Outsourcing unter Sicherheitsaspekten - wie kann das aussehen?

Michael Mehrhoff, Isabel Münch

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn
michael.mehrhoff@bsi.bund.de
isabel.muench@bsi.bund.de

Abstract: Outsourcing gewinnt im Rahmen der Verschlankung von Behörden und Unternehmen und der Konzentration auf Kernkompetenzen an Bedeutung. Sicherheitsgesichtspunkte werden dabei leider zu wenig berücksichtigt. Im Rahmen des Vortrages wird dargestellt, welche Kriterien eine Institution bei der Entscheidung über das Outsourcing von internen Prozessen und bei der Durchführung von Outsourcing-Vorhaben berücksichtigen sollte, um das Sicherheitsniveau nicht zu verwässern, sondern im Idealfall sogar zu verbessern.

1 Einleitung

Beim Outsourcing werden Arbeits- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert. Outsourcing kann sowohl Nutzung und Betrieb von Hardware und Software, aber auch Dienstleistungen betreffen. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Applikation, einer Webseite oder des Wachdienstes.

Das Auslagern von Geschäfts- und Produktionsprozessen ist ein etablierter Bestandteil heutiger Organisationsstrategien. Speziell in den letzten beiden Jahrzehnten hat sich der Trend zum Outsourcing enorm verstärkt und dieser scheint auch für die nächste Zukunft ungebrochen.

Die hierfür angeführten Gründe sind vielfältig: So kann sich die Organisation auf ihre Kernkompetenzen konzentrieren, Kosten sparen, auf spezialisierte Kenntnisse und Ressourcen zugreifen, interne Ressourcen für andere Aufgaben freisetzen, die interne Verwaltung straffen, die Geschäfts- und Produktionsprozesse besser skalieren und die Flexibilität sowie die Wettbewerbsfähigkeit erhöhen.

Zunehmend lässt sich in der Praxis jedoch erkennen, dass schlecht vorbereitete Outsourcing-Projekte zu Problemen führen. Die Computerwoche 23/2003 führt dazu Folgendes aus: "Die Marktforscher von Gartner schätzen, dass allein in Westeuropa im vergangenen Jahr rund sechs Milliarden Euro mit fehlgeschlagenen Outsourcing-Vorhaben in den Sand gesetzt wurden."

Beim Outsourcing von IT-gestützten Organisationsprozessen werden die IT-Infrastrukturen der auslagernden Organisation und ihres Outsourcing-Dienstleisters in der Regel eng miteinander verbunden, so dass Teile von internen Geschäftsprozessen unter Leitung und Kontrolle eines externen Dienstleisters ablaufen. Ebenso findet auf personeller Ebene ein intensiver Kontakt statt. Damit steigen die Risiken, dass bei dieser Anbindung beispielsweise sensitive Organisationsinformationen gewollt oder ungewollt nach außen preisgegeben werden und dadurch unter Umständen sogar die Geschäftsgrundlage des Unternehmens oder der Behörde vital gefährdet werden kann. Sicherheitsaspekte und die Gestaltung vertraglicher Regelungen zwischen Auftraggeber und Outsourcing-Dienstleister spielen im Rahmen eines Outsourcing-Vorhabens somit eine zentrale Rolle.

2 Sicherheitsprobleme beim Outsourcing

Bei Outsourcing-Vorhaben können eine Vielzahl von Sicherheitsproblemen parallel auf physikalischer, technischer und auch menschlicher Ebene auftreten, die nicht nur die ausgelagerte Anwendung, sondern unter Umständen die ganze Organisation betreffen können. Outsourcing ist immer eine Entscheidung über die strategische Ausrichtung der Organisation, ihre Kernkompetenzen, die Wertschöpfungskette und viele weitere wesentliche Belange eines Organisationsmanagements.

Zwei typische Outsourcing-Probleme sind, dass häufig einerseits eine Outsourcing-Strategie gar nicht existiert oder lücken- bzw. fehlerhaft ist, und andererseits, dass sich im Konfliktfall die vorhandenen vertraglichen Regelungen (Service Level Agreements) mit dem Outsourcing-Dienstleister als unzulänglich erweisen.

Beim Auslagern von Aufgaben entsteht (insbesondere bei einer engen Verbindung der jeweiligen IT-Infrastrukturen) grundsätzlich immer eine Abhängigkeit vom Dienstleister. Die entscheidende Frage ist, wie tief diese geht und ob sich der Auftraggeber daraus wieder lösen kann: Problematisch sind hier vor allem, dass ein Know-how-Verlust kaum zu vermeiden ist, die Mitarbeiterfluktuation häufig steigt und Systeme und Ressourcen an den Outsourcing-Dienstleister übertragen werden.

3 Sicherheitsmaßnahmen

Um ein angestrebtes Outsourcing-Vorhaben sicher durchzuführen, sind verschiedene Schritte zu durchlaufen, die im Folgenden kurz dargestellt sind.

Strategische Planung des Outsourcing-Vorhabens

Schon im Rahmen der strategischen Entscheidung, ob und in welcher Form ein Outsourcing-Vorhaben umgesetzt wird, müssen die sicherheitsrelevanten Gesichtspunkte herausgearbeitet werden. Zunächst ist zu klären, welche Aufgaben oder IT-Anwendungen überhaupt für Outsourcing in Frage kommen. Zu beachten sind dabei die grundsätzliche Unternehmensstrategie (Flexibilität, Abhängigkeit), betriebswirtschaftliche Aspekte und rechtlichen Rahmenbedingungen.

Zur Abschätzung aller Vorteile und Nachteile sollte schon in der Planungsphase eine Sicherheitsanalyse zur Identifikation von notwendigen Sicherheitsmaßnahmen durchgeführt werden. Dabei kann sich auch herausstellen, dass es Aufgaben gibt, die aus Sicherheits- oder Kostengründen nicht ausgelagert werden sollten.

Definition der wesentlichen Sicherheitsanforderungen

Wenn die Entscheidung zum Outsourcing gefallen ist, müssen die wesentlichen übergeordneten Sicherheitsanforderungen als Basis für das Ausschreibungsverfahren festgelegt werden.

Auswahl des Outsourcing-Dienstleisters

Der entscheidende Punkt für eine gelungene Ausschreibung ist ein möglichst detailliertes Anforderungsprofil und ein darauf basierendes Pflichtenheft. Neben Aufgabenbeschreibung und Aufgabenteilung müssen auch die Sicherheitsanforderungen, die Festlegung des Qualitätsniveaus und die Kriterien zur Messung von Servicequalität und Sicherheit wichtige Punkte im Auswahlverfahren sein.

Vertragsgestaltung

Auf Basis des Pflichtenheftes muss nun ein Vertrag mit dem Partner ausgehandelt werden, der die gewünschten Leistungen inklusive Qualitätsstandard und Fristen im Einklang mit der vorhandenen Gesetzgebung festschreibt. In diesem Vertrag müssen auch die genauen Modalitäten der Zusammenarbeit geklärt sein: Ansprechpartner, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistungen, Ausgestaltung der IT-Sicherheitsvorkehrungen, Umgang mit vertraulichen Informationen, Verwertungsrechte, Weitergabe von Information an Dritte etc. Probleme treten häufig dann auf, wenn nicht festgelegt wird, wer für die Auswahl und Umsetzung von IT-Sicherheitsmaßnahmen verantwortlich ist.

Erstellung eines Sicherheitskonzepts für den ausgelagerten IT-Verbund

Ein ausgelagerter IT-Verbund kann sowohl aus Komponenten bestehen, die sich ausschließlich im Einflussbereich des Outsourcing-Dienstleisters befinden, als auch aus Komponenten beim Auftraggeber. In der Regel gibt es in diesem Fall Schnittstellen zur Verbindung der Systeme. Für jedes Teilsystem und für die Schnittstellenfunktionen muss die IT-Sicherheit gewährleistet sein. Daher müssen Auftraggeber und Outsourcing-Dienstleister in enger Zusammenarbeit ein detailliertes Sicherheitskonzept erstellen.

Der Auftraggeber ist normalerweise nicht direkt an der Erstellung des Sicherheitskonzepts des Outsourcing-Dienstleisters beteiligt, sollte aber in einem Audit prüfen lassen, ob es vorhanden und ausreichend ist. Dabei sollten spezielle Sicherheitsmaßnahmen für die Test- und Einführungsphase vorgesehen sein.

Planung der Migrationsphase

Besonders sicherheitskritisch ist die Migrationsphase, die deshalb eines sorgfältigen Migrationskonzeptes bedarf, das insbesondere die Einrichtung eines funktionierenden IT-Sicherheitsmanagements beim Auftraggeber umfassen muss. Besonders zu Testzwecken und in Phasen großer Arbeitsbelastung werden gerne "flexible" und "unkomplizierte" Lösungen gewählt, die selten sehr sicher sind. Es ist daher beispielsweise sicherzustellen, dass produktive Daten nicht ohne besonderen Schutz als Testdaten verwendet werden. Dies muss durch das IT-Sicherheitskonzept ausgeschlossen werden. Dem Sicherheitsmanagement kommen u. a. folgende Aufgaben zu:

- Es sollte ein gemischtes Sicherheitsmanagement-Team gebildet werden, bestehend aus Mitarbeitern von Auftraggeber und Outsourcing-Dienstleister.
- Zuständigkeiten und Kompetenzen müssen festgelegt werden, dabei ist es wichtig, eine klare Führungsstruktur und eindeutige Ansprechpartner auf beiden Seiten zu benennen.
- Die Tests und deren Durchführung, Abnahmeprozeduren sowie die Produktionseinführung müssen geplant werden.
- Die Anwendungen und Systeme, die der Dienstleister übernehmen soll, müssen dokumentiert werden.

Sicherstellung des laufenden Betriebs

Wenn der Outsourcing-Dienstleister die Systeme bzw. Geschäftsprozesse übernommen hat, sind verschiedene Maßnahmen zur Aufrechterhaltung der IT-Sicherheit im laufenden Betrieb notwendig wie regelmäßige Kontrollen und Durchführung von Systemwartungen.

Schlussbetrachtungen

Durch Outsourcing wird weder automatisch das vorhandene Sicherheitsniveau untergraben noch verbessert. Um sicher und erfolgreich betrieben zu werden, benötigt Outsourcing ganz bestimmte Rahmenbedingungen. Hierzu muss das Vorhaben vor allem in allen Facetten durchdacht, die Sicherheitsanforderungen bestimmt und die zu ergreifenden Sicherheitsmaßnahmen festgelegt werden.

Es gibt allerdings auch Situationen, in denen aus Sicherheitsgründen kein Outsourcing betrieben werden sollte, beispielsweise wenn aus organisatorischen oder rechtlichen Gründen keine ausreichenden Kontrollen der externen IT-Systeme und Mitarbeiter durchführbar sind.