

# Outsourcing – eine Frage der Sicherheit

**In vielen IT-Abteilungen regiert derzeit der Rotstift, da die Auswirkungen der aktuellen Krise an den Finanzmärkten auf die reale Wirtschaft nicht ausbleiben. Das Thema Outsourcing bekommt dadurch erneut Rückenwind: In Boomzeiten gilt es als gute Möglichkeit, um Zugang zu neuen Technologien und Ressourcen zu erhalten und in Krisenzeiten gilt Outsourcing als Kostensenker. Dabei ist kaum ein Thema gleichzeitig so umstritten. Gernot Keckeis, Director Identity & Security bei Novell, und Michael Junk, IT-Security & Compliance Manager bei Novell, untersuchen, welche Vorteile die Auslagerung von einzelnen Geschäftsprozessen mit sich bringen kann und welche Hürden gemeistert werden müssen:**

Zahlreiche gesetzliche Vorschriften und der zunehmende Druck von Finanzmärkten stellen IT-Entscheider vor neue Herausforderungen, denn die IT-Systeme und Geschäftsprozesse in den Unternehmen müssen den komplexen rechtlichen Rahmenbedingungen entsprechen. Zudem machen neue Anforderungen an Corporate Governance und Compliance auch um Outsourcing-Dienstleistungen keinen Bogen. Die ideale Form des Outsourcing ist individuell verschieden, aber durch die Orientierung an Fragen nach den gesetzlichen Regelungen und Richtlinien, deren praktischer Umsetzung, den Standards und Zertifikaten, die sich im Markt durchgesetzt haben sowie an Referenzmodellen lässt sich das jeweils ideale Modell besser eingrenzen.

Auslöser für eine Entscheidung zum Outsourcing bilden oft kurzfristige Kapazitätsengpässe oder Kostenprobleme. Das greift jedoch zu kurz: Informationstechnische und unternehmerische Aspekte wie zum Beispiel Stabilität, Sicherheit, Funktionalität, Verfügbarkeit, Zuverlässigkeit, Flexibilität oder Pflege von Informationssystemen und Daten müssen ebenfalls berücksichtigt werden. Weitere potenzielle Risiken wie Umweltbedrohungen, der Ausfall von Mitarbeitern, externe Abhängigkeiten und andere Gefahren von innen (Netzausfälle) und außen (Anschläge, Diebstähle) müssen bei der Entscheidung eine Rolle spielen.

Daher ist es unerlässlich, die kritischen Bereiche im Sicherheitsprozess genau unter die Lupe zu nehmen und zu dokumentieren. Denn auch nach dem Outsourcing muss das Unternehmen als Ganzes noch funktionieren und in der Lage sein, für das Thema Ausfall und Datenschutz die Anforderungen seitens des Gesetzgebers zu erfüllen. Auch das Thema IT-Compliance und die Einhaltung von gesetzlichen Regelungen sollten beim Outsourcing nicht zu kurz kommen. Generell sind die Schwachstellen der IT Sicherheit heute eher in der stark vernetzten Leistungserbringungskette zu suchen, als in nicht funktionsfähigen Firewalls. Um den enormen Sicherheitsanforderungen gerecht zu werden, ist es empfehlenswert, nach dem Ansatz „Plan, Do, Check and Act“ vorzugehen. Unter „Plan“ fallen dabei Aspekte, wie die Definition des

Geltungsbereiches, Definition und Auswahl der Informationssicherheitspolitik (IS – Politik) sowie die Definition eines systematischen Ansatzes für den Umgang mit Risiken. Außerdem erfolgt in dieser Phase die Übernahme der Restrisiken durch das Management sowie die Freigabe der Einführung und des Betriebs des ISMS.

Die Umsetzung ('Do') beginnt idealerweise mit der Definition und Implementierung eines Risikobehandlungsplans, der Aktionen, Verantwortungen, Rollen und Prioritäten in Bezug auf IS-Risiken beschreibt. Dann folgt die praktische Umsetzung der ausgewählten IS-Maßnahmen sowie der Trainings- und Awareness-Programme. Außerdem werden Verfahren eingeführt, um auf sicherheitsrelevante Vorfälle möglichst schnell reagieren zu können.

In der Check-Phase folgt die Ausführung der Überwachungsverfahren und –maßnahmen. Hinzu kommen regelmäßige Sicherheitsaudits, die Überprüfung des Niveaus von Restrisiken und tragbaren Risiken sowie die Durchführung interner ISMS-Audits und Management-Reviews. Außerdem werden sicherheitsrelevante Aktivitäten und Ereignisse aufgezeichnet.

In der vierten Phase 'Act' folgt die Definition, Implementierung und Überwachung von Korrektur- und Vorbeugungsmaßnahmen. Erkenntnisse aus Sicherheitsvorfällen der eigenen oder fremden Organisationen werden angewandt und die ISMS-Aktivitäten und – Ergebnisse werden im regelmäßigen Austausch mit allen Beteiligten kommuniziert.

Das zeigt: Die Implementierung eines funktionsfähigen Sicherheits- und Risikomanagementsystems geht mit einem kontinuierlichen Verbesserungsprozess einher. Die Implementierung eines Regelkreislaufes ist notwendig, um heute die notwendige IT Sicherheit und ein dem Risiko angemessenes Managementsystem für das Outsourcing aufzusetzen.

Zu beachten ist auch, dass die Qualität der ausgelagerten Prozesse nur indirekt durch den Auftraggeber beeinflusst werden kann. Die sorgfältige Auswahl des Dienstleisters sollte daher hohe Priorität haben. Je nach dem welche Prozesse ausgelagert werden, kann nicht nur die weitere Arbeit im Unternehmen, sondern auch das Image nach außen betroffen sein.

Sicher der wichtigste Punkt während eines Auslagerungs-Prozesses ist die zeitnahe und offene Kommunikation mit den betroffenen Mitarbeitern. Werden diese nicht umfassend und zeitnah informiert, kann dies zu Gerüchten und Szenarien führen, welche die Umsetzung des Vorhabens erschweren oder gar gefährden können. Change Management und interne Kommunikation müssen also gut geplant und umgesetzt werden.

Hält ein Unternehmen bei der Umsetzung diese Regeln ein, so hat Outsourcing folgende Vorteile: Die Konzentration auf die Kernkompetenzen ist wieder möglich und Geschäftsprozesse werden rationeller. Die Gesamtbetriebskosten sinken und lassen sich besser kalkulieren. Auslagerungen können Unternehmen zudem flexibler und mobiler machen, da sie schneller auf Veränderungen reagieren und wachsen können. Außerdem werden keine Mittel durch Investitionen gebunden und das Kreditrating verbessert sich.

Aber auch die Nachteile einer Auslagerung müssen klar sein: Vor allem das Outsourcing von

Schlüsselprozessen birgt Risiken durch entstehende Abhängigkeiten, wenn beispielsweise ein externer Zulieferer sich als unzuverlässig herausstellt. Wichtiges Know-how kann verloren gehen. Auch die Abgrenzung vom Mitbewerber, der auf denselben Dienstleister zurückgreifen kann, wird schwieriger. Die erwarteten Kostenvorteile treffen zudem mittel- und langfristig nicht immer ein.

### **Über Novell:**

Novell, Inc. (Nasdaq: NOVL) bietet eine Linux-Plattform, die für die nahtlose Integration in verschiedenste Plattform- und Anwendungsumgebungen konzipiert ist, sowie ein Portfolio an integrierter IT-Management-Software, mit der Unternehmen weltweit Kosten, Komplexität und Risiken reduzieren können. Mit dieser Infrastruktur-Software und einem umfassenden Partnernetzwerk verbindet Novell heterogene IT-Umgebungen und ermöglicht so, dass Menschen und Technologie als eine Einheit zusammenarbeiten. Weitere Informationen unter [www.novell.com](http://www.novell.com).

### **Pressekontakt**

Ulrike Beringer

Novell GmbH

Telefon: +49 (0) 89 / 28 673 850

eMail: [uberinger@novell.com](mailto:uberinger@novell.com)

Saskia Stolper

Hotwire

Telefon: +49 (0) 69 / 25 66 93-50

eMail: [saskia.stolper@hotwirepr.com](mailto:saskia.stolper@hotwirepr.com)