

Software Escrow – unabdingbarer Bestandteil eines internen Kontrollsystems (IKS)

Von Dr. Peter Neuenschwander

Anwalt & Partner

Schweizer Neuenschwander & Partner
Zürich-Zollikon

Eine essenzielle Komponente jeder Corporate Governance ist das interne Kontrollsystem, welches zudem vom Gesetzgeber für alle revisionspflichtigen Aktiengesellschaften und Gesellschaften mit beschränkter Haftung ausdrücklich vorgeschrieben ist.

Das IKS eines Unternehmens ist die Gesamtheit aller von der Geschäftsführung angeordneten Massnahmen, Methoden und Vorgänge, die einen ordnungsgemässen Ablauf des Betriebs sicherstellen. Teil eines solchen internen Kontrollsystems ist die Beurteilung sämtlicher relevanten Risiken; d.h., die Risiken müssen identifiziert und mit angemessenen Gegenmassnahmen abgewehrt werden.

Ausgestaltung und Umfang des IKS ist in der Schweiz vom Gesetzgeber nicht vorgegeben. Die Notwendigkeit eines solchen Systems ergibt sich aber bereits aus der generellen Pflicht der Geschäftsleitung, die Interessen ihres Unternehmens sorgfältig zu wahren. Zudem hat der Gesetzgeber in Art. 728a Ziff. 1 OR vorgesehen, dass die Revisionsstelle die Existenz eines IKS prüft und dem Verwaltungsrat ihre Feststellungen über das IKS in ihrem umfassenden Bericht mitteilt (Art. 728b Ziff. 1 OR). Ein mangelhaftes IKS kann deshalb für revisionspflichtige Gesellschaften zu Problemen im Rahmen der Prüfung durch die Revisionsstelle führen. Unabhängig von der Revisionspflicht kann ein mangelhaftes IKS für alle mit der Geschäftsführung betrauten Personen im Extremfall bei Eintritt eines Schadens, der mit einem genügenden IKS hätte verhindert werden können, zu einer persönlichen Haftung führen.

Aufgrund der zunehmenden Bedeutung und Abhängigkeit der betrieblichen Prozesse von der IT, muss jedes IKS zwangsläufig auch die Risiken dieser Abhängigkeit berücksichtigen, und es müssen angemessene Massnahmen

zur Vermeidung bzw. Minimierung dieser Risiken getroffen werden.

Mit dem Erwerb einer Software-Lizenz ist die zeitlich unbeschränkte Nutzung der Software nicht gewährleistet. Denn auch wenn ein zeitlich unlimitiertes Recht zur Nutzung einer Software erworben wurde, entsteht im Lauf der Zeit unweigerlich Anpassungsbedarf. Neben Fehlerkorrekturen stehen hier v.a. die Kompatibilität mit anderer Software, insbesondere dem Betriebssystem, und die Anpassung an Änderungen von gesetzlichen Anforderungen im Vordergrund. Letzteres gilt zwar in erster Linie für Gesellschaften in regulierten Branchen, wie z.B. Banken oder Versicherungen, dürfte aber über kurz oder lang für alle Unternehmen relevant werden.

Anpassungen von Software erfolgen regelmässig im Rahmen der Wartung, die vom Softwarehersteller angeboten wird. Solange vom Softwarehersteller Wartung für eine Software bezogen werden kann, kann deshalb damit gerechnet werden, dass die Software im ursprünglich vorgesehenen Umfang verwendet werden kann.

Das Risiko für den Anwender besteht darin, dass der Softwarehersteller vom Markt verschwinden könnte (z.B. aufgrund eines Konkurses) oder die Wartung der Software einstellt. Tritt dies ein, verfügt der Lizenznehmer zwar noch über den aktuellen Stand der Software in ausführbarer Form (Objektcode), jedoch ist die Fehlerbehebung und Anpassung an zukünftige Entwicklungen nicht mehr gewährleistet, da dies mit dem Objektcode nicht möglich ist. Dies hätte zur Folge, dass mittelfristig auf eine andere Lösung umgestellt werden müsste, was hohe Kosten generieren könnte, und unter Umständen in der Zwischenzeit der ordentliche Betrieb der Software nicht mehr möglich wäre.

Das Risiko ist dabei geringer für Software, bei der auf dem Markt ein reifes Konkurrenzprodukt vorhanden ist, und höher, je spezifischer die Lösung auf den Lizenznehmer massgeschneidert wurde. Zudem ist das Risiko

höher, je essenzieller die Software für den ordentlichen Betriebsablauf ist (z.B. Kern-Bankenapplikationen oder Steuerungs-Software in Fabriken). Das Risiko kann nur dadurch verringert werden, dass dem Lizenznehmer in den genannten Fällen ein Zugriff auf den Source Code der Software zur Verfügung steht, der ihm die Anpassung der Software ermöglicht, entweder durch ihn selbst oder einen Dritten.

Für den Softwarehersteller ist ein freier Zugriff auf den Source Code grundsätzlich nicht akzeptabel, weil dieser seine Geschäftsgeheimnisse beinhaltet und einem Dritten die Möglichkeit eröffnen würde, unter Nutzung der vom Softwarehersteller erzeugten Erkenntnisse günstig ein Konkurrenzprodukt herzustellen und zu vertreiben.

Ein Software Escrow kommt nun beiden Interessen entgegen (vgl. etwa www.escrow.ch). Der Source Code wird dabei bei einem Dritten, dem hierfür spezialisierten Escrow Agent, hinterlegt und darf von diesem nur herausgegeben werden, falls ein vorgängig gemeinsam vertraglich definierter Anlass eintritt, z.B. der Konkurs des Softwareherstellers oder die Einstellung der Softwarewartung. Somit wird ein Zugriff auf den Source Code so lange verhindert, als der Softwarehersteller auf dem Markt tätig ist und die Software wartet. Ist dies nicht mehr der Fall, erhält der Lizenznehmer Zugriff auf den Source Code und kann die Software selbständig bzw. mit Hilfe eines Dritten (oder ausgeschiedenen Mitarbeitern des Herstellers) pflegen, womit der Betrieb der Software sichergestellt werden kann.

Software Escrow ist eine in der Industrie akzeptierte Lösung, die je länger je mehr zu einem Standard für betriebskritische Software wird. Da die Kosten im Vergleich zu den dadurch abgedeckten Risiken gering sind, muss Software Escrow für betriebskritische Software als unabdingbarer Bestandteil eines internen Kontrollsystems betrachtet werden.

peter.neuenschwander@snplegal.com
www.snplegal.com