Software Compliance

Risiken und Maßnahmen

Wolfgang Bruhn, Johannes Engel

15. März 2012

1 Einführung

Viele Unternehmen kennen die Situation: Seit Jahren arbeitet man in einer mehr oder weniger vertrauensvollen Partnerschaft mit einem Software-Hersteller zusammen, und dann kommt plötzlich ein Brief, in dem der eine Lizenzüberprüfung ankündigt. Und auf einmal ist es um die vertrauensvolle Zusammenarbeit geschehen, denn vielfach wird eine solche Ankündigung als Fehdehandschuh verstanden. Die Kunden interpretieren dieses Verhalten des Software-Herstellers als Misstrauensbeweis und liegen damit auch vielfach richtig, da das deutsche Urheberrecht eine solche Prüfungsmöglichkeit nur für den Fall einräumt, dass der Rechteinhaber – in diesem Fall der Softwarehersteller – einen begründeten Verdacht hegt, dass der Lizenznehmer gegen Lizenzbedingungen verstößt.

Für die Software-Hersteller sind diese Lizenzplausibilisierungen und die daraus resultierenden Nachforderungen zu einem nicht zu unterschätzenden Umsatz-Generator geworden. Für die Kunden aus verständlichen Gründen gleichzeitig zu einem erheblichen Ärgernis. Nicht nur, weil auf diesem Weg mögliche Unterlizenzierungen aufgedeckt werden und dadurch Kosten entstehen, sondern auch, weil die Vorbereitung und Durchführung eines solchen Projekts erhebliche Zeit und einen hohen Personaleinsatz erfordert, Kräfte, die dem Unternehmen während dieser Zeit an anderer Stelle fehlen.

Über all diesen Vorgängen steht das Schlagwort Compliance, das seit einigen Jahren sehr häufig im Unternehmensumfeld zu hören ist. Gemeint ist damit allerdings nicht nur die Vermeidung von Korruption und Vorteilsnahme wie in einigen der bekannten Fälle der letzten Jahre; vielmehr spielt das Thema auch und besonders in der IT jedes Unternehmens eine bedeutende Rolle. Dies wird auch dadurch sichtbar, dass viele große Software-Hersteller zunehmend das Mittel der Compliance-Prüfung (Software-Audit) für sich entdeckt zu haben scheinen und verstärkt zur Generierung von Umsätzen zu nutzen. Viele Unternehmen stehen jedoch vor großen Herausforderungen bei der Sicherstellung von Compliance im Software-Umfeld.

In dem vorliegenden Artikel werden wir primär Risikoquellen für Software-Incompliance beschreiben und – neben einem kurzen Exkurs in einige der wichtigsten Lizenzmetriken – Strategien zur Risiko-Vermeidung vorstellen. Abschließend folgen noch einige Hinweise, wie sich auch während und nach einer Lizenzprüfung noch in begrenztem Umfang die resultierenden Nachforderungen begrenzen lassen.

2 Risiken und Risikovermeidung

Aus der beschriebenen Vielfalt der Lizenzmetriken ergibt sich unmittelbar die hohe Komplexität des Lizenzmanagements schon für kleine Software-Portfolios. Mit steigender Größe des eingesetzten Software-Portfolios wächst dann auch die Unübersichtlichkeit des Themas exponentiell an. Entsprechend hoch ist das Risiko für Unternehmen, dass Software nicht lizenzkonform eingesetzt wird. Die aus diesem Risiko resultierende Gefahr lässt sich an drei Erwägungen festmachen:

1.) Im Fall nachgewiesener Verstöße gegen die Lizenzierungs-Bedingungen stehen häufig massive Schadenersatzforderungen des Herstellers an, die nicht selten gerade bei den großen Software-Herstellern durchaus kritische Höhen erreichen kann.

2.) Die Qualität der internen Planung ist besonders stark abhängig von der Transparenz im Blick auf den Lizenzbedarf. Ist diese Transparenz nicht gegeben, so leidet demzufolge die Kapazitätsplanung für die Zukunft.

3.) Sollte ein Fall von Software-Incompliance öffentlich werden, bedeutet das einen massiven Image-Schaden für das Unternehmen, da diese Tatsache auf einen zu geringen Stellenwert des Themas im Unternehmen oder beim Management schließen lässt.

2.1 Risikoquellen

Die Quellen für das Risiko der Software-Incompliance sind vielfältig. Im Großrechner-Bereich kommt es vielfach vor, dass separate Systeme als sog. SYSplex, d. h. als ein System mit

mehreren Standorten, abgerechnet werden, obwohl die Bedingungen dafür nicht vollständig erfüllt sind. Auch das Ausführen von nicht-freigegebenen Applikationen auf sog. „Specialty engines“ (zIIP, zAAP, IFL) über Spezialsoftware (bspw. Neon zPrime) wurde lange Zeit als probates Mittel gegen steigende Software-Kosten propagiert, stellt aber aus der Sicht von IBM einen Verstoß gegen die Lizenzbedingungen dar; ein diesbezüglicher Streit zwischen IBM und Neon wurde vor der gerichtlichen Klärung beigelegt, indem Neon das betreffende Software-Produkt vom Markt nahm und in einer Pressemitteilung von der weiteren Verwendung abrät.

Im Bereich kleinerer und mittlerer Server rührt eine Incompliance-Situation in vielen Fällen aus einer „wilden“ Virtualisierung her, d. h. der Virtualisierung existierender Infrastruktur ohne Beachtung der lizenzrechtlichen Besonderheiten des Software-Einsatzes in virtuellen Umgebungen. Hier spart professioneller Rat bei der Planung und Umsetzung eines Virtualisierungs-Projekts häufig viel Geld und jede Menge Ärger.

Generell erleben wir es sehr häufig, dass besonders die Komplexität der Lizenzbedingungen und -metriken entscheidend zum Entstehen von Incompliance beiträgt, da ein falsches oder unzureichendes Verständnis der Lizenzbedingungen zu einem vertragswidrigen Einsatz der Software führt.

2.2 Exkurs: Lizenzmetriken

Die Nutzungsbeschränkungen einer Software-Lizenz sind in den meisten Fällen individuell für das jeweilige Produkt. Dabei verfügt jeder Hersteller über ein eigenes Repertoir von sog. *Lizenzmetriken*, d. h. messbaren Kenngrößen für den Umfang der Software-Lizenz. Hier ist allerdings Vorsicht geboten, denn wie so häufig liegt der Teufel im Detail. Begriffe suggerieren manchmal gleiche Mess- oder Zählweisen, unterscheiden sich bei genauem Hinsehen aber in subtilen Details. Als Beispiel sei hier im Bereich der Passport-Advantage-Software von IBM der Unterschied zwischen „Concurrent Users“ und „Floating Users“ genannt: Beide messen die Anzahl gleichzeitiger Nutzer einer Software, allerdings wird beim Lizenzmodell der Floating Users für mehrere gleichzeitige Sitzungen eines Nutzers nur eine Lizenz benötigt, während beim Modell der Concurrent Users für jede Sitzung eine Lizenz notwendig ist.

Noch dazu sind die verwendeten Begriffe nicht genormt, so dass der gleiche Name bei verschiedenen Herstellern unterschiedliche Bedeutungen haben kann.

Man kann unterscheiden zwischen verschiedenen Klassen von Lizenzmetriken:

- Nutzer-basierte Lizenzmetriken: Die Lizenzen werden hier entweder dauerhaft bestimmten Nutzern des Programms zugeordnet, oder die Anzahl gleichzeitiger Nutzer wird lizenziert. Im ersten Fall ist eine Neuzuordnung nicht (bspw. bei Bindung an den Namen des Nutzers) oder nur in Ausnahmefällen möglich, bspw. wenn der ursprüngliche Nutzer die Abteilung oder sogar das Unternehmen verlässt (bspw. bei Bindung an die Funktion). Im zweiten Fall kommt üblicherweise ein Lizenzserver zum Einsatz, der bei jedem Programmstart prüft, ob die dort eingetragene Anzahl der Lizenzen einen weiteren Programmstart zulässt.
  Nutzer-basierte Lizenzen kommen häufig bei Entwicklungswerkzeugen zum Einsatz sowie bei Portal-Lösungen und Arbeitsplatz-Systemen.

- Kapazitäts-basierte Lizenzmetriken: Hierzu zählen alle Metriken, die auf die Leistungsfähigkeit der Hardware abzielen, die das betroffene Programm ausführt. Im einfachsten Fall bedeutet das, dass für jede ausführende Maschine eine Lizenz benötigt wird; vielfach üblich sind Prozessor-(kern-)Lizenzen, wobei vielfach auch noch die verschiedenen Prozessortypen nach ihrer Leistungsfähigkeit gewichtet werden (bspw. Oracles „Processor Core Factor Table“ oder IBMs „Processor Value Units“).
  Diese Lizenztypen findet man vorwiegend bei klassischen Middleware- und Backend-Systemen, bspw. Datenbanken oder Anwendungsserver.

- Lizenzmetriken auf der Basis verwalteter Systeme: Bei diesen Lizenztypen, die sich häufig bei Überwachungs- und Infrastruktur-Software findet, ist die Art und Anzahl der von der Software verwalteten Systeme maßgeblich für die benötigten Lizenzen. Für Überwachungssysteme kann das bspw. die Anzahl der überwachten Geräte sein, von Servern bis hin zu Geldautomaten oder Routern.

- Andere Lizenzmetriken: Grundsätzlich sind Software-Hersteller und Kunde frei in der Wahl der Lizenzmetriken, so dass es über die bereits beschriebenen Klassen hinaus viele weitere gibt. Denkbar ist z. B. eine Lizenzierung abhängig vom mit einem Produkt erzielten Umsatz etwa für Online-Shop-Systeme.

2.3 Risikovermeidung

Zur Vermeidung dieser Risiken ist es zwingend erforderlich, dass alle Beteiligten ein Bewusstsein für die Probleme und Risiken entwickeln und bestmöglich zusammenwirken. Dazu zählen

- Einkauf
- Lizenzmanagement
- Administratoren
- Produkt- und Infrastrukturverantwortliche

- Projektmanager und Anwendungsentwickler.

Eine der großen Gefahren liegt darin, die Verantwortung für die Software-Compliance nur einer der genannten Parteien zuzuweisen, sei es das Lizenzmanagement, die Infrastrukturverantwortlichen oder andere. Um das zu vermeiden, sind mehrere Maßnahmen sinnvoll:

- Schulung aller beteiligten Mitarbeitern und dadurch Sensibilisierung für die Risiken in ihrem Verantwortungsbereich
- Frühzeitige Einbindung von Lizenzmanagement und Einkauf bei der Projekt- und Bedarfsplanung
- Enge Abstimmung zwischen IT-Betrieb und Lizenzmanagement zur Sicherstellung eines lizenzkonformen Betriebs.
- Stetige Pflege eines Software Asset-Management-Systems, um permanent den Lizenzstand mit dem Installationsstand abzugleichen; dieser sollte dabei durch regelmäßige und automatisierte Scans der Server und Clients im Unternehmen erhoben werden. Die am Markt verfügbaren Systeme haben alle Stärken und leider auch Schwächen gerade bei der Erkennung, so dass möglicherweise mehr als ein System notwendig ist, um die installierten Produkte der verschiedenen Hersteller sicher zu erfassen.

Auch wenn die Software-Hersteller selbst vielfach über ihre Business Partner derartige Maßnahmen anbieten, so will es doch wohl überlegt sein, ob man nicht lieber einen unabhängigen Partner mit der Schulung und Beratung beauftragt, um einem eventuellen Interessenskonflikt aus dem Weg zu gehen und eine ganzheitliche Sicht auf das Thema jenseits eines bestimmten Software-Herstellers zu ermöglichen.

3 Verhalten im Fall einer Lizenzprüfung

Bei allen großen Software-Herstellern ist eine sog. „Audit-Klausel“ in den Software-Verträgen üblich, die dem Hersteller ein mehr oder weniger umfangreiches Prüfungsrecht zusichert und den Kunden zur Duldung dieser Prüfung sowie zur Begleichung daraus entstehender Forderungen verpflichtet. Eine solche Prüfung ist dem Kunden rechtzeitig vorher anzukündigen und darf den Geschäftsbetrieb nicht in unzumutbarer Weise beeinträchtigen. Im Normalfall werden Software-Hersteller diese Prüfung nicht selbst durchführen, sondern sie bedienen sich dazu Dritter, häufig Unternehmen, die auch als Wirtschaftsprüfer bekannt sind.

3.1 Maßnahmen während der Lizenzprüfung

Hat der Software-Hersteller nun bereits eine Lizenzüberprüfung angekündigt, so sind die Möglichkeiten im Normalfall begrenzt, eine nicht vorhandene Lizenzkonformität noch zu beheben. Da nach deutschem Urheberrecht eine solche Prüfung nur auf einen begründeten Verdacht hin zulässig ist, muss auch davon ausgegangen werden, dass dem Hersteller interne Regelverstöße bereits bekannt sind. Um nichtsdestotrotz den Schaden für das Unternehmen möglichst gering zu halten, sollten einige Maßnahmen ergriffen werden in der Vorbereitung und während der Lizenzprüfung.

- Zunächst sollte mit dem Prüfer eine Vertraulichkeitsvereinbarung geschlossen werden, die verhindert, dass interne Informationen unfreiwillig an die Öffentlichkeit gelangen.
- Sodann ist es sehr hilfreich, wenn vor der eigentlichen Prüfung mit dem Software-Hersteller als Auftraggeber der zeitliche und inhaltliche Rahmen der Lizenzprüfung fest vereinbart werden, um die Störung des Geschäftsbetriebs zu minimieren und eine langwierige Suche nach kleinsten Details zu vermeiden. Dies ist besonders sinnvoll vor dem Hintergrund, dass natürlich auch interne Ressourcen gebunden werden für die gesamte Dauer der Prüfung.
- Die verbleibende Zeit sollte genutzt werden, um durch schnell umsetzbare Maßnahmen die internen Reporting-Systeme zu überprüfen, etwa um Falscherkennungen und dadurch eine noch zusätzlich erhöhte Incompliance soweit wie möglich zu vermeiden. Dazu zählen u. a. die Bereinigung von übrig gebliebenen Installationsfragmenten ungenutzter Produkte, die Schaffung von Transparenz durch die Konsolidierung von Systemen mit gleichen Anwendungen sowie die Zusammenstellung sämtlicher relevanten Kaufverträge und Lizenznachweise.

Da die meisten Unternehmen für diesen Fall keine eigenen Mitarbeiter beschäftigen, werden sie zur schnellen und effizienten Umsetzung dieser Maßnahmen häufig auf externe Unterstützung zurückgreifen.
An dieser Stelle sei die Bemerkung gestattet, dass auch die besten Reporting- und Lizenzverwaltungs-Systeme stets nur so gut sind wie ihre Pflege und Befüllung. Da diese Software mit der Erkennung von Produktbündeln oder etwaiger vertraglicher Sonderregelungen deutlich überfordert ist, ist an an diesen und anderen Stellen der manuelle Pflege-Aufwand von größter Wichtigkeit, um ein korrektes Ergebnis zu garantieren. Dies zahlt sich üblicherweise sehr schnell aus, da sich so während und nach der Lizenzprüfung eventuelle Nachzahlungen für eine de facto möglicherweise gar nicht vorhandene Incompliance, Aufwendungen für eine rechtliche Auseinander-

setzung und Ressourcen für die nachträgliche Richtigstellung einsparen lassen.

Während der Lizenzprüfung ist dann eine vorsichtige Kommunikationsstrategie von entscheidender Bedeutung.

Häufig sind auch schon unbedachte Äußerungen von Mitarbeitern, etwa über Bereinigungsmaßnahmen während der Vorbereitung, zum Stolperstein geworden, da sie als Beleg für einen Verstoß gegen die Lizenzierungsbedingungen in der Vergangenheit gewertet werden können. So kann ein falsche Wort schnell einen großen (negativen) Wert für das Unternehmen bekommen, denn der Beweis einer lückenlosen Compliance ist besonders schwer und aufwändig zu führen, wenn Indizien dagegen sprechen. Im Ernstfall kann das auch für den einzelnen Mitarbeiter durchaus arbeitsrechtliche Konsequenzen haben. Sämtliche Mitarbeiter, die in Kontakt mit dem Prüfer kommen, sollten daher dahingehend geschult werden, dass sämtliche Informationen ausschließlich über eine zentrale Person an das Prüfungsunternehmen gegeben werden dürfen, damit eine einheitliche Kommunikation sichergestellt ist und zu jeder Zeit überprüfbar ist, welche Informationen dem Prüfer zugegangen sind. Außerdem kann auf diese Weise effektiv die Übermittlung unvollständiger Informationen verhindert werden, die anderenfalls zur Fehlinterpretationen führen könnte.

Es versteht sich von selbst, dass ein direkter Systemzugang für Externe unbedingt zu vermeiden ist. Maßgeblich dafür sind vor allem IT-Sicherheits- und Datenschutzvorgaben. Lässt sich der Einsatz von Testprogrammen und -skripts durch den Prüfer nicht vermeiden, so sollten diese vor dem Einsatz in jedem Fall auf Herz und Nieren getestet werden. Vor jedem Einsatz ist diese erfolgte Unbedenklichkeitsprüfung sicherzustellen, um Betriebsunterbrechungen oder Datenlecks zu verhindern.

3.2 Maßnahmen im Anschluss

Liegt der Bericht des Prüfers erst einmal vor, so gilt der faktische Installations- und Lizenzbestand damit als festgestellt. Obschon naturgemäß die Handlungsmöglichkeiten in diesem späten Stadium recht begrenzt sind, muss aber auch jetzt noch nicht alles verloren gegeben werden. So ist bspw. eine vorhandene Incompliance nicht immer zu 100% durch das betroffene Unternehmen zu vertreten, da vielfach der Software-Hersteller in die Planung und Bereitstellung des Einsatz-Szenarios eingebunden war und dadurch möglicherweise eine Mitverantwortung an der entstandenen Incompliance trägt. Diesen Nachweis zu führen erfordert schnelle und gründliche Recherche sowie einen geschulten Blick für die kritischen Punkte. Anschließend muss dann eine Einigung mit dem Software-Hersteller herbeigeführt werden über die Zurechenbarkeit der Incompliance und Maßnahmen zu deren Behebung.

Fazit: Auch wenn der Ernstfall einer Lizenzprüfung bereits eingetreten ist, so bedeutet dies noch nicht, dass es keine Maßnahmen mehr gibt, um die Nachforderungen zu reduzieren. Investitionen in die Ressourcen im Umfeld der Lizenzprüfung machen sich in den meisten Fällen recht schnell bezahlt.

Sie wollen noch mehr wissen? Bitte wenden Sie sich gerne an uns:

Herrn Dr. Johannes Engel
Junior Project Manager
E-Mail: j.engel@intero-consulting.de

Herrn Wolfgang Bruhn
Partner
E-Mail: w.bruhn@intero-consulting.de

Tel: 089/27 37 014-0.