



# 2. ■ Ratgeberserie für Unternehmen

Gefährden Sie nicht Ihr Unternehmen

So gewährleisten Sie die Lizenzierung Ihrer Software

## Welche Risiken geht Ihr Unternehmen ein?

2007 beauftragte die Business Software Alliance (BSA) das unabhängige Forschungsinstitut GfK NOP damit, die Einstellung kleiner und mittlerer Unternehmen (KMUs) in Europa gegenüber Software zu untersuchen und wie bewusst sie sich der Risiken sind, die mit dem Gebrauch von unlizenzierter Software (u.a. Raubkopien) einhergehen. 95% dieser Betriebe gaben an, sich sicher zu sein, dass ihre gesamte installierte Software ausreichend lizenziert ist. Eine gründliche Analyse von IDC zeigte jedoch, dass Software-Piraterie in Europa immer noch sehr verbreitet ist und in Westeuropa bei 34%, in Mittel- und Osteuropa bei 68% liegt.

Diese Diskrepanz zwischen der Wahrnehmung der Situation und der Realität lässt auf ein mangelndes Bewusstsein unter den Führungskräften im Hinblick auf Software und Software-Management schließen. Dies ist eine gefährliche Situation, denn Software hat sich rasch zu einem der wertvollsten und wichtigsten Unternehmenswerte entwickelt. Wenn Unternehmen weder in ihre Software investieren noch sie angemessen verwalten und schützen, gehen sie zahlreiche Geschäftsrisiken ein, die beträchtliche finanzielle Auswirkungen haben können.

Die Business Software Alliance zeigt mit diesem Leitfaden auf, welche Risiken unlicenzierte Software (Raubkopien, falsche und unzureichende Lizenzen) birgt, wie Sie Ihr Unternehmen schützen und den Nutzen der von Ihnen verwendeten Software maximieren können.

### Definitionen:

**Unlizenzierte Software:** Darunter versteht man jedes Softwareprodukt, das auf einem PC installiert worden ist, ohne dass die Lizenzvereinbarung die Installation gestattet oder eine Lizenz- bzw. Nutzungsvereinbarung mit dem Besitzer des Urheberrechts besteht. In diesem Dokument wird der Begriff „unlizenzierte Software“ für alle drei Formen der unten aufgeführten Verletzung des Urheberrechts für Software verwendet.

**Unterlizenzierte Software:** Darunter versteht man Software, die auf mehr PCs installiert worden ist, als es die Lizenzvereinbarung gestattet. Eine Lizenz kann zum Beispiel die Installation auf 20 PCs gestatten, wurde sie nun aber auf 30 PCs installiert, so gelten die zehn zusätzlichen Installationen als unlizenziert.

**Falsch lizenzierte Software:** Software wird für Zwecke eingesetzt, die die Lizenzvereinbarung nicht vorsieht, z.B. die kommerzielle Nutzung von Software, die nur für den akademischen Gebrauch lizenziert ist.

**Software-Raubkopien:** Jede Software, die (in beträchtlichem Maße) bewusst kopiert wurde, um die Besitzer des Urheberrechts durch illegalen Vertrieb zu betrügen, entweder mittels CDs oder Internet-Download-Sites. Dazu gehört auch gefälschte Software.

## Vorwort

Für viele kleine und mittlere Unternehmen (KMUs) hat sich das Risikomanagement sehr schnell verändert: Kontrolle und Transparenz sind stärker in den Vordergrund gerückt und der Druck, noch strengere Vorschriften einzuführen, scheint ständig zu steigen. Viele fühlen sich überrollt vom ständigen Aufruf zu besserem Risikomanagement. Welche Vorteile aber bietet dies einem Unternehmen? Warum sollte man Aspekten des Risikomanagements, wie z.B. dem Software-Asset-Management und der Datensicherheit, Aufmerksamkeit zollen?

KMUs stellen weltweit die große Mehrheit der Unternehmen dar. In Europa werden weit mehr als die Hälfte aller Jahresumsätze von ihnen erzielt und sie beschäftigen in den meisten Ländern die große Mehrheit der Arbeitnehmer. Sich nicht gegen große Geschäftsunterbrechungen vorzubereiten oder das mögliche Auftreten solcher sich nicht eingestehen zu wollen, macht viele Firmen sogar für kleine Störungen anfällig. Zusammen riskieren sie damit viele Tausend Arbeitsplätze und stellen eine Bedrohung für die vielen anderen Unternehmen dar, mit denen sie als Lieferanten oder Kunden zusammenarbeiten.

Die Geschäftsführer der KMUs sind daran gewöhnt, mit geschäftlichen Herausforderungen wie schwankenden Lieferpreisen, neuer Konkurrenz und anspruchsvollen Kunden fertig zu werden. Die Vertrautheit mit solchen alltäglichen Herausforderungen kann zu übersteigertem Vertrauen in die Fähigkeit der Firma führen, mit Katastrophen zurechtzukommen – auch in kleinem Rahmen.

Die Gesamtauswirkungen einer Geschäftsunterbrechung werden ebenfalls häufig unterschätzt. Eine Studie von Gartner Consultants weist darauf hin, dass 40% der Unternehmen, die eine größere Unterbrechung der Geschäftstätigkeit überstanden haben, innerhalb von 5 Jahren Schiffbruch erleiden. Eine andere Studie zeigt, dass Unternehmen, die mehr als dreißig Tage benötigen, um zum normalen Betriebsablauf zurückzukehren, mit sehr großer Wahrscheinlichkeit Bankrott gehen.

**Angesichts des heutzutage größeren Bewusstseins gegenüber dieser Anfälligkeit, überrascht es durchaus, dass so viele Unternehmen sich nicht auf Unterbrechungen vorbereiten. Diese Tatsache ist weithin bekannt, die Gründe dafür werden aber nur selten besprochen.**

Unsere in Henley durchgeführte Studie ergab, dass bei den Unternehmen, die in Risikomanagement-Aktivitäten investieren, die Einschätzung der Risikoquellen im Vergleich zur eigenen Risikofreudigkeit ein entscheidender Faktor ist. Dennoch wissen alle Geschäftsführer von KMUs ganz genau, dass der erfolgreiche Umgang mit Geschäftsrisiken mit Profiten belohnt wird und sie als grundlegender Bestandteil von Profit unvermeidbar sind.

Beim Risikomanagement geht es jedoch nicht nur um die Reduzierung von Risiken. Es geht darum, die Risikofreudigkeit der Firma zu kennen und die Risiken abzuschwächen, indem ihre Wahrscheinlichkeit und/oder ihre Auswirkungen soweit wie möglich reduziert werden, ohne die Geschäfte der Firma zu behindern. Mit einem optimalen Risikomanagement kann die Firma eine erhöhte Gefährdung zulassen und ihre Profite potenziell steigern, ohne ihre Risikobereitschaft zu übersteigen. Ein gutes Risikomanagement erhöht die Belastbarkeit einer Firma.

Viele Firmen erkennen nicht, welche Rolle Risiken bei ihrer Geschäftstätigkeit spielen. Größere Firmen gehen bei Investitionen in neue Projekte strukturiert vor und berücksichtigen Risiken bei ihren Ertragserwartungen. Kleinere Firmen wenden derart rigorose Methoden jedoch nicht immer an und gehen damit während ihres Wachstums zu viele potenzielle Risiken ein.

## **Ob dies durch die Konzentration der Geschäftsführer auf Cash-Flow oder Wachstum kommt - kleinere Firmen können ihre gesamte Existenz riskieren, wenn sie ohne Berücksichtigung von Risikomanagement wachsen.**

Dies hat Auswirkungen auf das Management des Datensicherheitsrisikos, was in naher Zukunft durch neue Technologien noch komplizierter wird. Die Entwicklung und Implementierung neuer Arten von IT und Software-Vertriebsmechanismen wird beträchtliche Auswirkungen auf die Anforderungen haben, die an die Risikomanagementprozesse gestellt werden.

Und zu guter Letzt sollten wir nicht vergessen, dass es die direkt wahrgenommenen Risiken sind, denen man sich mit Urteilsvermögen stellt (z.B. dem Überqueren von Straßen), viele mit Software verbundenen Risiken werden aber immer noch als „virtuell“ wahrgenommen. Während die meisten Geschäftsführer von KMUs ihre Erfahrung mit defekten Festplatten oder einem Computervirus haben, so hatten nur wenige mit sehr ernststen Konsequenzen umzugehen. Zwar können nur wenige große Katastrophen mit Software in Verbindung gebracht werden, sie haben sich aber schon gleichermaßen in großen als auch kleinen Organisationen ereignet.

Die rechtlichen Folgen des Gebrauchs unlizenzierter Software können beträchtlich sein. Weniger bekannt ist allerdings, dass Sie durch den Einsatz lizenzierter Software Zugang zu technischem Support haben, besseren Schutz gegen Viren oder Malware und daher weniger Unterbrechungen. In einer Welt, in der die Geschäftskontinuität von wesentlicher Bedeutung ist, können KMUs schlechter Unterbrechungen auffangen als große Firmen. Sie sind normalerweise nicht so belastbar wie große Organisationen, die über diverse Standorte, Geldreserven und externe Berater verfügen. Wie die dargelegten Forschungsergebnisse und Ratschläge zeigen, passiert es schnell wachsenden kleinen Firmen oft, dass sie wichtigen Risikomanagementaufgaben, wie der Prüfung der Software-Lizenzierung, nicht genügend Aufmerksamkeit zollen, obwohl sie dort am verwundbarsten sind.

Wie in diesem Leitfaden angesprochen, ist man sich dieser erhöhten Anfälligkeit wenig bewusst, was aus der mangelnden Aktivität und Vorbereitung, die berichtet wurde, hervorgeht. Was aber können wir dagegen unternehmen und was sollten wir tun? Ich schlage vor, dass wir einmal die Konsequenzen eines schlechten Risikomanagements und den Nutzen eines guten Risikomanagements betrachten.

Zu oft verbergen wir Probleme, weil wir negative Auswirkungen auf unseren Ruf befürchten. Allerdings können wir nur durch die Kommunikation mit unseren Kollegen effektive Risikomanagement-Strategien entwickeln, mit denen die

Geschäftsführung das richtige Maß an Aufmerksamkeit auf jene wenigen Risikomanagement-Aktivitäten legt, die wirklich wichtig sind und um dafür zu sorgen, dass wir die Belohnungen für den erfolgreichen Umgang mit Wirtschaftsrisiken erhalten können und die Gefahren, die unangebrachtes Eingehen von Risiken birgt, vermeiden.

Dieser Leitfaden trägt zu diesen Kommunikationsbemühungen bei. Was die Software-Lizenzierung betrifft, so ist das Verhältnis von Risiken und Belohnung ziemlich einfach zu verstehen. Betriebsablauf und Firmenimage profitieren sehr von der richtigen Software-Lizenzierung. Die Belohnung für unzulängliche Lizenzen ist nicht nur gering – sie ist nicht zu kontrollieren und die Wurzel noch größerer Risiken.

## Jean-Noel Ezingard, Henley Management School.



## Software und Geschäftsrisiko

Software gehört zu den kostbarsten Vermögenswerten eines Unternehmens und so ergab eine kürzlich von der BSA durchgeführte Studie, dass 94% der Unternehmen in Europa IT als unentbehrlich für die erfolgreiche Arbeit ihres Unternehmens erachten<sup>1</sup>. Spezialsoftware ermöglicht Architekten, Ingenieuren, Wissenschaftlern, Finanzorganisationen und Designern, wettbewerbsfähig und innovativ zu sein. Aber auch bei den alltäglichen Geschäftsvorgängen ist fast jedes Unternehmen von Tabellenkalkulationsprogrammen für das Management von Finanzvorgängen abhängig, von Datenbanken zur Speicherung äußerst wichtiger Informationen, von E-Mail zur Kommunikation (mit Kollegen, Kunden und Lieferanten) und von Desktop-Publishing-Paketen, um Präsentationen und Marketing-Unterlagen zu erstellen.

Daher mag es überraschen zu erfahren, dass es für 36% der in EU-Unternehmen benutzen Software keine gültige Lizenz gibt.<sup>2</sup>

Unkenntnis eines Unternehmens über den Status seiner Software-Lizenzen ist keine Rechtfertigung. Daher ist es von größter Bedeutung, dass Unternehmen sowohl die Risiken der Software-Piraterie auf das Geschäft genauestens kennen, als auch die Schritte, die sie unternehmen können, um diese Risiken zu vermeiden und ein rechtmäßiges Vorgehen sicherzustellen.

Genau wie ein Unternehmen seine Mitarbeiter angemessen und bestimmten gesetzlichen Vorschriften entsprechend zu führen hat, gilt dies auch für die Software, die es benutzt. Während die meisten Unternehmen die Finanz- und Personalbestimmungen kennen und Prozesse implementiert haben, tragen sie auch eine Verantwortung gegenüber sich selbst und allen Interessensgruppen, ihre Software-Werte umsichtig zu verwalten und ein entsprechendes Bewusstsein in ihrem Unternehmen zu fördern.



<sup>1</sup> Quelle: GfK-NOP-Studie „Commercial Risk“ von 2007

<sup>2</sup> Quelle: IDC-Studie „Software Piracy“ von 2007

Dies mag zuerst schwierig erscheinen, insbesondere, wenn das Unternehmen schnell wächst und es beträchtliche Veränderungen bei der Unternehmensstruktur gibt. Dennoch muss neben der Berücksichtigung der besten Arbeits- und Kommunikationsweisen mit Interessensgruppen und Mitarbeitern, der Prüfung potenzieller Veränderungen des Finanzstatus und der Überprüfung von Verträgen mit Lieferanten und Kunden auch Zeit in das Management der Software-Erfordernisse investiert werden. Langfristig wird sich dies als gut investierte Zeit erweisen.

Bei einem guten Software-Management geht es nicht nur darum, die Risiken zu vermeiden, die die Benutzung unlizenzierter Software für Ihr Unternehmen bedeutet. Es kann auch zu Effizienzsteigerungen und beträchtlichen Kosteneinsparungen führen – nicht nur im Hinblick auf die direkten Softwareausgaben, sondern auch bei den Prozessen und der damit verbundenen Infrastruktur.

Ein effektives Software-Management bietet zahlreiche Vorteile: Es kann Ihnen eine bessere Ausgangsposition bei Verhandlungen mit Software-Anbietern verschaffen und sorgt dafür, dass Sie über die nötigen Informationen verfügen, um bei Ihren Softwareeinkäufen mit Gewissheit das Richtige zu tun.

**Es ermöglicht eine strategische Planung und verhindert die Unter- oder Überlizenzierung, während gleichzeitig die Belastungen für Verwaltung und Support sowie die dazugehörigen Kosten gesenkt werden.**

**Darüber hinaus wird Ihre IT-Abteilung in die Lage versetzt, besser zu kontrollieren, zu welcher Software Mitarbeiter Zugang haben und ob sie nicht autorisierte Software in Ihr Netzwerk einführen können.**

## Die wirtschaftlichen Auswirkungen

Software-Piraterie hat nicht nur negative Auswirkungen auf die Geschäftswelt, sondern viel weitreichendere Folgen für die Wirtschaft insgesamt. Software-Piraterie mindert die Einnahmen, die Software-Hersteller sonst in Forschung und Entwicklung sowie Arbeitsplätze investieren würden. Da Software eine Schlüsselrolle in der Informationswirtschaft spielt, wirkt sich dies nach und nach auch auf andere Teile der IT-Branche und die Wirtschaft insgesamt aus.

Die IT-Branche beschäftigt nicht nur Abertausende von Mitarbeitern und trägt beträchtlich zum Bruttoinlandsprodukt bei, sie fördert auch in den meisten anderen Wirtschaftsbereichen die Produktivität. Es ist daher von entscheidender Bedeutung, dass Unternehmen den Wert von Software anerkennen und dafür sorgen, dass jede legal genutzt und richtig lizenziert ist.

Optimale Geschäftsverfahren und eine gute Urteilsfähigkeit hinsichtlich der sozialen Verantwortung von Unternehmen fördern Fairness und ethisches Verhalten in der Geschäftswelt. Auch die notwendige Rücksichtnahme auf die Stakeholder Ihres Unternehmens, einschließlich auf die Entwickler der Software, die für Ihr Unternehmen von wesentlicher Bedeutung ist, profitieren davon.



## Unlizenzierte Software: Was sind die Risiken?

Nach einer von der BSA in Auftrag gegebenen Studie<sup>3</sup> glaubt ein Fünftel der KMUs in Europa, dass kein Risiko mit dem Herunterladen, der Installation und der Nutzung unlizenzierter Software verbunden ist. Dieses Vorgehen birgt jedoch viele Geschäftsrisiken. Kein Risiko zu befürchten und zu glauben, man müsse sich über unlizenzierte Software keine Gedanken machen, ist ein beunruhigender Trend. Wenn Sie die mit unlizenzierter Software verbundenen Risiken nicht erkennen, setzen Sie Ihr Unternehmen jedoch zahlreichen Gefahren aus.

**Der Gebrauch unlizenzierter Software kann sich auf operative, technische und finanzielle Aspekte auswirken und rechtliche Konsequenzen für ein Unternehmen haben.**



<sup>3</sup> Quelle: GfK-NOP-Studie „Commercial Risk“ von 2007

## Operative und technische Risiken

### Datenverlust und beschädigte Daten

IDC-Studien<sup>4</sup> haben ergeben, dass Raubkopien, die durch illegales Herunterladen oder gefälschte CDs beschafft wurden, zu 50 Prozent „zusätzlichen Code“ beinhalten, wie z.B. Trojaner, Viren oder Spyware, die Abstürze von IT-Systemen verursachen oder Unbefugten Zugang zu Ihren vertraulichen Geschäftsdaten verschaffen können. Zudem bieten Raubkopien oft keine Sicherheitsupdates. In manchen Fällen können bei unlizenzierter Software nur die wichtigsten Updates angewandt werden und Ausfallzeiten und Sicherheitslücken können sich umgehend negativ auf Ihr Endergebnis auswirken.

### Funktionalitätsverluste

Zusätzlich zu den Sicherheitsrisiken, die der Gebrauch von Raubkopien, die von Websites oder P2P-Networks heruntergeladen wurden, birgt, ist solche Software häufig unzulänglich oder kann Funktionalitätsverluste und Probleme mit der Kompatibilität verursachen, die man mit legalen, lizenzierten Versionen nicht hätte. Unlizenzierte Kopien erhalten ggf. nicht alle Updates vom Hersteller, d.h., Ihre Mitarbeiter können die Software nicht umfassend nutzen, wodurch sich Ihre Konkurrenz Wettbewerbsvorteile verschafft: Sie kann schneller, umfassender oder effektiver reagieren, da sie über die nötigen Hilfsmittel verfügt. Es besteht zudem das Risiko, dass Daten beschädigt oder nicht richtig gespeichert werden, was zu bedenklichem Datenverlust führen kann.

### Mangelnder technischer Support

Da Betriebsabläufe sehr von der Informationstechnologie abhängen, ist es ausgesprochen wichtig, dass entsprechender Support zur Verfügung steht. Benutzer von unlizenzierter Software haben häufig keinen Zugang zum unverzichtbaren technischen Support, den die Händler anbieten, und arbeiten daher weniger effizient.

### Rufschädigung

Der Ruf eines Unternehmens kann deutlich Schaden nehmen, wenn entdeckt wird, dass es illegale Software benutzt, auch wenn dieser Schaden nur schwer zu quantifizieren ist. Denken Sie nur an die Auswirkungen, wenn Ihre Kunden nicht den erwarteten Service erhalten. Eine in Großbritannien durchgeführte Studie ergab somit auch, dass 42% der Befragten meinten, ihre Kunden wären weniger geneigt mit ihnen Geschäfte zu machen, wenn sie von dem Gebrauch illegaler Software wüssten.<sup>5</sup>

<sup>4</sup>Quelle: IDC-Studie „The Risks of Obtaining and Using Pirated Software“ von 2006

<sup>5</sup>Quelle: YouGov-Studie „Corporate Ethics“ von 2006

## Finanzielle und rechtliche Risiken

### Rechtliche Konsequenzen

Die Entwicklung von Software beinhaltet jahrelange Investitionen und vereint die kreativen Ideen und Talente von Programmierern, Autoren und Grafikkünstlern. Wie fast alle kreativen Werke ist Computer-Software durch Urheberrechte geschützt und diese Rechte müssen von den Anwendern respektiert werden, damit die Software-Branche weiterhin innovativ sein kann.

Wenn Sie Software kaufen, werden Sie nicht zum Besitzer der Urheberrechte. Stattdessen werden Sie durch den Kauf einer Lizenz zum Lizenznehmer und erhalten das Recht, die Software unter bestimmten, vom Besitzer des Urheberrechts festgelegten Bedingungen zu benutzen. Dies ist normalerweise der Herausgeber der Software. Die Lizenz ist ein Rechtsdokument, das die Nutzungsbedingungen für ein bestimmtes Software-Produkt festlegt. Wenn ein Unternehmen gegen die Bedingungen der Software-Lizenz verstößt – indem es die Software absichtlich oder unabsichtlich auf eine Art und Weise kopiert, vertreibt oder installiert, die in der Lizenz untersagt ist – so verletzt es das Urheberrecht und verstößt gegen das Gesetz. Das Zivil- und Strafrecht ist in Europa unterschiedlich, es können aber beträchtliche Strafgebühren erhoben werden.

### Die Kosten, erwischt zu werden

Wenn Sie unter Verdacht stehen, unlicenzierte Software zu benutzen, greift die Business Software Alliance ein. Werden Sie der Missachtung des Software-Urheberrechts überführt, da Sie auf den PCs Ihres Unternehmens unlicenzierte Software installiert haben, muss sich Ihr Unternehmen auf die Zahlung hoher Schadensersatzforderungen und Rechtskosten einstellen. Ihr Unternehmen wird außerdem legale Versionen der benötigten Software kaufen müssen, um weiterarbeiten zu können.

### Geldstrafen

Abhängig von Ihrer Branche kann der Gebrauch unlizenzierter Software dazu führen, dass Ihnen Geldstrafen von diversen Behörden drohen – ob von Finanz-, Vollstreckungs- oder Datenschutzbehörden. Viele solcher Behörden haben Kriterien, die akzeptable Vorgehensweisen festlegen, und unlicenzierte Software kann gegen diese Vorgehensweisen verstoßen, was Ihrem Unternehmen zusätzliche Geldstrafen einbringen kann.

### Kosten durch die Beseitigung des Problems

Wenn bei Unternehmen illegale Software entdeckt wird, müssen Sie häufig alle unlicenzierten Versionen löschen und diese nicht lizenzierte Software somit durch legale Versionen ersetzen. Es lohnt sich einfach nicht, durch Kosteneinsparungen bei der Software-Lizenzierung dieses Risiko einzugehen, ganz abgesehen von der Unterbrechung, die Ihrem Unternehmen widerfahren könnte, wenn es in einen potenziellen Rechtsstreit verwickelt wird.

## Wie gelangt unlizenzierte Software auf die PCs Ihres Unternehmens?

In einem Unternehmen kann unlizenzierte Software aus diversen Quellen stammen: Nicht autorisierte Downloads von Mitarbeitern, versteckte Downloads über Pop-up-Fenster durch den Besuch einiger Websites und ein schlechtes Software-Lizenz-Management sind nur einige davon. Die Gründe für solche Versehen sind häufig mangelndes Bewusstsein bei den Geschäftsführern und Mitarbeitern, unzulängliche IT-Richtlinien und schlechtes Vorgehen beim Software-Management. Leider wird unlizenzierter Software in einigen Fällen absichtlich benutzt und die Geschäftsführung ist sich der Situation völlig bewusst, aber nicht der damit verbundenen Risiken.

Wie man die unten dargelegten Probleme bekämpft, wird in dem Abschnitt „Wie reduziert man die Risiken“ besprochen.

### **Schlechtes Software- und Software-Lizenz-Management**

Die Bedeutung von Software, die erhältlichen Arten von Software und die unterschiedlichen Formen der Software-Lizenzierung zu kennen, kann sich beträchtlich auf die Abläufe und das Wachstums Ihres Unternehmens auswirken und sollte daher bei Geschäftsentscheidungen berücksichtigt werden. Wenn Sie das Bewusstsein hinsichtlich der Software-Werte in Ihrer Organisation erhöhen und dafür sorgen, dass sie umfassend verwaltet und geschützt werden, können sie effektiver eingesetzt werden, um Produktivität und Effizienz zu erhöhen.

Für jede Erfordernis stehen unterschiedliche Software-Lizenzen zur Verfügung: Von einfachen Formaten, bei denen man durch Anklicken sein Einverständnis bekundet, bis zu viel komplexeren, ausgehandelten Vereinbarungen. Diese werden von Jahr zu Jahr flexibler. Viele Standard-Lizenzen gestatten die Installation auf einem bis zu fünf PCs, während ein Volumenlizenzprogramm eine bestimmte Anzahl von Installation von einer Master-CD gestattet. Für jede über die festgelegte Anzahl hinausgehende Installation braucht man die Einwilligung des Software-Herstellers oder -Resellers. Allzu oft führt das Fehlen genauer Installationsaufzeichnungen oder strikter Unternehmensrichtlinien dazu, dass Unternehmen schließlich gegen das Gesetz verstoßen.

Zu einer Unterlizenzierung kommt es, wenn Software auf mehr PCs genutzt wird, als die Lizenz gestattet. Dies ist häufig eine Folge ineffektiven Software- und Software-Lizenz-Managements. Wenn die Lizenz die Installation der Software auf zwanzig PCs gestattet, ist jede Installation der Software auf zusätzlichen PCs nicht lizenziert und verstößt gegen die Lizenzbedingungen. Es handelt sich hierbei praktisch um eine illegale Kopie und mit unlizenzierter Software erwischt zu werden, birgt die beachtlichen, oben aufgeführten Risiken.

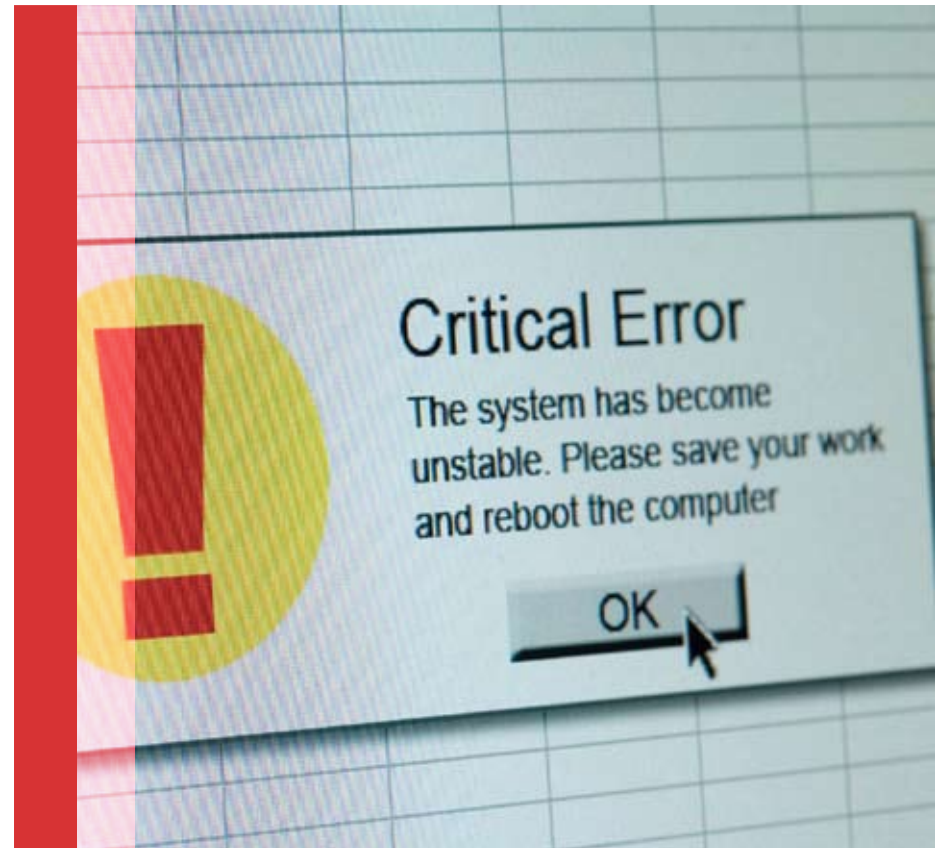
## Über das Internet heruntergeladene Software

Das Internet ist für das Geschäftsleben unverzichtbar und viele Unternehmen verlassen sich sehr darauf. Allerdings kann es auch dazu führen, dass unerwünschte, nicht genehmigte Software auf Unternehmens-PCs heruntergeladen wird, es sei denn, es gibt entsprechende Prüfungen und Kontrollen.

Da Internetverbindungen viel schneller geworden sind, ist es jetzt sehr viel leichter, Musik, Filme und andere Medien zu kaufen und/oder herunterzuladen. Es ist zunehmend einfacher geworden, Produkte ohne zusätzliche Speichermedien von einem Computer auf einen anderen zu übertragen und mit nur geringem Risiko, entdeckt zu werden. Software-Piraterie, die einst Kenntnisse über komplexe Computer-Codes erforderte, kann heute mit einem Mausklick stattfinden.

Ohne Blockiertechnologie zur Verhinderung solcher nicht autorisierten Downloads, können Mitarbeiter Ihres Unternehmens Software ohne Ihr Wissen und Einverständnis herunterladen.

Dies birgt eine Reihe von Risiken. Wenn ein Angestellter unlicenzierte Software installiert hat, ist dennoch der Besitzer oder Geschäftsführer des Unternehmens für die Urheberrechtsverletzung verantwortlich und das Unternehmen kann rechtlich und finanziell dafür zur Verantwortung gezogen werden. Wenn die heruntergeladene Software unbekanntem Ursprungs ist, kann sie Viren, Spyware oder Trojaner enthalten, denen der direkte Zugang zu Ihrem IT-Netzwerk ermöglicht wurde.



Ein zunehmendes Risiko geht auch von Pop-up-Fenstern aus, die auf dem Bildschirm erscheinen, wenn ein Mitarbeiter bestimmte Websites besucht. Häufig bieten diese preiswert Software oder Bilder zum Herunterladen an, dienen manchmal aber als Fassade für illegale Aktivitäten und installieren Software, Viren und Spyware auf den PC, indem sie den Mitarbeiter einfach zum Anklicken des Pop-ups verleiten.

### **Internet-Auktionsbörsen**

Eine der größten Erfolgsgeschichten des Internets sind zweifellos Auktionsbörsen. Dort kann man Bücher, Spielzeug, Sammlerstücke, sogar Häuser im Internet verkaufen. Flexibilität, Geschwindigkeit und Erfolg dieser Websites sind nicht nur ein Beweis für ihre Popularität, sondern auch für die Vorteile, die sie sowohl Käufern als auch Verkäufern bieten. Unter der Mehrheit der ehrlichen und echten Angebote gibt es jedoch Fallen für den unvorsichtigen Käufer. Die billigeren Preise für scheinbar authentische Software können kleine und wachsende Unternehmen reizen, die Kosten sparen möchten. Die Möglichkeit, seine Identität zu verbergen oder zu ändern, verleitet jedoch viele dazu, dieses Medium für illegale Aktivitäten zu nutzen. Daher sind Auktions-Websites zu einem Lieblingsmedium für jene geworden, die unlicenzierte Software oder Raubkopien verkaufen möchten.

**Eine 2006 von IDC-Analysten durchgeführte Studie hat ergeben, dass weniger als 49% der auf eBay angebotenen Microsoft-Software ungefälscht war.<sup>6</sup>**

Nachdem man den Kauf illegaler Software erkannt hat, kann es jedoch sehr schwierig sein, eine Entschädigung dafür zu bekommen. Von den betrogenen Verbrauchern, die sich beschwert hatten, erhielten nur sehr wenige Rückerstattungen für ihren Kauf. Und von denen, die Geld zurückerhielten – nachdem Sie viel Zeit und Mühe in ihre Forderungen investiert hatten – deckten die Rückerstattungen oft nicht einmal den Preis der Raubkopien.

<sup>6</sup> Quelle: IDC-Studie „The Risks of Obtaining and Using Pirated Software“ von 2006

## **Mobiles Arbeiten**

Arbeitskräfte werden weltweit zunehmend mobiler und Arbeitgeber statten ihre Mitarbeiter mit diversen Geräten aus, damit sie Zuhause oder außerhalb des Büros effizienter arbeiten. Mit der größeren Freiheit gehen aber auch neue Herausforderungen einher: Die starke Ausbreitung von Geräten, die unterwegs oder Zuhause benutzt werden, macht es Mitarbeitern zunehmend möglich, illegale Software auf das Netzwerk ihrer Arbeitgeber herunterzuladen. Ihr Unternehmen ist jedoch immer noch für die auf Laptops installierte Software verantwortlich, da sie weiterhin eine Unternehmensressource sind. Das Gleiche gilt für PCs, die dem Arbeitgeber gehören, aber von Mitarbeitern Zuhause benutzt werden.

Alle Bestimmungen zur Internetnutzung, die Sie haben, müssen daher den Heimgebrauch von Unternehmenswerten mit einschließen.

## **Betrügerische Händler**

Es gibt eine kleine Minderheit von Software-Händlern, die die Regeln großzügig auslegen und wissentlich illegale Waren verkaufen. Da viele KMUs das IT-Management an externe Händler übergeben, ist es äußerst wichtig, die Autorisierung Ihres Software-Händlers zu prüfen.

Stellen Sie sicher, dass Ihr Software-Lieferant oder -Reseller Ihnen nachweisen kann, dass er die Software von autorisierten Vertriebskanälen erhält.

**Sie können die Autorisierung von Vertriebsmethoden leicht überprüfen, indem Sie Software-Hersteller direkt kontaktieren und sie fragen, wer eine Vertriebsberechtigung für ihre Produkte hat.**

## Verringerung der Risiken

Ihr Betrieb kann diverse Schritte unternehmen, um die Risiken zu minimieren, die von unlizenzierter Software ausgehen.

### Regelmäßige Prüfungen und effektive Gebrauchsbestimmungen

Hierbei geht es nicht um ein technologisches, sondern ein geschäftliches Problem, das häufig durch optimale Geschäftsverfahren gelöst werden kann. Bedenkt man die Risiken, so ist es wichtig, auf geschäftlicher Ebene für bestimmte Prozesse, die eingeführt werden sollen, Fremdhilfe in Anspruch zu nehmen.

Jedes Unternehmen sollte mindestens regelmäßig die auf seinen PCs installierte Software überprüfen und über Bestimmungen verfügen, die den Gebrauch der Unternehmenstechnologie durch die Mitarbeiter festlegen (einschließlich der Technologie, die Mitarbeiter Zuhause oder unterwegs nutzen, die aber dem Unternehmen gehört). Es sollte deutlich gemacht werden, dass diese Bestimmungen durchgesetzt werden. Involvieren Sie zudem die für das Personal zuständigen Mitarbeiter, um den Erfolg zu gewährleisten.

### Software Asset Management

Überraschenderweise hat ein Drittel aller KMUs noch nie etwas vom Software Asset Management gehört.<sup>7</sup>

Das Software Asset Management (SAM) ist eine Methodik, mit deren Hilfe Unternehmen Prozesse zur Optimierung ihrer Software-Investitionen definieren und implementieren. Das Software Asset Management ist flexibel genug für Unternehmen aller Größen und kann in jeder Entwicklungsstufe angewendet werden. Mit ihm kann ermittelt werden, wo Ihr Unternehmen den oben besprochenen Risiken ausgesetzt ist und es sorgt für den Einsatz von Prozessen, die verhindern oder es weniger wahrscheinlich machen, dass Sie solchen Risiken zum Opfer fallen.

SAM bringt Mitarbeiter, Prozesse und ggf. Technologie zusammen, um sicherzustellen, dass die Software-Werte so effektiv und effizient wie möglich verwaltet, geschützt und genutzt werden. Zudem werden Lizenzen und Gebrauch systematisch zurückverfolgt, ausgewertet und verwaltet. Der durch SAM erzielte Nutzen kann beträchtlich sein: Abgesehen davon, dass es Ihnen Ruhe und Gewissheit verschafft, kann es Betrieben auch dabei helfen, die IT-Ausgaben zu senken, da sie ihre Software-Erfordernisse, einschließlich neuer Software und Lizenz-Erweiterungen, genau planen und budgetieren können.

Sie können eine Reihe von Schritten unternehmen, um SAM in Ihrer Firma effektiv zu gestalten. Sie brauchen diese Elemente nicht alle von Anfang an einzubeziehen, denn jedes führt zu einigen Verbesserungen. Die Erkenntnis, dass Software ein äußerst wichtiger Unternehmenswert ist und ihre Verwaltung ein wichtiges Geschäftsanliegen, muss jedoch den Ausgangspunkt bilden.

<sup>7</sup>Quelle: GfK-NOP-Studie „Commercial Risk“ von 2007

## Acht Schritte zur Implementierung des Software Asset Managements:

### 1 Einbindung des gesamten Unternehmens

Die Implementierung des Software Asset Managements (SAM) bringt zweifellos einen beträchtlichen Kulturwandel mit sich. Daher muss unbedingt dafür gesorgt werden, dass sowohl die Geschäftsleitung als auch die Anwender der Software das Projekt unterstützen und die Notwendigkeit von SAM verstehen.

### 2 Ernennung eines Software Asset Managers

Wenn Sie niemanden haben, der für die gesamte Software des Unternehmens zuständig ist, ist es sehr schwierig, Ihre Software-Werte im Auge zu behalten. Diese Person muss nicht in der IT-Abteilung arbeiten, am besten geeignet aber ist, abhängig von der Größe Ihrer Organisation, der für die IT-Verwaltung zuständige Mitarbeiter (der daher am Software-Einkauf beteiligt ist). Wenn es bei Ihnen nur eine Person gibt, die für IT zuständig ist – was in kleineren Firmen häufig der Fall ist –, machen Sie es zu einem deutlichen und definierten Teil ihrer Stellenbeschreibung.

### 3 Überprüfung der aktuellen Software- und Lizenznutzung

Sie müssen eine Bestandsaufnahme Ihrer aktuellen Software-Vermögenswerte machen, um genau zu wissen, welche Software in Ihrem Unternehmen in Betrieb ist und welche Lizenzen Sie für diese Software benötigen.

Nur wenn Sie wissen, was für Software installiert ist, wie viele Computer Ihre Organisation hat und ob es Kopien von Programmen gibt, die vielleicht von Ihren Mitarbeitern installiert wurden, sind Sie in der Lage, potenzielle Risiken oder Probleme zu ermitteln und Maßnahmen dagegen zu ergreifen.

### 4 Erstellen einer SAM-Datenbank

Eine gute Datenbank zur Speicherung sämtlicher Informationen in Bezug auf Ihre Software ist unverzichtbar für den Erfolg Ihrer SAM-Strategie. Sie könnten ein Tabellenprogramm benutzen oder in etwas investieren, das für diese Aufgabe entworfen wurde. Wie Sie sich auch entscheiden, es wird von unschätzbarem Wert sein.



## 5 Zentralisierung der Beschaffung und Verteilung Ihrer Software

Wenn die Ausgaben für Software und die Verantwortung für deren Beschaffung nicht vollständig überblickt werden können, ist es fast unmöglich, den gesamten Nutzen von SAM zu realisieren.

## 6 Festlegen von Verfahren und Grundsätzen

Eine der besten Vorkehrungen ist, zu kontrollieren, wie Software in Ihr Unternehmen gelangt. Deutliche, nachdrückliche Grundsätze für Mitarbeiter, die festlegen, was erlaubt ist und was nicht, helfen, die Situation zu kontrollieren.

Wenn Sie dafür sorgen, dass die SAM-Strategien von den Mitarbeitern vollständig verstanden und angenommen werden, sind Sie einen Schritt weiter bei der Kontrolle des Umfelds, in dem Software in Ihre Organisation eingeführt wird.

## 7 Regelmäßige Kontrolle

Seien Sie sich bewusst, dass SAM ein kontinuierlicher Prozess ist und durch regelmäßige Prüfungen kontrolliert werden muss, damit es reibungslos und effizient funktioniert.

## 8 Hinzuziehen eines unparteiischen Beraters

Um Unternehmen zu helfen, die die Risiken unlizenzierter Software vermeiden möchten, stellt die Business Software Alliance auf seiner Website ([www.bsa.org](http://www.bsa.org)) ein Hilfsmittel zur Verfügung, das Ratschläge und Software-Management-Tools anbietet. Um mehr darüber zu erfahren, besuchen Sie bitte diese Website mit ihren nützlichen Tipps und Tools.



## Was tun bei einer möglichen Gefährdung?

Unternehmen sollten Software wie alle anderen kostbaren Vermögenswerte behandeln. Wenn Sie Maßnahmen ergreifen und die hier aufgeführten Vorschläge umsetzen, können Sie die mit illegaler Software verbundenen Risiken kontrollieren und die Vorteile eines effizienteren IT-Einsatzes nutzen.

Wenn Sie jedoch befürchten, dass Ihr Unternehmen durch illegale Software gefährdet ist, gibt es diverse Einrichtungen, an die man sich wegen Hilfe wenden kann. Reseller und Händler sollten die erste Anlaufstelle sein, um Ihre Fragen im Hinblick auf Software-Lizenzen zu beantworten.

Weitere, auf der BSA-Website zur Verfügung stehende Hilfsmittel sind:

1

### **Ein Software-Management- und Lizenzierungs-Leitfaden:**

Diese Broschüre kann in sieben Sprachen heruntergeladen werden und Unternehmen dabei helfen, Software-Management-Verfahren zu implementieren und Fragen hinsichtlich der ordnungsgemäßen Lizenzierung zu klären.

2

### **Eine Auflistung von Resource-Management-Anbietern:**

Eine Auflistung von Links zu bekannten Software-Händlern und -Beratern, die Unternehmen bei Lizenzierungsangelegenheiten und der Implementierung von Software-Management-Programmen unterstützen können.

## Führen Sie einen kostenlosen Online-Gesundheitscheck durch

Der Gesundheitscheck wurde von der BSA entwickelt, um Unternehmen effektiv beim Ermitteln, Kennenlernen und Verwalten ihrer IT-Vermögenswerte zu helfen.

Er kann in wenigen Minuten:

1. Eine Analyse Ihrer aktuellen Software-Management-Situation durchführen
2. Potenziell anfällige Bereiche aufzeigen
3. Verbesserungen vorschlagen
4. Einen maßgeschneiderten Prüfungsbericht für Ihre Unterlagen anfertigen

<http://global.bsa.org/healthchecktool>

## Anhang: Hauptergebnisse der Gfk-NOP-Studie

2007 hat die BSA eine europaweite Studie in Auftrag gegeben, die die Einstellung von KMUs hinsichtlich Software-Piraterie untersuchen sollte und ob bekannt ist, welche Risiken die Benutzung illegaler Software für ein Unternehmen birgt.

- 1 94% der europäischen KMUs gaben an, dass IT „sehr“ oder „recht“ wichtig ist für den erfolgreichen Betrieb ihres Unternehmens.
- 2 Ein Fünftel der in verschiedenen Ländern Europas (außer Russland) befragten Personen glaubt, dass der Gebrauch von unlizenzierter Software „keine Risiken“ birgt.
- 3 87% realisieren nicht, dass der Gebrauch illegaler Software sie anfälliger für Viren macht.
- 4 97% betrachten es nicht als Problem, alte Software-Versionen zu benutzen, da illegale Versionen nicht aktualisiert werden können.
- 5 23% der Befragten nannten „Strafverfahren“ als größtes Risiko, gefolgt von „Geldstrafen“ (21%). Nur 3% gaben an, dass „der Betrieb von alten Versionen/ die Unfähigkeit zu aktualisieren“ ein Risiko wäre – trotz der wirtschaftlichen Bedrohung durch Wettbewerber mit den neuesten Lösungen.

- 6 KMUs in Mittel- und Osteuropa sowie in Russland verwiesen jedoch doppelt so oft auf „Datenverlust/-beschädigung“ als Risiko durch unlicenzierte Software im Vergleich zu westeuropäischen Betrieben. Zudem sehen 27% der Befragten in Russland „Software-Versagen“ als Risiko, aber nur 8% der Geschäftsleute in Westeuropa teilten diese Ansicht.
- 7 Größere KMUs (100-250 Mitarbeiter) haben häufiger einen Vorgang zur Verwaltung der benutzten Software (37%) als kleinere KMUs (19%).
- 8 Insgesamt sind „regelmäßige Prüfungen der Mitarbeiter-PCs“ die bevorzugte Methode, den Software-Gebrauch zu kontrollieren und zu verwalten (33%), gefolgt von einer „Unternehmensrichtlinie“ (25%).

## Die Studie

Diese Studie wurde im Auftrag der BSA von der GfK NOP telefonisch bei 1.800 kleinen und mittelgroßen Unternehmen in Europa durchgeführt und zwar in Großbritannien, Frankreich, Deutschland, den Niederlanden, Italien, Spanien, Russland, Polen und Ungarn.

In jeder Region wurden 200 Befragungen durchgeführt. Für die Zwecke dieser Studie wurden Unternehmen mit 10 bis 250 Mitarbeitern als KMUs bezeichnet.



#### **BSA Worldwide Headquarters**

1150 18th Street, NW  
Suite 700  
Washington, DC 20036  
USA  
Tel: +1 202 872 5500  
Fax: +1 202 872 5501

#### **BSA Europe, Middle East & Africa**

2 Queen Anne's Gate Buildings  
Dartmouth Street  
London SW1H 9BP  
Großbritannien  
Tel: + 44 (0) 20 7340 6080  
Fax: + 44 (0) 20 7340 6090

#### **BSA Asia-Pacific**

300 Beach Road  
#25-08 The Concourse  
Singapore 199555  
Tel: + 65 6292 2072  
Fax: + 65 6292 636

<http://www.bsa.org>

Die Business Software Alliance (BSA) ist die Stimme der Softwarebranche und ihrer Hardware-Partner gegenüber Regierungen und Kunden auf dem globalen Markt. Ihre Mitglieder stellen einen der am schnellsten wachsenden Industriezweige der Welt dar. Die BSA unterstützt durch ihre politischen und informativen Initiativen die technologische Innovation in den Bereichen Urheberrecht, Internet-Sicherheit, Handel und E-Commerce.

BSA, Business Software Alliance und das BSA-Logo sind Warenzeichen der Business Software Alliance Incorporated und können in bestimmten Rechtsgebieten geschützt sein.  
© 2007 Business Software Alliance. Alle Rechte vorbehalten.