung der Mitwirkungspflichten vorgesehen werden.

Falls der Outsourcingunternehmer Infrastruktur oder Informationssysteme vom

Auftraggeber übernimmt, kann dieser grundsätzlich selbst zur Gewährleistung verpflichtet sein. Da dies nicht der Zielsetzung solcher Verträge entspricht, wird der Auftraggeber dem Outsourcing-Unternehmer in der Regel nur seine eigenen Gewährleistungsansprüche gegenüber Dritten bzw. Serviceverträge mit Dritten abtreten. Immerhin kann er auch in diesem Fall für absichtlich verschwiegene Mängel haften.

Schäden entstehen oft durch das unglückliche Zusammenwirken verschiedener Ursachen. Hat zum Beispiel ein Hackerangriff nur deshalb zu einem Schaden geführt, weil sowohl der Hersteller einer Komponente des Sicherheitssystems als auch der Outsourcing-Unternehmer Sorgfaltspflichten vernachlässigt haben, haften grundsätzlich alle Beteiligten gegenüber dem Auftraggeber für die volle Schadenssumme. Die interne Aufteilung des Schadens richtet sich nach vertraglichen Abmachungen beziehungsweise nach der Art der Haftungsgrundlage und dem Verschulden der Beteiligten.

Informationssicherheit kann in vielen Bereichen nur durch gemeinsame Anstrengungen des Auftraggebers und des Outsourcing-Unternehmers erreicht werden. Hätte der Auftraggeber bzw. seine Arbeitnehmer oder Systemadministratoren einen Schaden verhindern oder vermindern können, führt dies meist zu einer Herabsetzung oder zu einem Ausschluss der Schadenersatzpflicht.

Bisher gibt es in der Schweiz praktisch keine Gerichtsentscheide in Zusammenhang mit ungenügender Sicherheit beim Outsourcing. Es bestehen zahlreiche rechtliche Unsicherheiten in diesem Bereich. Trotzdem lohnt sich sowohl für den Auftraggeber als für den Outsourcingunternehmer eine möglichst präzise Analyse des rechtlichen Risikopotenzials – nicht zuletzt auch mit Blick auf einen adäquaten Versicherungsschutz. Zudem empfiehlt sich die Implementierung eines effizienten Controllingverfahrens während der Vertragserfüllung.

Das Recht der IT-Sicherheit – Verantwortlichkeit von Herstellern und IT-Dienstleistern

In der Praxis stellt sich immer wieder die Frage, wann Hersteller und IT-Dienstleister für die ungenügende Sicherheit ihrer Produkte und Leistungen haften. Die Fachgruppe Security wird am 4. Juni 2003 in Zürich eine Tagung zu diesem Thema durchführen. Anerkannte Spezialisten diskutieren Präzedenzfälle und rechtliche Vorsorgemöglichkeiten. Nähere Informationen werden unter www.fgsec.ch publiziert.