IT-Outsourcing? Aber sicher!

Secorvo White Paper

Eine Checkliste

Version 1.0
Stand 01. Juli 2002

Ingmar Camphausen, Dr. Volker Hammer, Stefan Kelm,
Dr. Dörte Neundorf, Dr. Holger Petersen

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Inhaltsübersicht

Abkürzungen

GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
IT	Informationstechnik (Informations- und Kommunikationssysteme)
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
SLA	Service-Level Agreement

1 IT-Outsourcing? Aber sicher!

Das aus der amerikanischen Managementpraxis stammende Kunstwort Outsourcing setzt sich aus den Bestandteilen *outside*, *resource* und *using* zusammen. Im Kern beschreibt der hinter dem Begriff "Outsourcing" stehende Sachverhalt die betriebswirtschaftliche Frage nach dem "make-or-buy". Welche Leistungen werden mit den im eigenen Unternehmen vorhandenen Ressourcen erstellt, und welche werden von externen Anbietern bezogen? Outsourcing ist somit die langfristig ausgerichtete Externalisierung bestimmter Teilleistungen oder Funktionen einer Unternehmung und deren Übernahme durch externe Dienstleister. Entsprechend der Maxime "do what you can do best – outsource the rest" werden Aufgaben, die nicht zu den Kernkompetenzen eines Unternehmens gehören, ausgelagert und die entsprechenden Leistungen von darauf spezialisierten Dienstleistern bezogen.

Für das Outsourcing von IT-Leistungen eines Unternehmens können viele Gründe sprechen, so z.B. die Vermeidung hoher einmaliger Anschaffungskosten für Hard- und Software, die Verringerung der Betriebs- und Implementierungskosten, eine Verbesserung der IT-Qualität durch die Spezialisierung des Dienstleisters, eine flexiblere Skalierbarkeit oder kürzere Innovationszyklen.

Grundsätzlich gilt: Outsourcing verändert die IT-Situation in jedem Unternehmen. Dies betrifft auch die Sicherheit der IT-Systeme und -Anwendungen. Daher müssen zur Gewährleistung der erforderlichen Sicherheit bei IT-Outsourcing zusätzliche Aspekte beachtet werden, die bei Eigenbetrieb der IT-Infrastruktur keine oder nur eine untergeordnete Rolle spielen. Dies sind Maßnahmen zur Sicherung der Vertraulichkeit und Authentizität von Daten, aber auch Schritte zur Gewährleistung der erforderlichen Verfügbarkeit, zur Einhaltung der gesetzlichen Vorgaben und zur Qualitätssicherung der outgesourcten Dienstleistungen.

Diese Checkliste möchte Ihnen daher helfen, bei der Entscheidung für das Outsourcing Ihrer IT-Systeme und bei dessen Umsetzung diese sicherheitsrelevanten Punkte adäquat zu berücksichtigen. Damit kann neben den Zielen des Outsourcings, wie der Erhöhung der Effizienz oder Funktionalität, auch die Sicherheit Ihrer Systeme dauerhaft gewährleistet werden.

Besonders wichtig sind die folgenden strategischen Aspekte:

- Die Verankerung der IT-Sicherheit sollte (wie die Grundkonzeption vieler anderer Bereiche) weiterhin bei Ihnen als Auftraggeber verbleiben. Dies umfasst zumindest die Rahmenvorgaben und die Kontrolle der Einhaltung dieser Vorgaben, ggf. auch die Konzeption von Kernelementen.
- Zuständigkeiten und Eskalationswege müssen klar definiert sein. Sie sollten konzeptionell festgelegt und danach praktisch etabliert und getestet werden. Dabei ist auch die Festlegung genauer Prozesse zum Change Management zu beachten, wenn sich sicherheitsrelevante Prozesse oder Ansprechpartner ändern.
- Zu klären ist die Frage, inwieweit die Verankerung der Verantwortung für die IT-Sicherheit für Ihre Kunden eine Rolle spielt. Schadet es dem Vertrauen zwischen Ihnen und Ihren Kunden, wenn Sie die Absicherung Ihrer Daten Dritten überlassen? Könnte dies zu einem Wettbewerbsvorteil für Mitbewerber führen, die die Datenhaltung selbst betreiben? Oder ist es ein Marktvorteil für Sie, wenn Ihre Systeme von einem „Profi“ betrieben werden?
- Schließlich sollte eine Verankerung aller sicherheitsrelevanten Absprachen im Vertrag oder im Service Level Agreement (SLA) erfolgen. Dort sollte insbesondere auch geklärt

werden, inwieweit der Unterauftragnehmer bei Verstößen gegen die Vereinbarungen und durch Mängel verursachte Schäden haftet.

In den nächsten Abschnitten haben wir sicherheitsspezifische Fragen, die relevant für Outsourcing sein können, als Checkliste zusammengestellt. Nicht alle Punkte treffen auf jedes Unternehmen und jedes Outsourcing-Projekt zu; die Liste gibt jedoch einen Überblick über wichtige Punkte, um Ihnen eine Auswahl der für Sie relevanten Aspekte zu ermöglichen.

2 Outsourcing-Konzeption unter Sicherheitsaspekten

2.1 Sicherheitskonzept

Das von Ihnen vorgegebene Sicherheitsniveau kann nur erreicht werden, wenn Ihr Dienstleister ein durchgängiges Sicherheitskonzept besitzt und dieses auch umgesetzt wird. Daher sind u.a. die folgenden Fragen zu klären:

- Wie werden Ihre Sicherheitskonzepte und die Ihres Dienstleisters vereinheitlicht und zusammengeführt?
- Wie wird gewährleistet, dass alle Systeme (bei Ihnen, beim Dienstleister, ggf. bei Unterauftragnehmern Ihres Dienstleisters) im Sicherheitskonzept berücksichtigt sind?
- Wie werden Sicherheitsniveaus definiert, die auf alle beteiligten Systeme anwendbar sind? Wer definiert Vorgaben für die Umsetzung?
- Welche Art von Sicherheitsdienstleistungen soll Ihr IT-Dienstleister erbringen?
  - Schutz Ihrer Systeme (z.B. durch Firewalls)
  - Sicherung der Kommunikationsverbindungen zwischen Ihnen und Ihrem Dienstleister
  - Besonderer Schutz von bestimmten Daten und Informationen
  - Besondere Sicherheitsanwendungen (z.B. Verschlüsselung, Digitale Signatur, Authentisierung)
  - Maßnahmen als Reaktionen auf sicherheitsrelevante Vorfälle, z.B. Hacker-Angriffe, oder die Entdeckung von Sicherheitslücken in kritischen (Betriebssystem-) Anwendungen.
  - Prozesse und Systeme, die die reaktiven Dienstleistungen unterstützen, z.B. Intrusion-Detection-Systeme
  - Weiterführende Prozesse zur Erhöhung der IT-Sicherheit, z.B. regelmäßige Risikoanalyse oder Produktevaluation, Pflege der Sicherheitskonzepte und -maßnahmen
- Wie, von wem und wie häufig wird die Umsetzung der im Sicherheitskonzept definierten Sicherheitsmaßnahmen überprüft?
- Werden Teile der Leistungen vom Dienstleister bei Unterauftragnehmern eingekauft? Falls ja, wie wird deren Berücksichtigung im Sicherheitskonzept und die Umsetzung der Vorgaben überprüft?

Beim Outsourcing von IT-Dienstleistungen kann die Forderung eines IT-Grundschutz-Audits der IT-Systeme des Dienstleisters sinnvoll sein, um ein Mindestmaß an Sicherheit zu gewährleisten. Da IT-Grundschutz-Audits in regelmäßigen Zeitabständen wiederholt werden müssen, empfiehlt sich, diese Forderung vertraglich zu vereinbaren.

2.2 Verantwortlichkeit für Sicherheitsaufgaben

Die Verantwortlichen für die IT-Sicherheit im Unternehmen und beim Dienstleister (Sicherheitsbeauftragter, Leiter IT-Sicherheit, Firewalladministrator etc.) müssen nach Möglichkeit persönlich benannt sein. Alle Beteiligten – und das schließt die Mitarbeiter Ihres Unternehmens *und* des Dienstleisters ein. Sie müssen die Prozesse kennen und sie in der täglichen Praxis umsetzen, um die Sicherheit ihrer IT-Systeme gewährleisten zu können. Im Detail sind folgende Fragen zu beantworten.

- Wer ist für die Gewährleistung der Sicherheit zuständig? Weiterhin Sie selbst oder der Dienstleister? Wer muss auf Sicherheitslücken und Probleme reagieren? Wer überwacht die Systeme? Wer prüft regelmäßig die getroffenen Maßnahmen auf Konsistenz und Wirksamkeit?
- Wie werden Reaktionsmöglichkeiten bei Störfällen sichergestellt, die der möglicherweise erschwerten unmittelbaren Kommunikation zwischen dem Anwender (der das Problem feststellt), dem externen IT-Betrieb und den internen Verantwortlichen Rechnung tragen?
- Gibt es eine klare Bennennung von Ansprechpartnern des externen Dienstleisters für alle Belange? Wie werden diese Kontakte im Unternehmen bekannt gemacht (initial, bei Änderungen)?
- Wer definiert die Vorgaben – z.B. das zu ereichende Sicherheitsniveau oder die Behandlung von als vertraulich klassifizierten Daten? (Vermutlich ist es hier meist sinnvoll, wenn Sie diese Aufgabe übernehmen und dem Dienstleister geeignete Vorgaben machen.)
- Wer erstellt die Sicherheitskonzepte und Handlungsanweisungen? Sie selbst, damit sie zu Ihrer Unternehmensphilosophie und der internen Struktur passen? Oder der Dienstleister, der aufgrund seiner Erfahrung möglicherweise schneller ein sachgerechtes Konzept erstellen kann?
- Wer kontrolliert die Einhaltung Ihrer Vorgaben? Sie selbst, der Dienstleiter oder ggf. eine dritte Stelle, z.B. ein Prüfunternehmen?

2.3 Know-How-Transfer

Um IT-Sicherheit in Ihrem Unternehmen zu gewährleisten, bedarf es entsprechender Fachkenntnis der relevanten Standards, Systeme, Tools und Applikationen. Die erforderliche Fachkenntnis können Ihre Mitarbeiter auf Dauer nur behalten, wenn IT-Sicherheit Teil der täglichen Praxis bleibt. Daher sind u.a. folgende Punkte zu klären:

- Wird durch das Outsourcing wichtiges IT-Sicherheits-Know-How in Ihrem Unternehmen abgebaut? Wird dadurch die Reaktionsfähigkeit auf sicherheitsrelevante Vorfälle (Ausfälle, Angriffe etc.) kritisch beeinträchtigt?
- Wie wird das bei Ihnen vorhandene Know-How geeignet zum IT-Dienstleister transferiert, um – insbesondere bei Ihren Spezialanwendungen – Sicherheitslücken aufgrund von Fehlern im Betrieb und in der Administration zu vermeiden?

- Wie kann IT-Sicherheits-Know-How bei einem Wechsel des Dienstleisters so transferiert werden, dass ein ununterbrochener Betrieb mit angemessenem Sicherheitsniveau auch während der Übernahme gewährleistet ist?

2.4 Gesetzliche Vorgaben

In der Regel müssen Sie mit ihren IT-Systemen gesetzliche Vorgaben erfüllen; die Verantwortung für die Erfüllung dieser Vorgaben ist dabei oft nicht delegierbar.

Zu diesen Anforderungen zählen z.B.

- Pflichten gegenüber den Finanzbehörden (Abgabenordnung, GoBS, GDPdU),
- die Pflicht der Unternehmensleitung gemäß KonTraG, ein System zur Risiko-Früherkennung und –vorsorge zu etablieren, das es ermöglicht, existenzgefährdende Risiken – gerade auch beim Einsatz der Unternehmens-IT – rechtzeitig zu erkennen und abzuwenden und
- die Gesamtverantwortung gemäß der Datenschutzgesetze für die „Verarbeitung personenbezogener Daten im Auftrag".

Um eine korrekte Umsetzung sicherzustellen, ist es sinnvoll, alle wesentlichen Rahmenbedingungen vorab zusammenzustellen und deren Umsetzung mit dem Dienstleister abzustimmen.

Durch Sie als Auftraggeber muss unter Umständen eine regelmäßige Kontrolle erfolgen, damit Sie Ihren gesetzlichen Verpflichtungen gerecht werden. Daher sollten Sie von vornherein darauf achten, dass entweder interne Mitarbeiter mit entsprechender Qualifikation für solche Prüfungen zur Verfügung stehen oder Sie einen zweiten unabhängigen Dienstleister damit beauftragen können.

2.5 Notfall-Konzept

Um im Falle eines erfolgreichen Angriffs auf Ihre IT-Systeme schnell und angemessen reagieren zu können, sollte für Ihre IT-Systeme ein Notfall-Konzept existieren, das die Verantwortlichkeiten und Eskalationsschritte bei einem Störfall definiert. Im Detail sollte es u.a. Antworten auf folgende Fragen enthalten.

- Wer ist für die Erstellung, für die Pflege und den Test des Notfallkonzept zuständig? Wie erfolgt (sofern erforderlich) eine Aufteilung der Zuständigkeiten?
- Gibt es definierte Abläufe zum Wiederaufbau der IT nach einer großen Störung (z.B. Brand im Rechenzentrum)? Wer ist dafür zuständig?
- Sind klare Eskalationswege/-prozesse festgelegt und etabliert?
- Genügt das Notfallkonzept Ihrer Risikoanalyse und den daraus abgeleiteten Vorgaben (maximale Ausfallzeiten für IT-Systeme wichtiger Geschäftsprozesse, Leistungsumfang von Ad-hoc-Ersatzsystemen etc.)?
- Sind Reporting-Pflichten des Dienstleisters festgelegt, die die Zusicherung bestimmter Benachrichtigungszeiten die Bereitstellung bestimmter Protokolldaten beinhalten?
- Wird durch regelmäßige Tests die Funktionsfähigkeit der Notfallkonzepte überprüft?
- Wird das Notfallkonzept in regelmäßigen Abständen auf seine Vollständigkeit, Angemessenheit und Aktualität überprüft?

2.6 Audit des Dienstleisters

Eine regelmäßige Überprüfung der Qualität der erbrachten Dienstleistung sollte von vornherein Bestandteil des Outsourcing-Konzepts sein. Eine sinnvolle Methode für eine solche Prüfung ist die regelmäßige Durchführung eines Audits.

Ziel eines (Sicherheits-) Audits ist es, die Wirksamkeit und korrekte Umsetzung vorhandener technischer und organisatorischer Sicherheitsmaßnahmen zu überprüfen und dabei bestehende Schwachstellen aufzudecken.

Ein solches Audit sollten Sie regelmäßig entweder selbst oder durch einen unabhängigen Dritten beim Dienstleister durchführen (lassen). Das Audit sollte von einem Team durchgeführt werden, das nicht in irgendeiner Form mit dem Betrieb der Systeme vertraut ist, um „Betriebsblindheit“ zu vermeiden.

Vorab zu klären sind die folgenden Punkte:

- Wie wird das Audit/die Kontrolle des Dienstleisters gestaltet? Wie häufig und wie detailliert wollen (und können) Sie den Dienstleister kontrollieren?
- Ist es sinnvoll, Dritte für ein solches Audit einzuschalten?
- Ist es sinnvoll, die Sicherheit von Netzen und Systemen durch einen „Penetration Test“ zu überprüfen?
- Haben Sie die für das Audit erforderlichen Zugriffsrechte vertraglich mit dem Dienstleister vereinbart?

3 Auswahl und Wechsel des Dienstleisters

Neben den genannten Fragen zur Konzeption der Dienstleistung gibt es auch im Rahmen der Auswahl der Dienstleitung und zur Vorbereitung eines Wechsels des Dienstleisters wichtige Aspekte, die die Sicherheit Ihres IT-Betriebes beeinflussen können. Diese sind im Folgenden zusammengestellt.

3.1 Auswahl des Dienstleisters

Sicherheitsaspekte sollten Sie unbedingt schon bei Auswahl des Dienstleisters berücksichtigen. Hier spielen insbesondere Fragen möglicher Interessenkollisionen und der Stabilität des Dienstleisters eine Rolle. Im Einzelnen könnten dazu z.B. die folgenden Fragen zählen:

- Wie ist die Eigentümerstruktur des Dienstleisters?
  - Gibt es absolute Mehrheiten/Sperrminoritäten?
  - Bestehen Verflechtungen mit konkurrierenden Unternehmen?
  - Liegt die Mehrheit in ausländischem Besitz?
- Gibt es absehbare Interessenkollisionen des Dienstleisters?
  - Gibt es eine starke Abhängigkeit von Aufträgen von Wettbewerbern?
  - Ist der Dienstleister auch für Konkurrenzunternehmen von Ihnen tätig?
  - Ist der Dienstleister ein Tochterunternehmen o.ä. eines Ihrer Wettbewerber?

- Wirtschaftliche Leistungsfähigkeit
  - Ist der Dienstleister so stabil, dass eine langfristige Geschäftbeziehung möglich ist?
  - Ist der Dienstleister solvent genug, im Falle einer schuldhaften Vertragsverletzung die vereinbarten Vertragsstrafen und/oder Schadensersatz in ausreichender Höhe zu leisten?

Da sich die Antworten auf diese Fragen auch während einer Geschäftsbeziehung ändern können, empfiehlt es sich, die Pflicht zur Information über relevante Änderungen in das Vertragswerk aufzunehmen und ggf. regelmäßige Überprüfungen (z.B. im Rahmen des Audits) vorzusehen.

3.2 Wechsel des Dienstleisters

Aus unterschiedlichen Gründen kann es zukünftig erforderlich sein, den IT-Dienstleister zu wechseln oder den IT-Betrieb wieder selbst zu übernehmen. Berücksichtigt man dies schon bei der Konzeption des Outsourcing, kann ein solcher Wechsel erheblich erleichtert werden. Mit Bezug auf die IT-Sicherheit wichtige Aspekte sind dabei u.a. die folgenden:

- Sind alle Dienstleistungen, Prozesse, Abläufe so dokumentiert, dass sie auch an anderer Stelle wieder aufgesetzt werden können? Haben Sie Zugriff (technisch, rechtlich) auf diese Dokumentationen auch bei/nach Beendigung des Vertrages?
- Verwendet der Dienstleister Systeme, die nicht allgemein am Markt verfügbar sind (z.B. Eigenentwicklungen)? Wenn ja, wie ist ein Transfer Ihrer Anwendungen aus diesen Systemen auf andere möglich?
- Ist eine Kooperationspflicht für den Dienstleister im Falle eines Wechsels vertraglich festgelegt?
- Ist die Vertraulichkeitsregelung ausreichend, um auch einen solchen Wechsel abzudecken?
- Ist genau festgelegt, wo der Dienstleister Ihre Daten speichert, damit eine kontrollierte Löschung bei Bedarf erfolgen kann und (nachweisbar) vollständig ist?

3.3 Zugriff bei Insolvenz des Dienstleisters

In seltenen Fällen kann es dazu kommen, dass Ihr Dienstleiter Insolvenz anmelden muss. Auch wenn Überprüfungen der wirtschaftlichen Situation Ihres IT-Dienstleisters Ihnen hoffentlich so frühzeitig Hinweise auf drohende Probleme geben, dass eine Insolvenz zu verhindern oder ein vorheriger Wechsel des Dienstleisters möglich ist, erscheint es sinnvoll, einige Vorsichtsmaßnahmen zu treffen:

- Welche Ihrer Daten, die beim Dienstleisters gespeichert sind, dürfen auf keinen Fall Dritten zur Kenntnis gelangen?
- Welche Daten brauchen Sie ungedingt und kurzfristig, um Ihren IT-Betrieb aufrecht zu erhalten?
- Welche vertraglichen Regelungen sind erforderlich, um Ihnen Zugriff auf diese Daten (und ggf. auch andere Systeme) im Falle einer Insolvenz des Dienstleisters zu gewährleisten?

4 Fazit

Zusammenfassend lässt sich feststellen, dass auch beim Betrieb einer IT-Infrastruktur durch einen *externen* Dienstleister ein angemessenes Sicherheitsniveau gewährleistet werden kann.

Voraussetzung dafür ist allerdings, dass im Rahmen der Konzeption, der Definition des Umfangs der Dienstleistung und der vertraglichen Regelungen sicherheitsrelevante Aspekte berücksichtigt werden. Außerdem sollte eine regelmäßige Überprüfung der relevanten Sicherheitsaspekte in die Prüfung der Qualität der Dienstleistung integriert werden.

Dabei sollten Sie auf eine gute Integration und Akzeptanz der sicherheitsfördernden Maßnahmen achten, um sie auch in der Realität und in der täglichen Praxis umsetzbar zu machen. Ein Rückgriff auf Erfahrungen bei der Erstellung interner IT-Sicherheits-Konzepte ist empfehlenswert, um die dort festgestellten Spezifika Ihres Unternehmens auch beim Outsourcing Ihrer IT gut zu berücksichtigen.