



Technische Aspekte des IT Offshoring

Arbeitspapier Nr. 5/2004

Amberg Michael, Wiener Martin

{amberg | martin.wiener}@wiso.uni-erlangen.de

Friedrich-Alexander-Universität Erlangen-Nürnberg

Lehrstuhl für Betriebswirtschaftslehre, insbes. Wirtschaftsinformatik III

Lange Gasse 20, 90403 Nürnberg, www.wi3.uni-erlangen.de

1 Einführung

Im Hinblick auf die technischen Aspekte des IT Offshoring gilt es zunächst die **IT-Dienstleistungen** darzulegen, die im Rahmen eines Outsourcing-Projekts von einem IT-Dienstleister erbracht werden können. In diesem Zusammenhang sind insbesondere die konkreten Einzelleistungen sowie entsprechende Qualitätsmaße zur Messung der Leistungserbringung durch den Service-Provider von Interesse. Zudem umfassen die technischen Aspekte Anforderungen an die **IT-Infrastruktur** auf Kunden- und Anbieterseite. Hierbei spielen insbesondere die Kompatibilität der vorhandenen Systeme sowie die Einführung neuer Systeme, die die Zusammenarbeit mit dem ausländischen Provider vereinfachen, eine gewichtige Rolle. Des Weiteren beschäftigt sich die technische Betrachtung des Offshoring mit der **IT-Sicherheit** in Bezug auf die Zusammenarbeit mit einem ausländischen Servicepartner. Hierbei gilt es im Wesentlichen Sicherheitsaspekte in Bezug auf die beteiligten Unternehmen sowie im Hinblick auf die Kommunikation zwischen diesen zu berücksichtigen.

2 IT-Dienstleistungen

In diesem Abschnitt werden konkrete Einzelleistungen im Rahmen der unterschiedlichen Leistungskategorien aufgezeigt. In Verbindung mit jeder Einzelleistung werden darüber hinaus mögliche Qualitätsmaße zur Messung der durch den beauftragten Dienstleister erbrachten Leistungsqualität vorgestellt. Die Kategorisierung der Dienstleistungen orientiert sich an den Leistungsformen des IT Offshoring (***Infrastructure Service Providing, Application Development Outsourcing*** und ***Business Process Outsourcing***).

2.1 Infrastructure Service Providing (ISP)

Im Hinblick auf das Infrastructure Service Providing (ISP) kann der Service-Provider unter anderem so genannte ***Desktop-Services*** erbringen. In diesem Fall ist der Service-Provider für die Versorgung der Anwender des Offshoring-Kunden mit Endgeräten (z. B. Desktop-PCs, Peripheriegeräte, PDAs) zuständig. Ein weiterer typischer Bestandteil von Desktop-Services stellt die Wartung von Hardware und Software dar. In Bezug auf die Hardware erweist sich ein Wartungsvertrag insbesondere dann als günstig, wenn der Offshore-Anbieter auch für die Bereitstellung der restlichen IT-Infrastruktur zuständig ist. Hierdurch lässt sich meist eine Erweiterung der Gewährleistungsfristen auf drei Jahre durchsetzen. Diese ist vorteilhaft, da man somit relativ nahe an das Ende des Innovationszyklus der Hardware-Komponenten herankommt. Im Hinblick auf die Software umfasst ein Wartungsvertrag in den meisten Fällen das Einspielen von Patches zur Fehlerbehebung sowie die Durchführung von Updates zur Aktualisierung der Software. Die Erweiterung von Software-Modulen fällt nicht in diese Leistungskategorie. (vgl. [Bräu2004, 98-101])

Als Qualitätsmaß im Hinblick auf die Desktop-Services kann primär die Einhaltung aller zugesicherten Dienstleistungen zu den vertraglich vereinbarten Zeitpunkten dienen. Zusätzlich kann auch die Zeitdauer bis zur Fehlerbehandlung durch den Provider in Abhängigkeit von der Priorität des aufgetretenen Problems zur Leistungsmessung herangezogen werden. (vgl. [Bräu2004, 103])

Im Rahmen des ISP kann auch die Planung und Konzeption sowie die Bereitstellung von ***Netzwerken*** durch den Outsourcing-Kunden in Auftrag gegeben werden. Hinsichtlich des Entwurfs einer Netzwerklösung eignet sich ein Offshore-Anbieter grund-

sätzlich für alle Netzwerktypen. In Bezug auf die Realisierung empfiehlt es sich allerdings, aufgrund der enormen Entfernung zwischen den Vertragspartnern, nur die Bereitstellung eines Wide Area Network (WAN) oder die Einrichtung eines Virtual Private Network (VPN) bei einem ausländischen Anbieter in Auftrag zu geben. Die Umsetzung eines Local Area Network (LAN) sollte in der Regel durch einen vor Ort ansässiger Dienstleister durchgeführt werden.

Die Vernetzung unterschiedlicher Unternehmensstandorte in Form eines WAN umfasst in der Regel auch den Betrieb von Firewalls. Diese sollen die IT der vernetzten Standorte vor unberechtigtem Zugriff und sonstigen Angriffen schützen. Alternativ hierzu kann der Offshore-Anbieter auch mit der Installation eines VPN für bestimmte Nutzergruppen beauftragt werden. (vgl. [Bräu2004, 103-105])

Während sich die Leistungsmessung im Rahmen der Planung und Konzeption eines Netzwerks als relativ schwierig gestaltet, besteht in Bezug auf den Netzwerkbetrieb eine Vielzahl von Qualitätsmaßen. Neben der Einhaltung der vertraglich vereinbarten Leistungen und der Reaktionszeit bei der Fehlerbehandlung kann insbesondere das Verfügbarkeits-Monitoring zur Messung der durch den Dienstleister zur Verfügung gestellten Netzwerkqualität eingesetzt werden. Hierbei wird zusätzlich zu den Ausfallzeiten in erster Linie die Bereitstellung der zugesicherten Bandbreite überwacht. (vgl. [Bräu2004, 108])

Eine weitere Dienstleistung in Bezug auf die IT-Infrastruktur stellt das **Hosting** dar. In Anbetracht der zunehmenden globalen Vernetzung und der stetigen Verbesserung der Telekommunikationstechnologien ist die Einbindung eines Offshore-Partners in diesem Zusammenhang mehr und mehr als unkritisch einzustufen. Das Hosting umfasst ein breites Spektrum an IT-Leistungen. Dieses reicht von der Speicherplatzbereitstellung bis hin zur Administration der Kundensysteme. Im Extremfall übernimmt der Offshore-Anbieter die Gesamtverantwortung für die zum Hosting gehörenden Leistungen. Neben der Bereitstellung von Speicher- und Rechenkapazität ist der Offshore-Anbieter in diesem Fall auch für die Verwaltung der entsprechenden Systeme zuständig. Darüber hinaus muss der IT-Dienstleister hierbei sicherstellen, dass kritische Daten durch einen Totalausfall des Systems nicht verloren gehen. Hierzu müssen Sicherheitsvorkehrungen, wie z. B. die Installation von Back-Up-Systemen oder die Durchführung einer regelmäßigen Datenspiegelung, getroffen werden. (vgl. [Bräu2004, 109-111])

Als Leistungsparameter sind in Verbindung mit Hosting-Leistungen vorwiegend die Verfügbarkeit und das Antwortzeitverhalten von Bedeutung. In Bezug auf die Systemverfügbarkeit kann insbesondere die Häufigkeit von Ausfällen und Störungen betrachtet werden. Als konkrete Maßzahlen werden in diesem Kontext die Mean-Time-to-Repair (MTR), die durchschnittliche Zeit zwischen der Meldung einer Störung und der Beseitigung sowie die Mean-Time-Between-Failure (MTBF), die durchschnittliche Zeit zwischen zwei Systemausfällen, herangezogen. (vgl. [Bräu2004, 114])

Die Bereitstellung und Verwaltung von **Applikationen** durch den Offshore-Anbieter stellt eine weitere Dienstleistung in Bezug auf das ISP dar. In diesem Zusammenhang ist in erster Linie das Application Service Providing (ASP) zu nennen. Die Leistungsparameter im Hinblick auf das Applikationsmanagement entsprechen weitestgehend denen des Hosting.

2.2 Application Development Outsourcing (ADO)

Im Rahmen des Application Development Outsourcing (ADO) gilt es im Allgemeinen zwischen Standard- und Individual-Software zu differenzieren. Bei Ersterer handelt es sich um eine fertige Software-Applikation, die die gängige Funktionalität für ein betriebliches Anwendungsgebiet abdeckt. Individual-Software hingegen wird speziell für eine konkrete Anwendung beim Auftraggeber entwickelt. In Abhängigkeit von dem jeweiligen Software-Typ können unterschiedliche Einzelleistungen bei einem Offshore-Anbieter in Anspruch genommen werden.

Im Hinblick auf **Standard-Software** kann der Offshore-Anbieter bereits in die Auswahl des Software-Produkts integriert werden. In vielen Fällen existiert eine Vielzahl von Standardlösungen, die eine ähnliche Funktionalität bieten. Demnach gilt es zu untersuchen, welches Produkt die Kundenanforderungen am besten erfüllt. Des Weiteren kann der Offshore-Anbieter bei der Anpassung der Standard-Software an die unternehmensspezifischen Charakteristika behilflich sein. Für den Fall, dass an einer Standardlösung größere Änderungen vorgenommen werden müssen, können auch funktionale Erweiterungen beim Offshore-Anbieter in Auftrag gegeben werden. (vgl. [Bräu2004, 123-124])

In Bezug auf **Individual-Software** lässt sich vorwiegend die Entwicklung von Software-Modulen als konkrete Einzelleistung nennen. In Abhängigkeit von den bisherigen Erfahrungen mit dem Offshore-Anbieter kann das auslagernde Unternehmen

entweder das komplette Software-Projekt oder lediglich Teile davon an den Anbieter vergeben. (vgl. [Bräu2004, 125]) Möchte der Outsourcing-Kunde nicht die komplette Verantwortung des Projekts an den ausländischen Provider abgeben, bietet sich insbesondere die Auslagerung von arbeitsintensiven Phasen (z. B. die Kodierphase) an den Service-Provider an (vgl. [Tran2004]).

In diesem Zusammenhang ist anzumerken, dass die Wartung und Pflege von Software grundsätzlich der Leistungsform des ISP zuzuordnen ist. Die hiermit verbundenen Tätigkeiten (z. B. das Aufspielen von Updates) erfordern keine Änderungen am Quellcode der Applikationen und sind folglich nicht in die Leistungskategorie der IT-Entwicklung einzustufen.

Als Qualitätsparameter für Entwicklungstätigkeiten lassen sich zum einen die Termin- und Budgettreue durch den Offshore-Anbieter aufführen. Negativ ausgedrückt könnten diese Kriterien auch als Zeitraum bzw. Höhe der Überziehung bezeichnet werden. Zum anderen gilt es die Qualität der abgelieferten Ergebnisse zu betrachten. Hierbei spielen insbesondere die Vollständigkeit im Hinblick auf die vereinbarte Funktionalität und die Fehlerfreiheit eine gewichtige Rolle. (vgl. [Bräu2004, 127])

2.3 Business Process Outsourcing (BPO)

Die Leistungsform des Business Process Outsourcing (BPO) wird im Rahmen dieses Kapitels nicht näher betrachtet. Aufgrund der Vielfalt der Prozesse, die Gegenstand eines BPO-Projekts sein können, ist es nicht möglich spezifische Einzelleistungen zu nennen. Zudem basiert diese Leistungsform des IT Outsourcing in vielen Fällen auf einer Auslagerung der IT-Infrastruktur.

3 IT-Komponenten

Die folgenden Anforderungen an die IT-Landschaft sollten sowohl durch den Outsourcing-Kunden als auch durch den ausländischen Dienstleister erfüllt werden. Zur Sicherstellung der notwendigen Flexibilität empfiehlt es sich, eine Kombination aus innovativen Technologien und bewährten Standards bereitzustellen. Hierdurch soll der Aufbau einer adäquaten, zuverlässigen und einfach zu verwaltenden Infrastruktur ermöglicht werden. (vgl. [Baye2002, 23])

In Bezug auf die IT-Infrastruktur, die einer Offshore-Partnerschaft zugrunde liegt, ist insbesondere die Installation leistungsfähiger **Netzwerke** von zentraler Bedeutung.

Hiermit wird sowohl das lokale Netzwerk innerhalb der Unternehmungen als auch die Vernetzung der Offshoring-Partner untereinander angesprochen. Performanzstarke Netzwerke ermöglichen eine zeitnahe Versorgung der verteilten Mitarbeiterteams mit Informationen. Neben der zur Verfügung stehenden Bandbreite der Kommunikationsstrukturen spielen die Zuverlässigkeit des elektronischen Datenflusses sowie die hohe Verfügbarkeit der eingerichteten Netzwerke eine entscheidende Rolle bei der erfolgreichen Abwicklung einer Offshoring-Kooperation. (vgl. [Baye2002, 22])

Mithilfe der Vernetzung der unterschiedlichen Projektstandorte lässt sich eine Vielzahl von **Kommunikationstechniken** zur Interaktion zwischen den Kooperationspartnern einsetzen. Aufgrund der weiten Entfernung und den bestehenden Zeitunterschieden bieten sich Techniken an, die eine Ort- und Zeitunabhängigkeit der Kommunikation unterstützen. (vgl. [Baye2002, 22]) Im Einzelnen können in Anlehnung an [Baye2002, 35-37] die folgenden Techniken zur Kommunikation zwischen den verteilten Projektteams herangezogen werden:

- **E-Mail**

Die E-Mail stellt im Rahmen von Offshore-Projekten in der Regel das wichtigste Medium zum Informations- und Datenaustausch zwischen den unterschiedlichen Mitarbeiterteams dar. Allen voran die asynchrone Kommunikation und die geringen Kosten erweisen sich hierbei als vorteilhaft.

- **Telefon**

Das Telefon ist heutzutage als das Standardkommunikationsmedium anzusehen. Durch die stark gesunkenen Entgelte für Auslandsverbindungen lassen sich die hiermit verbundenen Kosten in vielen Fällen nahezu vernachlässigen. Vorwiegend bei dringendem Kommunikationsbedarf bevorzugen die Projektpartner, aufgrund der synchronen Kommunikation, das Telefon zur Kontaktierung des räumlich entfernten Geschäftspartners.

- **Videokonferenz**

Die Videokonferenz bietet grundsätzlich die gleichen Vorzüge wie das Telefon. Allerdings kann die Tatsache, dass sich die Gesprächspartner sehen können insbesondere in der Anfangsphase eines Offshore-Projekts, wenn sich die Mitarbeiter der unterschiedlichen Projektteams noch nicht persönlich kennen, zu einer angenehmeren Atmosphäre beitragen. Bei der Schlichtung von möglicherweise auftretenden Konflikten zwischen den Projektpartnern ist die Video-

konferenz, als relativ persönliche Kommunikationstechnik, anderen Techniken vorzuziehen. Im Idealfall sollte der Outsourcing-Kunde in dieser Situation jedoch eine Delegation von Unternehmensvertretern zum Projektpartner entsenden. Eine persönliche Kommunikation lässt sich durch keine der hier aufgeführten Technologien ersetzen.

- **Intranet (bzw. Extranet)**

Das Intranet dient primär dem unternehmensinternen Informations- und Datenaustausch. Bei der Zusammenarbeit mit einem ausländischen Partnerunternehmen kann dieser Zugang zum Intranet des Kunden erhalten. Die Öffnung des Intranets für externe Partner bezeichnet man als Extranet. Auf diese Weise stehen den Mitarbeitern des ausländischen Service-Providers in der Regel der gleiche Datenbestand und die gleiche Funktionalität wie den internen Mitarbeitern des Kunden zur Verfügung. (vgl. [Baye2002, 37])

- **Newsgroups**

Das Veröffentlichen von Fragen bezüglich der Abwicklung des Outsourcing-Projekts in Newsgroups kann hilfreich sein, wenn das entsprechende Projektmitglied den zuständigen Ansprechpartner nicht kennt oder es sich um allgemeine Fragen handelt. Hierdurch können offene Probleme relativ schnell und unkompliziert gelöst werden. Zudem kann ein Erfahrungsaustausch bezüglich des Umgangs mit Software- und Hardware-Funktionen mithilfe der bereitgestellten Newsgroups erfolgen. (vgl. [Baye2002, 35])

- **Chat**

Der Chat ermöglicht eine Kommunikation zwischen räumlich getrennten Projektmitarbeitern in Echtzeit. Insbesondere zum kurzen Informationsaustausch eignet sich diese Kommunikationsform hervorragend. Ein Austausch von Daten ist allerdings hiermit nicht möglich. (vgl. [Baye2002, 36])

etc.

Grundsätzlich gilt es im Hinblick auf die Kommunikation mit dem ausländischen Partner anzumerken, dass sich ein Offshore-Projekt nicht ausschließlich mithilfe der instrumentellen Kommunikation koordinieren lässt. Vielmehr spielt die direkte Kommunikation mit dem Partnerunternehmen eine entscheidende Rolle. Allen voran das gegenseitige Kennen lernen zu Projektbeginn oder die Schlichtung von Konflikten im Verlauf des Projekts erfordern den persönlichen Kontakt zwischen den verteilten Pro-

jektteams. Ausschließlich in Ausnahmefällen (z. B. enormer Zeitdruck) sollte von der direkten Kommunikation abgesehen werden. (vgl. [NetS2004])

Je mehr Interaktion zwischen den unterschiedlichen Standorten notwendig ist, desto höhere Ansprüche werden an die Qualität der Netzwerke und die Zuverlässigkeit der eingesetzten Kommunikationstechniken gestellt. Im Extremfall kann bei einer hohen Datentransferrate eine Standleitung bzw. bei hohen Sicherheitsanforderungen eine verschlüsselte Datenübertragung über ein Virtual Private Network (VPN) erforderlich sein. (vgl. [Baye2002, 23])

Im Hinblick auf die eingesetzten **Anwendungs- und Betriebssysteme** sollte auf eine einfache Installation und Verteilung der entsprechenden Software-Komponenten geachtet werden (vgl. [Baye2002, 23]). Benutzen der Auftraggeber und der Offshore-Partner verschiedenartige Anwendungs- und Betriebssysteme, ist bereits im Vorfeld des Projekts sicherzustellen, dass diese kompatibel zueinander sind. Stellt sich erst zu einem späteren Zeitpunkt heraus, dass die Kompatibilität der an den einzelnen Projektstandorten eingesetzten Systeme nicht gegeben ist, kann dies im Extremfall zum Scheitern des kompletten Offshore-Projekts führen. (vgl. [Baye2002, 26])

Um die Zusammenarbeit zwischen den Projektpartnern so weit wie möglich zu vereinfachen, bietet es sich an ein global zugängliches **Dokumentenmanagementsystem (DMS)** für das Offshore-Projekt einzuführen. Dieses soll allen am Projekt beteiligten Mitarbeitern den Zugriff auf einen einheitlichen Informations- und Wissenspool (vgl. [Baye2002, 22]) sowie die gemeinsame Bearbeitung von Dokumenten ermöglichen.

Zusätzlich zu einem DMS ist im Rahmen von IT-Entwicklungsprojekten die Einführung von **zentralen Archiven** in Verbindung mit einem **Versionskontrollsystem** unverzichtbar. Insbesondere bei einer Parallelentwicklung erweist sich die Speicherung des Quellcodes und der Austausch des Programmiercodes zwischen den unterschiedlichen Entwicklungsstandorten ansonsten als kaum zu bewältigendes Problem. Neben der Bereitstellung der aufgeführten IT-Komponenten sollte das auslagernde Unternehmen bei einer verteilten Software-Entwicklung einen lokalen Support sowie eine lokale Systemadministration an allen Projektstandorten einrichten. Darüber hinaus gilt es bereits im Vorfeld einheitliche „Coding Conventions“ (z. B. für die Kommentierung des Quellcodes) festzulegen. (vgl. [Baye2002, 22])

In Bezug auf die IT-Infrastruktur empfiehlt [Baye2002, 26], die **technische Ausstattung** des Offshoring-Partners (z. B. die Auflösung der Monitore) zu überprüfen. Beispielsweise ist sicherzustellen, dass die ausländischen Entwickler bei der Implementierung einer graphischen Oberfläche dieselbe Bildschirmauflösung wie die späteren Anwender benutzen.

4 IT-Sicherheit

Grundsätzlich besteht bei der Übertragung firmeninterner Daten über öffentliche Netze die Möglichkeit des unbefugten Zugriffs durch Dritte. Um diese Gefahr so gering wie möglich zu halten, ist es nach [Baye2002, 26] empfehlenswert, frühzeitig entsprechende Sicherheitsmaßnahmen einzuleiten. Neben der Übertragung der Daten sind hiervon die Speicherung von vertraulichen Informationen sowie der Datenzugriff innerhalb der Partnerunternehmen betroffen. Demnach sollten im Anschluss an eine Analyse der Sicherheitsanforderungen entsprechende Konzepte für den Auftraggeber, den Auftragnehmer und die Datenübertragung bzw. die Kommunikation zwischen den Offshoring-Partnern erarbeitet werden. (vgl. [Haeb2004])

Zur Erstellung eines **Sicherheitskonzepts für die Kommunikation** zwischen den Offshoring-Partnern können in erster Linie die folgenden Ansätze herangezogen werden:

- **Absicherung der Datenleitungen**

Die einfachste Form der Absicherung des Datentransfers zwischen den Projektpartnern stellt die Verschlüsselung der Kommunikationsleitung dar. In diesem Fall werden alle Datenpakete, die zwischen den Partnern ausgetauscht werden, verschlüsselt. Zur Realisierung dieser Absicherungsform kann eine Verbindung zwischen den Projektstandorten über SSL (Secure Socket Layer) oder unter Zuhilfenahme eines Virtual Private Network (VPN) eingerichtet werden. (vgl. [Baye2002, 33])

SSL bietet im Wesentlichen eine verschlüsselte Datenübertragung zwischen einem Client-Browser und einem entsprechenden Web Server. Auf diese Weise können Informationen von dezentralen Standorten sicher abgerufen werden. (vgl. [Baye2002, 36]) Bei einem VPN erfolgt die Absicherung der Datenleitungen über verschlüsselte Datentunnel. Hierbei leitet eine spezielle Netz-

werk-Software die zu übermittelnden Daten über einen abgesicherten Datentunnel zum Empfänger. (vgl. [Baye2002, 38])

- **Datenverschlüsselung**

Im Gegensatz zur Leitungsabsicherung werden bei der Datenverschlüsselung nur diejenigen Informationen chiffriert, die der Sender explizit auswählt. Auf Senderseite müssen die zu übermittelnden Daten verschlüsselt und auf Empfängerseite wiederum entschlüsselt werden. Hierzu wird auf beiden Seiten ein entsprechender Schlüssel benötigt. (vgl. [Baye2002, 33])

Für die Verschlüsselung der E-Mail-Kommunikation kann beispielsweise PGP (Pretty Good Privacy) eingesetzt werden. Hiermit lassen sich E-Mail-Texte und Datenanhänge verschlüsseln. Die Verwaltung der zur Verfügung stehenden Schlüssel erfolgt bei PGP durch den Nutzer selbst. (vgl. [Baye2002, 37])

Ein **Sicherheitskonzept für den Auftraggeber bzw. den Auftragnehmer** könnte unter anderem die nachfolgenden Maßnahmen beinhalten. Mit diesen versuchen die Projektpartner in erster Linie den Zugriff auf projektinterne Daten durch hierzu nicht berechtigte Personen zu vermeiden.

- **Installation einer Firewall**

Eine Firewall wird in der Regel eingesetzt, um den externen Zugriff auf interne Ressourcen zu koordinieren. Hierbei können in Abhängigkeit von der anfragenden Quelle unterschiedliche Dienste zugelassen bzw. abgelehnt werden. (vgl. [Baye2002, 37])

- **Einrichtung eines Passwortschutzes**

Vertrauliche Dokumente können grundsätzlich mit einem Passwortschutz belegt werden. Hierdurch kann sichergestellt werden, dass Informationen auch unternehmensintern nicht von jedem Mitarbeiter eingesehen werden können.

- **Definition von Mitarbeiterrollen**

Ähnlich wie beim Passwortschutz kann mit der Definition von Rollen gewährleistet werden, dass Dokumente internen Mitarbeitern, die nicht über die erforderlichen Rechte verfügen, nicht zugänglich sind. Im Gegensatz zum Schutz vertraulicher Daten mithilfe von Passwörtern werden den Projektmitarbeitern bei der Definition von Mitarbeiterrollen grundsätzlich nur diejenigen Dokumente und Informationen angezeigt, auf die sie zugreifen dürfen.

Als weitere Absicherung vor einem unerlaubten Zugriff können in Abhängigkeit von der jeweiligen Rolle des Projektmitglieds unterschiedliche Zugriffsrechte definiert sein. Beispielsweise kann ausschließlich der Projektleiter bestimmte Dokumente ändern, während ein Projektteammitglied diese nur lesen kann.

- ***Verschlüsselung der Festplatten***

Die Festplattenverschlüsselung steht in enger Verbindung mit der Datenverschlüsselung (siehe oben). Hierbei werden alle Daten, die sich auf der Festplatte befinden, verschlüsselt. (vgl. [Baye2002, 38]) Diese Maßnahme ist insbesondere bei mobilen Geräten, wie z. B. Notebooks, sinnvoll (vgl. [Baye2002, 33]).

etc.

Die erarbeiteten Sicherheitskonzepte für die verschiedenen Offshoring-Akteure sowie für die Kommunikation zwischen diesen gilt es in jedem Fall im Vertragswerk zu hinterlegen. (vgl. [Haeb2004]) Treten im Projektverlauf Sicherheitslücken auf, ist nachvollziehbar, wer diese zu verantworten hat. Handelt es sich bei den Sicherheitsproblemen um bisher nicht berücksichtigte Aspekte, gilt es diese unverzüglich in den Offshoring-Vertrag aufzunehmen.

Literaturverzeichnis

- [Baye2002] *Bayerischer Industrie- und Handelskammertag (Hrsg.): Offshore IT für den Mittelstand. Leitfaden zur Schaffung und Sicherung von Arbeitsplätzen durch offshore IT-Entwicklung im Rahmen der Internationalisierung des Mittelstandes in Bayern. Software Forum Bayern e.V., München 2002.*
- [Bräu2004] *Bräutigam, Peter (Hrsg.): IT Outsourcing. Eine Darstellung aus rechtlicher, technischer, wirtschaftlicher und vertraglicher Sicht. Erich Schmidt Verlag, Berlin 2004.*
- [Haeb2004] *Haeberlein, Thomas: Outsourcing unter Sicherheitsaspekten. Bundesamt für Sicherheit in der Informationstechnik, Bonn 2004.*
- [NetS2004] *NetSkill AG: E-Interview. Das Ende der europäischen IT-Entwicklung.*
[http://www.competence-site.de/itmanagement.nsf/4e24e48e4c74907fc1256d200034ede0/8b7700dc8a0f3480c1256d8a0041a806!](http://www.competence-site.de/itmanagement.nsf/4e24e48e4c74907fc1256d200034ede0/8b7700dc8a0f3480c1256d8a0041a806!OpenDocument)
OpenDocument, Abruf am 2004-04-15.
- [Tran2004] *TransCrit: Offshore IT-Modelle. Unterschiedliche Modelle für Offshore IT.*
<http://www.transcrit.com/de/offshore/models.html>, Abruf am 2004-03-15.