

**Die Auslagerung betrieblicher Basisinfrastrukturdienste
für Informationstechnologien**

**Armin Heinzl, Universität Mannheim
Stefan Roßbach, IMG GmbH, Frankfurt**

**Working Paper 14/2004
Oktober 2004**

Die Auslagerung betrieblicher Basisinfrastrukturdienste für Informationstechnologien

Armin Heinzl, Universität Mannheim
Stefan Roßbach, IMG GmbH, Frankfurt

Zusammenfassung:

Der vorliegende Beitrag untersucht eine der elementarsten Wertschöpfungsstufen der betrieblichen Informationsverarbeitung: die Bereitstellung und den Betrieb der informationstechnologischen Basisinfrastruktur. Im Sinne einer Bestandsaufnahme werden aktuelle Herausforderungen bei der Nutzung der Basisinfrastruktur, die Entscheidungsdeterminanten für einen Fremdbezug der damit verbundenen Aufgaben, die Chancen und Risiken der Auslagerung von Basisinfrastrukturdiensten sowie die mentale Konfiguration eines „idealen“ Leistungsbündels untersucht. Die Aussagen werden auf der Basis einer explorativen Fallstudienuntersuchung gewonnen, an der sich insgesamt 11 Unternehmen im Sommer 2004 beteiligt haben.

Stichworte: Auslagerung, Informationstechnologie, Basisinfrastruktur, Fremdbezug

IT Base Infrastructure Outsourcing

Summary:

This paper deals with one of the most basic value chain elements in the field of information systems services: the provision and the seamless operation of a sophisticated IT base infrastructure. In order to capture the status quo in the corporate world, contemporary challenges of the IT base infrastructure, determinants of a make or buy decision, outsourcing opportunities and threats as well as the development of an “ideal” service bundle will be explored. The insight developed in this paper is based on a comprehensive multiple case study analysis which incorporated 11 large companies during the summer of 2004.

Keywords: Outsourcing, Information Technology, Base Infrastructure, Make or Buy,

1. Einführung

Unter dem Begriff des Informationstechnologie-Outsourcing wird im Allgemeinen die mittel- bis langfristige Auslagerung von Aufgaben und Ressourcen im Bereich der Informationstechnologie (IT) an einen oder mehrere unabhängige Dienstleister verstanden [1]. Während ein Trend zum Auslagern informationstechnologischer Aufgaben seit Beginn der 90er Jahre zunächst in den USA zu erkennen war, hat das IT-Outsourcing in der Zwischenzeit in Deutschland eine beachtenswerte Größe angenommen und gilt als einer der am stärksten wachsenden Outsourcingmärkte in Westeuropa [2]. Ging es potentiellen Outsourcingkunden zu Beginn der Outsourcingdebatte darum, ob mit einer Auslagerung allgemein Vorteile verbunden sind und ob Anbieter entsprechender Leistungen diese auch in angemessener Qualität bereitstellen, steht dies heutzutage außer Frage. Unternehmen beschäftigen sich gegenwärtig damit, welche IT-Aufgaben und -Ressourcen zur Auslagerung am Besten geeignet sind, um die Kostenstruktur und Servicequalität zu verbessern. Eine Diversifikation des Marktes von Komplettanbietern (Totales Outsourcing) bis zu selektiven Lösungen (selektives Outsourcing) ist in vollem Gange [3].

Eine Form des selektiven IT-Outsourcings ist die Nutzung fremder Basisinfrastrukturen. Darunter versteht man das Auslagern von Rechenzentrumsflächen an spezialisierte Anbieter, die eine hoch verfügbare Gebäudetechnik mit redundant ausgelegter Energieversorgung, Klimatisierung und ein hohes Maß an physischer Sicherheit garantieren. Zu den nachfragenden Unternehmen zählen sowohl Anbieter von IT-Dienstleistungen, wie z.B. Systemintegratoren, als auch Anwenderunternehmen, wie z.B. Finanzdienstleister. IT-Dienstleister veräußern die Serviceleistungen des Basisinfrastrukturanbieters ggf. unter Einschluss zusätzlicher Dienstleistungen weiter, während Anwenderunternehmen die angemieteten Rechenzentrumsflächen für den Eigengebrauch nutzen.

Der vorliegende Beitrag verfolgt das Ziel, mit Hilfe einer multiplen Fallstudienuntersuchung sowohl die Anforderungen aus Kundensicht als auch Nutzen steigernde Lösungsmöglichkeiten durch ein Outsourcing der

Basisinfrastruktur herauszuarbeiten und dabei u.a. folgenden Fragestellungen nachzugehen:

- Welchen aktuellen Herausforderungen stellen sich Unternehmen hinsichtlich ihrer informationstechnologischen Basisinfrastruktur?
- Was sind die Treiber einer Entscheidung für eine Auslagerung der IT-Basisinfrastruktur?
- Wo werden Chancen bzw. Risiken bei einer Auslagerung der Basisinfrastruktur gesehen?
- Wie sieht das „ideale“ Leistungsbündel eines Basisinfrastrukturanbieters aus ?

2. Grundlagen

Begriffsgrundlagen

Im Kontext von Dienstleistungen des Systembetriebs gibt es verschiedene Anglizismen, die es zu erörtern und abzugrenzen gilt. Hierzu zählen die Begriffe „co-location“, „housing“ und „hosting“. Unter „co-location“ versteht man die Anmietung von Stellfläche in einem Rechenzentrum (RZ) eines Dienstleisters und die dafür erforderliche Nutzung der Netzwerk-Anbindung und Stromversorgung [4]. Weitere Dienste, wie die Bereitstellung einer unterbrechungsfreien Stromversorgung (USV), die Klimatisierung der Räume, der Brandschutz oder die Gewährleistung physischer Sicherheit, werden abhängig vom Anbieter direkt zur Verfügung gestellt oder sind zumindest optional beziehbar [5]. Übernimmt der Mieter den Betrieb und die Wartung der informationstechnologischen Betriebsmittel, wird von „*housing*“ bzw. „*co-location housing*“ gesprochen. Das Anwenderunternehmen kann dabei einzelne Server in verfügbare Einschubvorrichtungen bzw. Gestelle (*racks*) des Dienstleisters einbauen. Alternativ sind umzäunte Gehäuse (*cages*) bzw. abgetrennte, separate Teile eines Rechenzentrums (*suites*) anmietbar. Neben diesen, durch den Dienstleister vorkonfektionierten und direkt betriebsbereiten „*plug & play*“-Lösungen (auch als „*fitted-out space*“ bezeichnet), bieten Basisinfrastrukturdienstleister teilweise so genannte „*shell & core*“-Räumlichkeiten an. [6] Dabei handelt es sich um Rohbauflächen, die der Mieter nach eigenen Anforderungen zu Nutzflächen ausbauen kann. Beim „*hosting*“ nutzt der Anwender im Gegensatz zum „housing“ die Ausstattung des Dienstleistungsanbieters. Erhält der Mieter einen eigenen Server,

der physikalisch getrennt von den anderen Mietern bereitgestellt wird, spricht man von „*dedicated hosting*“. Bei geteilter Nutzung eines Servers durch mehrere Anwender ist von „*shared hosting*“ die Rede [7].

Grundelemente der IT-Basisinfrastruktur

Die Basisinfrastruktur gewährleistet den sicheren, unterbrechungsfreien Betrieb der eingesetzten Informationstechnologien und bildet so die Grundvoraussetzung für die Funktionsfähigkeit und Verfügbarkeit der informationstechnologischen Ausstattung. Sie setzt sich aus überwachten Gebäuden bzw. Räumen zusammen, die mit Klimatisierung, Netzwerkanbindung, Energieversorgung ausgestattet sind und Schutz vor Brand- und Wasserschäden bieten. Abbildung 1 zeigt die zentralen Komponenten der IT-Basisinfrastruktur, die eine Hochverfügbarkeit und Sicherheit der eingesetzten Informationstechnologien gewährleisten.

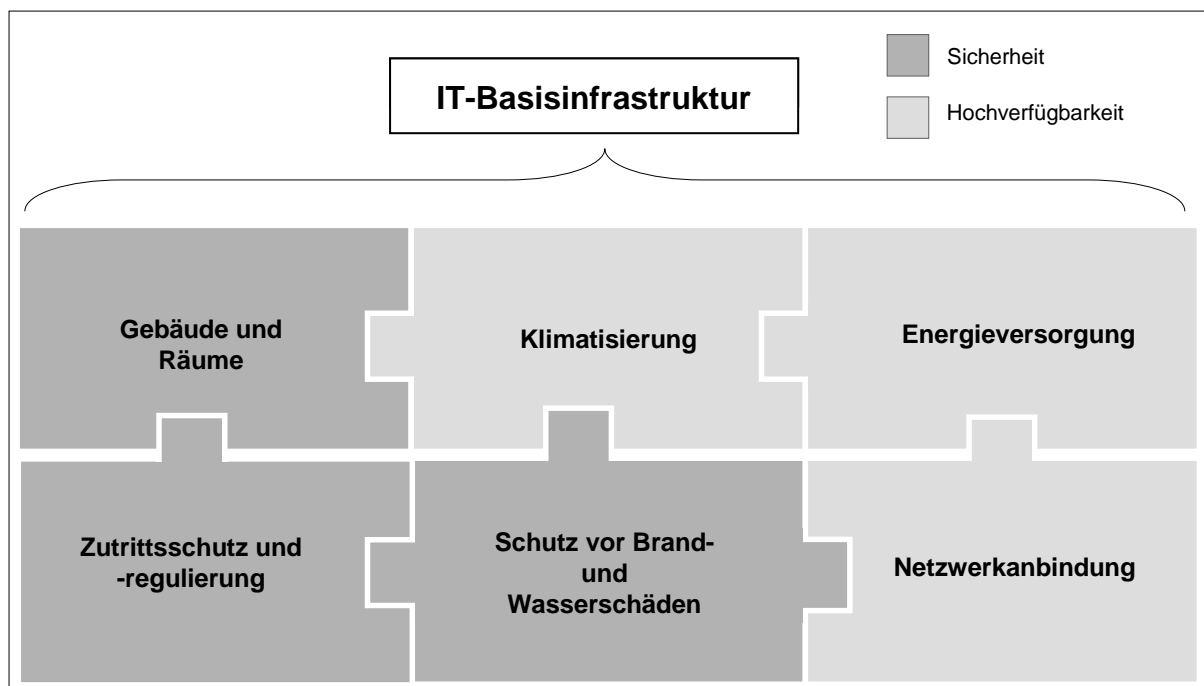


Abbildung 1: Komponenten der IT-Basisinfrastruktur

Von Gebäuden und Räumen, die dem „*housing*“ von Informationstechnologien dienen, wird erwartet, dass sie sowohl physisch als auch technisch sicher sind und einen Zugang zu mehreren Telekommunikationsnetzwerken gewährleisten. Sie müssen einen Grundschutz gegen folgende Risiken sicherstellen:

- höhere Gewalt (z.B. Blitz, Feuer und Wasser),

- organisatorische Mängel (z. B. unbefugter Zutritt zu schutzbedürftigen Räumen),
- technisches Versagen (z. B. Ausfall der Stromversorgung) sowie
- vorsätzliche Handlungen (z. B. Diebstahl, Sabotage, Vandalismus) [8].

Aus diesen Gründen sind angemessen dimensionierte, abgesicherte Stromversorgungen, moderne Klimatechniken, strenge Zugangssicherungen sowie Brandschutzvorrichtungen unverzichtbare Bestandteile der Basisinfrastruktur [9]. Spezielle Vorrichtungen bzw. Materialien, wie z.B. Brandschutztüren, Splitterschutzfolien, Abschirmungen und Isolierungen, können bestimmte Gefahren wie Brände, das Eindringen von Glassplittern, Druckwellen oder Strahlungen verhindern. Ebenso trägt eine hohe Übersichtlichkeit bei der Gestaltung von Räumen und Gebäuden zu einem schnelleren Erkennen von Gefährdungen und einer einfacheren Überwachung des gesamten Infrastruktursystems bei [10]. Hochwertige Gebäude spezialisierter Basisinfrastrukturanbieter zeichnen sich durch eine stabile Bauweise und eine hohe Tragfähigkeit der Decken aus. Weitere Qualitätsmerkmale sind eine flexible Raumaufteilung, große Raumhöhen zur einfachen Installation von Servergestellen und eine übersichtliche, strukturierte Kabelführung.

Zu den wichtigsten Anforderungen von Rechenzentren gehören eine hohe Ausfallsicherheit und eine stabile Energieversorgung [11]. Um Ausfällen vorzubeugen, ist eine *Unterbrechungsfreie Stromversorgung (USV)* notwendig. USV-Anlagen sind Geräte, die bei Stromausfällen, Spannungsschwankungen und Frequenzänderungen über eine Batteriepufferung automatisch die unterbrechungsfreie Weiterversorgung der angeschlossenen sensiblen Informationstechnologien und technischen Infrastrukturanlagen (z. B. Klimasysteme) sicherstellen [12]. Bei hohen Sicherheits- und längerfristigen Verfügbarkeitsanforderungen werden zusätzlich Netzersatzaggregate mit Dieselmotoren benötigt. Die Zeit bis zur Synchronisation und Aufschaltung der Netzersatzanlagen wird in diesem Fall über USV-Anlagen gepuffert.

Um Anlagenausfällen vorbeugen zu können, wird bei hochwertigen Rechenzentren für die Stromversorgung ein n+1- oder n+n-Konzept verfolgt. Beim n+1-Konzept wird zusätzlich zu den n Stromversorgungseinheiten, die normalerweise für den Rechenzentrumsbetrieb benötigt werden, *eine* weitere Einheit (+1) als redundantes

System bereitgestellt [13]. Beim n+n-Konzept sind für jede Einrichtung gleich zwei separate Stromversorgungen verfügbar, die jeweils zu 100% die Energielast übernehmen können. Fällt die Stromversorgungseinheit A aus, ist ein unterbrechungsfreier Betrieb des Rechenzentrums zu 100% durch Stromversorgungseinheit B sichergestellt. Neben der Verfügbarkeit von Hardware und Klimageräten wird dadurch auch die Versorgung strombetriebener Sicherheitsmaßnahmen, wie z. B. Zutritts-, Einbruchmelde- und Brandmeldeanlagen, gewährleistet. Gerade in Räumen mit dicht gepackter IT-Ausstattung besteht aufgrund der entstehenden Wärmelasten ein erhöhtes Brandrisiko. Neben der Überwachung der Räume durch Brandmeldeanlagen werden VESDA (*very early smoke detection alarm*)-Systeme in vielen Rechenzentren zur Brandfrühsterkennung mittels Erfassung durch Luftproben eingesetzt. Zur Brandlöschung finden verschiedene Löschsysteeme Verwendung, wobei in Rechnerräumen vorzugsweise Gaslöschanlagen eingesetzt werden, da sie keine Zerstörung der Geräte durch Wasserflutung hervorrufen [14]. Insgesamt wird in Rechenzentren darauf geachtet, dass in Räumen mit elektronischen Geräten keine Wasserleitungen durchlaufen und zusätzlich Wassermelder installiert werden.

Neben dem Schutz vor Feuer, Blitz und Wasser erfordert eine sichere IT-Basisinfrastruktur im besonderen Maße auch einen Schutz gegen Bedrohung durch unbefugte Dritte (Außentäter) und durch unbefugte Betriebsangehörige (Innentäter) [15]. Im Rahmen eines Gesamtkonzepts der Zutrittsregulierung und des Zutrittsschutzes werden verschiedene Bereiche berücksichtigt. Der Perimeterschutz umfasst den Außenbereich des Gebäudes bis zur Fassade (Gelände und Umzäunung), der Peripherieschutz die Gebäudehülle mit den damit verbundenen Öffnungen (Dach, Fenster, etc.) und der Raumschutz den gesamten Innenraum (Korridore, Zugangstüren, etc.). Um den Zutritt durch unbefugte Personen zu erschweren, werden Zutrittsbarrieren wie Zäune, Poller oder Durchfahrtssperren als physische Hindernisse geschaffen. Innerhalb des Geländes dienen u.a. Schleusen, Vereinzelungseinrichtungen oder Ausweisleser als Barrieren. Erweiterten Schutz bieten Wachdienste sowie automatische Einbruch- und Gefahrenmeldeanlagen. Darüber hinaus verfolgen zusätzliche Zutrittskontrollen das Ziel, nur Berechtigten den Zutritt zu bestimmten Bereichen zu ermöglichen. Die Kontrolle kann durch Pförtnerdienste oder durch den Einsatz von Zutrittskontrollanlagen realisiert werden.

Neben Schließsystemen mit konventionellen Schlössern und Kartensystemen (z.B. Magnetstreifenkarten oder Chipkarten) existieren Systeme, die auf speziellen Authentifizierungstechniken (z. B. biometrische Systeme) basieren.

Ein ganzheitliches Zutrittsregulierungs- und Schutzkonzept erfordert somit ein Zusammenwirken verschiedener baulicher, organisatorischer und personeller Maßnahmen. Zusammenfassend benötigt eine hochverfügbare und gleichzeitig sichere Basisinfrastruktur neben redundant ausgelegter Energieversorgung, Klimatisierung und Netzwerkanbindung auch eine Vielzahl von Schutzmaßnahmen, die physische und technische Sicherheit gewährleisten.

3. Untersuchungsmethodik

Die Auslagerung von IT-Basisinfrastrukturdiensten ist eine aktuelle Entwicklung im IT-Outsourcingmarkt. Die nachfolgende empirische Untersuchung verfolgt das Ziel einer Bestandsaufnahme. Neben aktuellen Herausforderungen sollen insbesondere die Kundenbedürfnisse, Auslagerungschancen und –risiken sowie Nutzenaspekte mentaler Konfigurationen dieser Auslagerungsform exploriert werden

Zur Erkenntnisgewinnung wurde ein semi-strukturierter Interviewleitfaden erarbeitet, der als Basis für eine Reihe von Experteninterviews diente. Dieser Leitfaden wurde nach jedem Interview erneut überprüft und ggf. durch neue Erkenntnisse verändert oder ergänzt. Zusätzlich auftretende Fragestellungen wurden in das Gespräch aufgenommen und in spätere Interviews eingearbeitet.

Bei der Auswahl der Teilnehmer wurden aufgrund der hohen Sicherheitsanforderungen gezielt Finanzdienstleister und Systemintegratoren ausgewählt. Im Finanzdienstleistungssektor, insbesondere im Bankenbereich, hat sich Outsourcing als Managementwerkzeug in jüngerer Vergangenheit etabliert [16]. Durch die Anforderung, Kosten zu senken und gleichzeitig Qualität und Effizienz zu steigern, sehen Finanzdienstleister die Notwendigkeit, grundlegend ihre Wertschöpfungsstrukturen von der Auslagerung einzelner IT-Aufgaben bis hin zur Externalisierung kompletter Geschäftsprozesse zu überprüfen [17]. Um ein differenziertes Bild innerhalb des Finanzdienstleistungssektors zu erhalten, wurden gezielt Unternehmen mit verschiedenen Schwerpunkten in ihrer Geschäftstätigkeit

ausgewählt. Neben Finanzdienstleistern wurden zudem Systemintegratoren als potenzielle Nachfrager nach Basisinfrastrukturdiensten identifiziert. Die befragten Unternehmen zählen gemäß einer Studie von PAC zu den größten Anbietern innerhalb des deutschen Outsourcingmarktes [18]. Die Auswahl der jeweiligen Interviewpartner konzentrierte sich auf Personen mit spezifischem Fachwissen im Bereich von IT-Basisinfrastrukturen und entsprechender Entscheidungsverantwortung. Es konnten insgesamt 11 Unternehmen zur Teilnahme an der Untersuchung gewonnen werden. Davon waren sieben Unternehmen Finanzdienstleister und vier Unternehmen Systemintegratoren. Alle Interviews wurden aufgezeichnet und anschließend transkribiert. Die Auswertung erfolgte im Anschluss mit QSR NVivo, einer Software zur qualitativen Datenanalyse [19]. Dazu wurden die Aussagen der Teilnehmer zunächst innerhalb der eigenen Branche gegenüber gestellt, Gemeinsamkeiten bzw. Widersprüche aufgedeckt und anschließend mit der anderen untersuchten Branche verglichen.

4. Empirische Befunde

4.1 Herausforderungen im Hinblick auf die IT-Basisinfrastruktur

Auf die allgemeine Frage, welchen Herausforderungen sich Unternehmen aktuell im Hinblick auf die IT-Basisinfrastruktur ausgesetzt sehen, äußerte lediglich ein Finanzdienstleister, dass momentan keine Herausforderungen in diesem Bereich auftreten. Vier von sieben Unternehmen der Finanzdienstleistungsbranche sehen neue Anforderungen im Zusammenhang mit der Erweiterung bzw. Verlagerung der Rechenzentrumsfläche. Systemintegratoren sehen die primäre Herausforderung in der Bereitstellung einer hochverfügbaren Infrastruktur für ihre Kunden. Damit verbunden sind erhöhte Anforderungen an ihre Rechenzentrumsflächen aufgrund immer leistungsfähiger werdender Geräte. Auf weniger Fläche konzentriert sich zunehmend mehr Technik, so dass höhere Anforderungen an die Klima- und Energieversorgung, Verkabelung sowie Netzwerktechnik entstehen.

Verfügbarkeit als Herausforderung

Insbesondere bei Finanzdienstleistungsunternehmen kann bereits ein kurzer Ausfall von wichtigen Applikationen geschäftskritisch werden. Eine hohe Verfügbarkeit der technischen Systeme ist deshalb unverzichtbar. Systemintegratoren haben ebenfalls hohe Verfügbarkeitsanforderungen. Dabei kommt es bei der Ausgestaltung darauf

an, welchen Endkunden sie ihre Dienstleistungen zur Verfügung stellen. Insbesondere bei Banken als Kunden sind die Anforderungen sehr hoch. Eine Einschätzung der maximal vertretbaren Ausfallzeiten hinsichtlich der Komponenten Strom, Klima und Netzwerk zeigt Tabelle 1:

Infrastrukturkomponente Max. Ausfall	Finanzdienstleister							Systemintegratoren		
	01	02	03	04	05	06	07	A	B	C
Strom	0	0	0	0	0	wenige Min.	0	10 Min.	0	0
Klima	30 Min	1 h	20 Min.	30 Min.	15 Min.	k. A.	0	k. A.	15 Min.	15 Min.
Netzwerk	0	10 Min.	0	4 h	8 h	2 h	0	0	0	k. A.

Tabelle 1: Maximal zulässige Ausfallzeiten

Von allen Unternehmen wird die Unterbrechung der Stromversorgung als sehr geschäftskritisch eingestuft, da schon ein kurzer Ausfall signifikante Folgen für den Geschäftsbetrieb hat. Inwieweit ein Ausfall der Klimatisierung sichtbare Schäden hervorruft, ist von der Anzahl der Geräte bzw. von der Aufstellung der Geräte im Rechnerraum abhängig. Die Bandbreite variiert von keiner bis zu einer Stunde Ausfallzeit. Insgesamt ist erkennbar, dass eine hochverfügbare IT-Basisinfrastruktur von hoher Wichtigkeit für die beteiligten Unternehmen ist.

Sicherheit als Herausforderung

Aus Sicht der verantwortlichen Aufgabenträger bietet die eigene Basisinfrastruktur insgesamt einen hinreichenden Schutz gegen Risiken. Vor allem die Gefahr eines *Stromausfalls* wird als gering eingestuft. Eine redundante Auslegung der Stromversorgung (n+1) in Verbindung mit USV-Aggregaten ist bei allen beteiligten Unternehmen durchgängig vorhanden. Dies belegt, dass die hohen Anforderungen an Verfügbarkeit durch die Umsetzung einer sicheren Stromversorgung gelöst werden. Am häufigsten wurden von den Beteiligten *Netzwerkfehler* als potenzielle, wengleich auch nur als mittlere Gefährdung genannt. Die Hälfte aller befragten Unternehmen sieht bereits in der Redundanz durch zwei Netzwerk-Zugänge eine gute Absicherung gegen Ausfälle bzw. Fehler des Netzwerks. Die anderen 50 %

begründen ihre kritischere Einschätzung damit, dass man bei der Anbindung an ein Fernnetz von externen Anbietern abhängig ist. Risikoerhöhend kommt hinzu, dass Netzwerkleitungen über eine große Distanz verlaufen und intelligente Netzwerk-Komponenten (z. B. Router, Switches, Server) dazwischen geschaltet sind. Die Vielzahl der beteiligten Komponenten kann zu Störungen führen.

Auf die Frage nach den Risikoarten *Vandalismus* und *Sabotage* als innere Risiken konnte von keinem der teilnehmenden Unternehmen Gefahren völlig ausgeschlossen werden. Risiken durch Menschen seien schwer einschätzbar. Durch systematische Zutrittskontrollen und -berechtigungen wird der Kreis derjenigen, die einen Rechnerraum betreten dürfen, deshalb stark eingeschränkt. Gegen *Terrorismus*, also Risiken von außen, wurden bei den Unternehmen eine Vielzahl von Schutzvorkehrungen durch bauliche Maßnahmen und Objektschutz an den Standorten der Rechenzentren umgesetzt. Eine Terrorismusgefahr wird insgesamt nicht als hoch eingeschätzt, wenngleich die Terrorangriffe des 11. September 2001 zu einer erhöhten Sensibilisierung geführt haben. Um vor Gefahren durch Terrorangriffe sicher zu sein, ist die Art und Weise des Schutzes der Datenbestände wichtig. Physisch werden sie durch bauliche, sicherheitstechnische und organisatorische Maßnahmen abgesichert. Unbefugter Zugang sowie Diebstahl und Zerstörung von Hardware kann so verhindert werden. Das Vorhandensein von Hardwarekomponenten in mehrfacher Ausführung und an unterschiedlichen Standorten kann das Risiko von Datenverlusten durch vollständige Redundanz (Spiegelung) der Daten minimieren. Ein Ersatzrechenzentrum übernimmt dann im Falle von Störungen die Aufgaben des Hauptrechenzentrums. Alle befragten Firmen haben mindestens zwei Rechenzentren. Es kann sich dabei um ein Hauptrechenzentrum und ein Nebenrechenzentrum handeln oder auch um eine „dual-all“-Lösung, bei der jedes Rechenzentrum produktiv ist und gleichzeitig als Backup-Rechenzentrum des anderen fungiert. Bei synchroner Spiegelung der Daten sind die Daten an beiden Standorten zeitgleich verfügbar. Allerdings lässt sich diese Variante nach Aussagen der interviewten Experten aufgrund technischer Restriktionen nur bei einer maximalen Distanz von ca. 40 - 50 km umsetzen. Für größere Entfernungen besteht die Möglichkeit der asynchronen Spiegelung, die aber eine zeitverzögerte Bereitstellung der Daten zur Folge hat. Damit geht die Gefahr

einher, dass bei einem Ausfall durch die Verzögerung wichtige Daten verloren gehen können.

Ein Finanzdienstleistungsunternehmen denkt darüber nach, zukünftig neben zwei synchron gespiegelten RZ-Standorten noch einen dritten Standort in mehreren hundert Kilometer Entfernung vorzuhalten. Dort sollen dann die wichtigsten Applikationen verfügbar sein, damit schlimmstenfalls zumindest die Überlebensfähigkeit des Unternehmens gesichert ist. Ein solches Szenario könnte beispielsweise auftreten, wenn durch einen Terrorangriff beide sich nahe zueinander befindlichen RZ-Standorte zerstört würden. Solche Standorte werden daher auch als Ausfallrechenzentrum, Notfall- und Katastrophenzentrum (NuK) oder Disaster Recovery-Rechenzentrum bezeichnet.

Ökonomische Herausforderungen

Neben den Attributen Sicherheit und Verfügbarkeit sehen sowohl Finanzdienstleister als auch Systemintegratoren ökonomische Herausforderungen in Bezug auf ihre IT-Basisinfrastruktur. Die befragten Finanzdienstleistungsunternehmen äußerten sich sehr unterschiedlich zu der Frage, ob ihre Basisinfrastruktur aktuell den allgegenwärtigen Kostendruck absorbieren muss. Mehrheitlich wurde die Aussage getroffen, dass Kosten zwar genau betrachtet werden, aber darunter die Qualität der Basisinfrastrukturdienste nicht leiden darf. Priorität hat bei den Finanzdienstleistern die Bereitstellung einer hochverfügbaren Infrastruktur, die den hohen internen Vorgaben und zusätzlichen externen regulatorischen Anforderungen (z.B. Kreditwesengesetz (KWG) oder Basel II) gerecht wird. Auch Opportunitätskosten eines evtl. Ausfalls der Systeme spielen eine große Rolle bei den Kostenüberlegungen. Bei Systemintegratoren hingegen wird der Kostendruck bei Infrastrukturmaßnahmen expliziter berücksichtigt. Aufgrund der zunehmenden Preissensibilität der Anwenderunternehmen werden die eigenen Mitarbeiter angehalten, verfügbare Einsparpotenziale aktiv auszuschöpfen.

Insgesamt wird in beiden Branchen großer Wert auf eine sichere und hochverfügbare Infrastruktur gelegt, und dementsprechend werden kaum Zugeständnisse aufgrund von Kostenüberlegungen gemacht.

Durch die *Konsolidierung* der eigenen Basisinfrastruktur wird von den großen Unternehmen versucht, historisch gewachsene Strukturen zu erneuern, um sie dem aktuellen Stand der Technik anzupassen und die Qualität verbessern zu können. Durch die Konsolidierung verfolgen die beiden größten Finanzdienstleister auch das Ziel einer Kostenersparnis. Synergie-Effekte und höhere Effizienz der Rechenzentrumsinfrastruktur werden angestrebt. Allerdings birgt bei Systemintegratoren eine Konsolidierung der Basisinfrastruktur die Gefahr, dass durch die Zusammenführung verschiedener Kunden an einem Standort die Überschaubarkeit geringer wird. Die Komplexität wird erhöht und dies hat steigende Managementkosten zur Folge.

Als weitere ökonomische Herausforderungen werden von den Finanzdienstleistern und Systemintegratoren die Erhöhung der *Flexibilität* und *Skalierbarkeit* erachtet. Die Ausnahme bilden die beiden größten Finanzdienstleister in der Untersuchung. Dort werden Projekte frühzeitig geplant und mit der Geschäftsleitung abgestimmt, so dass die Notwendigkeit einer kurzfristigen Reaktion im Basisinfrastrukturbereich auf ein Minimum beschränkt wird. Des Weiteren wird in diesen Unternehmen die Skalierbarkeit aufgrund großzügig ausgelegter Ressourcen als weniger kritisch angesehen. Fünf von sieben Finanzdienstleistern sehen in der Erhöhung der Flexibilität und Skalierbarkeit eine große Chance, kurzfristig auf neue Anforderungen reagieren zu können. Diese Unternehmen nutzen auch spezialisierte Anbieter von Basisinfrastrukturlösungen. Dort können Optionsflächen angemietet werden, die im Bedarfsfall zu Rechenzentrumsflächen ausbaufähig sind. Insbesondere die verkürzte „time-to-market“ im Vergleich zur Eigenerstellung von Technikflächen und der verringerte Investitionsbedarf werden dabei als Vorteil gesehen. Bei Systemintegratoren sind die Erfordernisse an eine schnelle Reaktion durch mehrere zu betreuende Kunden mit unterschiedlich wachsendem Flächenbedarf noch höher. Von Systemintegratoren wird erwartet, dass sie schnell auf neue Kundenanforderungen reagieren können. Deshalb wird versucht, zukünftige Bedarfe und Entwicklungstrends hinreichend zu antizipieren. Falls ein höherer Bedarf nicht mit eigenen Ressourcen abgedeckt werden kann, werden Rechenzentrumsflächen von externen Anbietern angemietet. In Verbindung mit der Skalierbarkeit der Fläche geht auch die Skalierbarkeit der Strom- und Klimaversorgung einher. Neuere Geräte

werden zwar kleiner und leistungsfähiger, aber sie stellen eine erhöhte Anforderung an Klimatisierung und Stromversorgung dar. Systemintegratoren erwarten von einem externen Anbieter, dass dieser nicht nur den wachsenden Flächenbedarf abdeckt, sondern dass auch die mit dem Flächenbedarf verbundene technische Ausstattung entsprechend skalierbar ist. Genau dies erwarten die Mandanten der Systemintegratoren, was eine weitere Herausforderung darstellt.

Die Befunde zeigen, dass sich Unternehmen im Kontext der IT-Basisinfrastruktur einer Vielzahl von Herausforderungen stellen müssen. In Abbildung 2 werden die aktuellen Herausforderungen noch einmal im Überblick dargeboten.

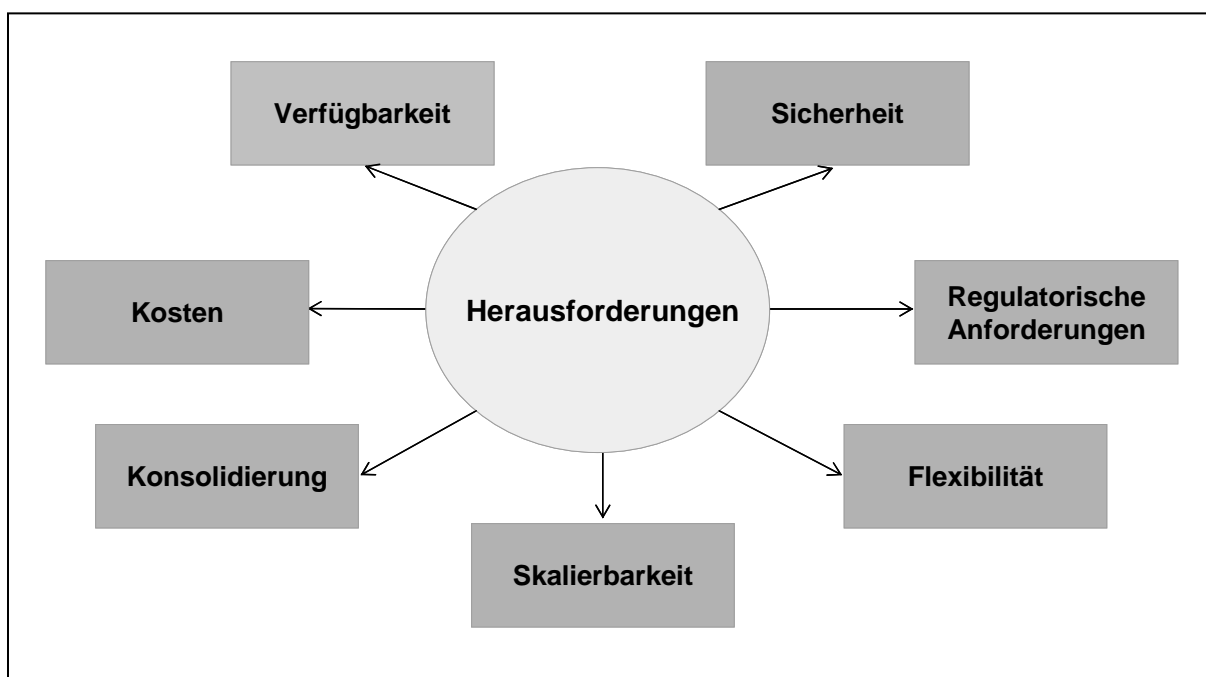


Abbildung 2: Herausforderungen an IT-Basisinfrastruktur

3.2 Die Auslagerung der IT-Basisinfrastruktur als Handlungsoption

Neun der elf befragten Unternehmen haben entweder ihre Basisinfrastruktur ausgelagert oder mieten Rechenzentrumsflächen aufgrund eines gewachsenen Flächenbedarfs bei Spezialanbietern an. Lediglich zwei Unternehmen lehnen die Auslagerung von Aufgaben in diesem Kontext ab, da Informationstechnologien jeweils als Kernkompetenz und geschäftskritisch angesehen werden.

Motive für eine Auslagerung

Die Entscheidung für eine Auslagerung der Basisinfrastruktur hat bei Finanzdienstleistern mehrere Gründe. Im spezifischen Fach- und Erfahrungswissen von spezialisierten Anbietern von Basisinfrastrukturdiensten sehen Finanzdienstleister eine Verbesserung der Qualität gegenüber der bisher selbst betriebenen Infrastruktur. Die Option, durch ein Outsourcing schnell auf Kapazitätsengpässe reagieren zu können, stellt einen weiteren Treiber dar. Ein Spezialanbieter ist im Stande, fertig ausgebaute Technikflächen in kurzer Zeit bereit zu stellen. Hohe und langfristige Investitionen in Einzelkomponenten, wie z.B. Klimageräte, USV-Aggregate und Dieselgeneratoren können so vermieden werden. Spezialanbieter nutzen Synergien, indem sie die Komponenten für mehrere Mieter einsetzen können. Neben der Qualitätsverbesserung ist die Motivation der Auslagerung bei Finanzdienstleistern insbesondere in der Kosteneffizienz und Flexibilität zu sehen. Auch Systemintegratoren möchten sich durch eine Flächenanmietung einen Zugang zu hoher Qualität verschaffen. Ebenso ist auch das flexible Reagieren auf neue Anforderungen durch ein verkürztes „time-to-market“ ein wichtiger Treiber. Schließlich wird eine Fokussierung auf Kernkompetenzen ermöglicht. Systemintegratoren können so vorhandene Ressourcen gewinnbringender einsetzen. Ein weiterer wichtiger Grund bei der Entscheidung für einen externen Anbieter ist die Möglichkeit des Zugangs zu mehreren Netzanbietern (carrier). Ein Standort ohne entsprechenden Zugang zu Fernnetzen ist für Systemintegratoren ungeeignet, da die Anbindung an verschiedene Netzanbieter sonst nur mit erheblichem Aufwand zu realisieren ist.

Chancen und Risiken einer Auslagerung

Die angesprochenen Haupttreiber einer Entscheidung für eine Auslagerung von Basisinfrastrukturdiensten sind eng mit den Chancen dieser Form des selektiven Outsourcings verbunden. Qualitätsverbesserungen resultieren, wie bereits beschrieben, aus dem spezifischen Know-how und den infrastrukturbezogenen Ressourcen des Dienstleistungsanbieters. Spezialisierte Anbieter setzen moderne, aufeinander abgestimmte Technologien ein und gewährleisten eine hohe Versorgungssicherheit. Darüber hinaus können interne Kapazitäten freigesetzt werden. Mitarbeiter, die sich zuvor um die Basisinfrastruktur gekümmert haben, erhalten Freiräume, um näher am Kerngeschäft des Unternehmens agieren zu können. Somit resultiert daraus auch die Chance, die Qualität der eigenen

Dienstleistungen zu verbessern. Ein kleineres Finanzdienstleistungsunternehmen sieht durch die Auslagerung die einzige Möglichkeit überhaupt einen angemessenen Qualitätsstandard sicher zu stellen. Des Weiteren wird von den untersuchten Unternehmen in der Auslagerung der Basisinfrastruktur die Chance gesehen, Rechenzentrumsflächen nach aktueller Bedarfslage zu vergrößern bzw. zu verkleinern, d.h. Flächen können vom Anbieter innerhalb von kurzer Zeit bereitgestellt werden. Die Zeit, bis eine fertig ausgebaute RZ-Fläche zur Verfügung steht, wird im Vergleich zu einer Eigenerstellung erheblich reduziert. Der Flächenbedarf kann so an das Geschäftswachstum skalierbar angepasst werden. Eine erhöhte Flexibilität spiegelt sich auch in kurzfristigeren Mietverträgen (mit Laufzeiten ab fünf Jahren) im Vergleich zu einer langfristigen Investition in einen eigenen Standort wider. Eine Kapitalbindung in Aktivitäten, die nicht zum Kerngeschäft zählen, kann dadurch reduziert werden.

Sofern bei der Vertragsgestaltung die Dienstleistungen des betreffenden Anbieters umfassend und eindeutig spezifiziert sind, kann dies zu mehr Kostentransparenz führen. Werden allerdings keine klaren Regelungen zwischen dem auslagernden Unternehmen und dem Dienstleister getroffen, hat dies eine mangelnde Überschaubarkeit der Leistungen zur Folge. Die Abhängigkeit vom Anbieter wird daher auch als mögliches Risiko von den untersuchten Unternehmen betrachtet. Risiken des Verlustes von Fachwissen und Einflussmöglichkeiten spiegeln sich darin wider. Durch den Vertrag mit einem spezialisierten Unternehmen wird eine zusätzliche Schnittstelle geschaffen, die es zu kontrollieren gilt. Dies kann u.U. zu längeren Entscheidungswegen führen und einem erwünschten Flexibilitätsgewinn entgegen stehen.

Ebenso wird eine Gefahr im opportunistischen Verhalten bei mangelnder Leistungsqualität des Anbieters gesehen. Diese Risiken können im Vorfeld schon durch einen klar definierten Leistungsumfang in einer sog. Service Level Agreement (SLA) minimiert werden. Eine derartige Regelung ermöglicht einen Machtausgleich zwischen den Vertragspartnern. Zu den wichtigen Bestandteilen eines SLA-Dokuments gehört neben der detaillierten Leistungsbeschreibung die Regelung der Kommunikation, des Know-how-Transfers, des Störungs- und Problemmanagements, der Entlohnung, der Haftungsregelungen sowie von

Vereinbarungen über eine gemeinsame Sicherheitsstrategie. Bei der Aushandlung von SLA wird es von einigen befragten Unternehmen als schwierig erachtet, dass entweder lange Verhandlungen zur Regelung aller Details nötig sind oder Interpretationsspielräume bei Servicenehmern und -gebern auftreten. [20] Schließlich wird von den Teilnehmern noch ein Risiko in einer mangelnden Akzeptanz innerhalb des Unternehmens gesehen, da eine Auslagerung zwangsläufig auch eine Veränderung des Aufgabenfeldes der Mitarbeiter nach sich zieht. Da in den Aussagen der beiden untersuchten Branchen keine wesentlichen Unterschiede erkennbar waren, stellt Tabelle 2 zusammenfassend die Chancen und Risiken einer Auslagerung der IT-Basisinfrastruktur in einer Argumentebilanz gegenüber.

Auslagerung der IT-Basisinfrastruktur	
Chancen	Risiken
<ul style="list-style-type: none"> <input type="checkbox"/> Qualitätsverbesserung (Kompetenz, moderne, spezielle und aufeinander abgestimmte Komponenten) <input type="checkbox"/> Versorgungssicherheit (Klima, Strom, Carrier-Anbindung) <input type="checkbox"/> Kosteneffizienz (Skaleneffekte, geringere Kapitalbindung) <input type="checkbox"/> Kostentransparenz (klar definierter Service- /Leistungsumfang, SLA) <input type="checkbox"/> Flexibilitätsgewinn (verkürztes „time-to-market“, kurzfristige Mietverträge) <input type="checkbox"/> Skalierbarkeit (bedarfsgerechtes Anmieten von RZ-Flächen) <input type="checkbox"/> Fokussierung auf Kernkompetenzen (Optimierung der IT-Fertigungstiefe) 	<ul style="list-style-type: none"> <input type="checkbox"/> Qualitätsverluste (geringere eigene Qualitätsanforderungen des Anbieters, mangelndes branchenspezifisches Know-how) <input type="checkbox"/> Intransparenz der Leistung (bei uneindeutig geregeltem Leistungsumfang) <input type="checkbox"/> Abhängigkeit vom Anbieter (geringere Einflussmöglichkeiten, Know-how Verlust) <input type="checkbox"/> Verlängerung von Entscheidungswegen (Schaffung von zusätzlicher Schnittstelle) <input type="checkbox"/> Flexibilitätsverlust (durch lange, detaillierte SLA-Verhandlungen) <input type="checkbox"/> Erhöhter Managementaufwand (Koordinationskosten, Controllingaufwand) <input type="checkbox"/> Mangelnde Akzeptanz der Mitarbeiter (reduziertes Aufgabenfeld der Mitarbeiter)

Tabelle 2: Chancen/Risiken bei einem Outsourcing von IT-Basisinfrastrukturen

Ideales Leistungsbündel aus Kundensicht

Auf die Frage, welches Leistungsbündel sich Kunden idealerweise von einem Basisinfrastrukturanbieter wünschen, antworteten jene Teilnehmer, die bereits eine solche Form der Auslagerung gewählt haben, dass ein ideales Angebot bereits am Markt verfügbar sei. Das Konzept wird als in sich stimmig erachtet. Positiv hervorgehoben wird von Unternehmen aus der Finanzdienstleistungsbranche, dass das Angebot der spezialisierten Anbieter schlank gehalten ist. Die Schnittstelle zum Outsourcer ist somit überschaubar und gut zu kontrollieren. Aus diesem Grund präferieren die befragten Finanzdienstleister den selektiven Bezug externer Basisinfrastrukturdienste im Rahmen eines separaten Outsourcingvertrages und nicht die Einbettung von Infrastrukturdiensten als Bestandteil eines kompletten Outsourcings.

Zwei der drei Systemintegratoren sehen in den Basisinfrastrukturdiensten eine Kernkompetenz ihrer Geschäftstätigkeit, wohingegen ein Unternehmen in diesem Segment in der entsprechenden Auslagerung eine nutzbringende Lösung für die eigene Geschäftstätigkeit sieht. Zu einem optimalen Leistungsangebot gehört für Systemintegratoren vor allem die Skalierbarkeit und die Fähigkeit des Anbieters, kurzfristig auf neue Anforderungen reagieren zu können. Von Finanzdienstleistern und Systemintegratoren wird die Anmietung von „fitted-out“ Räumlichkeiten präferiert, die idealerweise nach kundenindividuellen Anforderungen ausgebaut sind. Darüber hinaus gehende Dienste, wie z.B. die Beschaffung von Systemkomponenten oder das System-Management, fragen Finanzdienstleister vorzugsweise in Form eines selektiven Outsourcings bei darauf spezialisierten Unternehmen nach. Da Systemintegratoren selbst als Outsourcingdienstleister am Markt agieren, besteht kein Bedarf, zusätzliche Infrastrukturdienste bei einem IT-Basisinfrastrukturanbieter zu beziehen.

Zusammenfassend beinhaltet ein ideales Leistungsbündel aus der Sicht der befragten Unternehmen eine Bereitstellung einer hochverfügbaren und sicheren IT-Basisinfrastruktur von einem spezialisierten Anbieter, der kundenindividuell ausgebaute Räumlichkeiten flexibel und skalierbar anbieten kann.

Zukünftige Entwicklung

Nach Einschätzung der Gesprächspartner wird die Nachfrage nach Basisinfrastrukturdiensten in den nächsten Jahren ansteigen, wenngleich die Mehrzahl der Teilnehmer ein moderates Wachstum erwartet. Sechs von sieben interviewten Finanzdienstleistern sehen insbesondere eine zunehmende Nachfrage bei kleineren mittelständischen Unternehmen, die entweder wenig Erfahrung mit der Errichtung und dem Management komplexer IT-Basisinfrastrukturen haben oder nicht über die erforderlichen Ressourcen hierzu verfügen. Nach Ansicht der Teilnehmer wird vor allem zukünftig von kleineren Unternehmen, in denen Informationstechnologien keine wettbewerbsrelevante oder geschäftskritische Bedeutung besitzen, eine verstärkte Nachfrage nach Basisinfrastrukturdiensten ausgehen. Für Unternehmen, die einem starken Kostendruck ausgesetzt sind, entsteht die Möglichkeit, Fixkosten in variable Kosten umzuwandeln und damit die Kapitalbindung in einer Aktivität, die nicht zum Kerngeschäft zählt, zu verringern. Miet- bzw. Dienstleistungsverträge ersetzen langfristige Investitionen in eigene Standorte.

Ein Outsourcingdienstleister kann seine Kapazitäten an die Nachfrage der einzelnen Kunden anpassen und mittels flexibler Preismodelle seine Dienstleistungen abrechnen (pay-per-use) [21]. Eine verstärkte Marktnachfrage von mittelständischen Unternehmen nach Disaster Recovery-Lösungen und Backup-Rechenzentren wird in den nächsten Jahren aus Sicht der Finanzdienstleistungsunternehmen erwartet. Da der Bezug von Basisinfrastrukturdiensten leicht umsetzbar ist, sehen vor allem Finanzdienstleister zukünftig ein verstärktes Interesse von kleineren Unternehmen.

Systemintegratoren beobachten im Zuge des schnellen Wachstums des gesamten IT-Outsourcingmarktes einen ungebrochenen Trend in der Nachfrage nach Basisinfrastrukturlösungen. Systemintegratoren erwarten insbesondere von Unternehmen im Bankensektor, dass sie diese Form der Auslagerung als Lösungsmöglichkeit verstärkt nutzen werden.

Die Erwartungen der Gesprächspartner zeigen, dass zukünftig von einem Wachstum dieser Auslagerungsform ausgegangen wird. Nahezu alle Finanzdienstleister identifizieren primär kleinere bzw. mittelständische Unternehmen als treibende Kraft

für den Anstieg und nicht explizit Unternehmen der eigenen Branche, wie es Systemintegratoren erwarten.

4. Fazit

Im vorliegenden Beitrag wurde die Auslagerung von Basisinfrastrukturdiensten als Form der selektiven Auslagerung von informationstechnologischen Aufgaben im Finanzdienstleistungssektor sowie im Systemintegrationsgeschäft mittels teilstrukturierter Interviews untersucht. Dabei wurden in der Analyse speziell Kundenbedürfnisse und der Nutzen betrachtet, der durch eine solche Auslagerung generiert werden kann. Die Basis der Untersuchung bildete eine Definition und Darstellung der einzelnen Basisinfrastrukturkomponenten. Dadurch konnten die grundsätzlichen Anforderungen geklärt und im Anschluss in der empirischen Untersuchung der Herausforderungen betrachtet werden. Es wurde deutlich, dass Hochverfügbarkeit und Sicherheit die zentralen Herausforderungen sowohl für Finanzdienstleister als auch für Systemintegratoren sind. Daneben stellen Flexibilität, Skalierbarkeit und Konsolidierung aktuelle Herausforderungen für beide Gruppen dar. Als wesentlichen Treiber zur Nutzung externer Ressourcen konnten erhöhte Qualitätserfordernisse und Kapazitätsengpässe identifiziert werden.

Neben einer Qualitätsverbesserung durch hochwertige Ressourcen des Anbieters und einer Versorgungssicherheit durch redundante Bereitstellung von Strom, Klima und Anbindungen an Netzanbieter wurden Kosteneffizienz, Flexibilität, Skalierbarkeit und die Fokussierung auf Kernkompetenzen als Chancen der Auslagerung der IT-Basisinfrastruktur gesehen. Dem gegenüber konnten aber auch potentielle Risiken aus Sicht der Endnutzer ermittelt werden. Hierbei wurden vor allem Gefahren durch Intransparenz der Leistung und Abhängigkeit vom spezialisierten Serviceanbieter genannt.

Mit der empirischen Untersuchung konnte gezeigt werden, dass diese spezifische Form der Auslagerung den befragten Unternehmen Nutzen stiften kann. Dieser Nutzen wird durch den Zugang zu sicheren und hochverfügbaren Ressourcen sowie durch die Möglichkeit geschaffen, flexibel auf neue Markterfordernisse zu reagieren. Insgesamt wurde deutlich, dass eine Auslagerung der Basisinfrastruktur bei Unternehmen, die IT als ihre Kernkompetenz ansehen, zu einer Externalisierung und

Fragmentierung einzelner Stufen der IT-Wertschöpfungskette führt. Die damit zunehmende zwischenbetriebliche Arbeitsteilung führt einerseits zu Qualitäts- und Kostenvorteilen. Sie erhöht aber andererseits auch die Managementkomplexität und induziert mögliche Abhängigkeiten, die vor der Auslagerung von Infrastrukturkomponenten aufmerksam berücksichtigt werden sollten.

Literaturquellen:

- [1] **Heinzl, A. (2001):** *Outsourcing der IV*; in: Mertens, P. (Hrsg.): Lexikon der Wirtschaftsinformatik, Springer, Berlin [u. a.], 2001, S. 359 f.
- [2] **Kennedy, E./Irshad, K. (2003):** *Top 100 European Outsourcing Deals of 2002*, IDC, London [u. a.], 2003, S. 15 f.
- [3] **Georgius, A./ Heinzl, A.:** Strategien und Erfolgsfaktoren von Anbietern im IT und Business Process Outsourcing in Deutschland; erscheint in: Ferstl, O./Sinz, E. (Hrsg.): eEconomy, eGovernment, eSociety – Proceedings der 7. Internationalen Tagung Wirtschaftsinformatik, Bamberg 2005.
- Lacity, M. C./Willcocks, L. P. (2001):** *Global information technology outsourcing : in search of business advantage*; Wiley, Chichester [u. a.], 2001, S. 3.
- [4] **Zimmermann, S./Hafen, D. (2003):** *Rechenzentren kämpfen ums Überleben*; in: Network World, Band Heft 11, S. 30 f.
- [5] **Applegate, L. M./Austin, R. D./McFarlan, F. W. (2003):** *Corporate information strategy and management : text and cases*; 6. Aufl., McGraw-Hill, Boston u. a., 2003, S. 401.
- [6] **Chase, E. (2001):** *Mission critical: Assessing the benefits of in-house vs. outsourced managed environments*, Digiplex, Oslo, 2001, S. 16.
- [7] **Sarsam, R. (2002):** *Web-Hosting: Der Vorhang ist gefallen*, Computerwoche Online; in:<http://www.computerwoche.de/index.cfm?pageid=254&artid=38094&type=detail&kw=Co> location, abgerufen am: 16.02.2004.
- [8] **BSI (2003):** *IT-Grundschutzhandbuch*, Bundesamt für Sicherheit und Informationstechnik; in: <http://www.bsi.de/gshb/deutsch/menuue.htm>, abgerufen am: 26.03.2004.
- [9] **Probst, C. (2003):** *Referenzmodell für IT-Service-Informationssysteme*; Logos, Berlin, 2003, S. 36.
- [10] **Hoppe, G./Prieß, A. (2003):** *Sicherheit von Informationssystemen : Gefahren, Maßnahmen und Management im IT-Bereich*; Verlag Neue Wirtschafts-Briefe, Herne [u. a.], 2003, S. 259 f.

- [11] **Ovum (2002):** *Data Center and Telecom Hotels: After the space race*, Ovum, London [u. a.], 2002, S. 4.
- [12] **Bernstein, H. (2001):** *PC-Sicherheit*; VDE Verlag, Berlin [u. a.], 2001, S. 131.
- [13] **Applegate, L. M./Austin, R. D./McFarlan, F. W. (2003):** *Corporate information strategy and management : text and cases*; 6. Aufl., McGraw-Hill, Boston u. a., 2003, S. 430.
- [14] **Droux, D. (1984):** *Physische EDV-Sicherheit*; in: Liebl, K. (Hrsg.): *Computermissbrauch, Computersicherheit : Fälle - Abwehr - Aufdeckung*, Hohl, Ingelheim [u. a.], 1984, S. 282 ff.
- [15] **Weber, F./Stumm, S. (1997):** *IT-Sicherheit durch infrastrukturelle Maßnahmen*; Bundesanzeiger Verlagsges. mbH, Köln, 1997, S. 7.
- [16] **Lancelotti, R./Schein, O./Spang, S./Stadler, V. (2003):** *ICT and Operations outsourcing in banking - Insight from an interview-based pan-European survey*; in: *Wirtschaftsinformatik*, Band 45, Heft 2, S. 131.
- [17] **International Bankers Forum (2003):** *Mehr als Geld und Zinsen: Outsourcing im Deutschen Bankensektor*, Accenture International Bankers Forum e. V., Frankfurt am Main, Kronberg, 2003, S. 6.
- [18] **PAC (2003):** *Outsourcing Germany Update May 2003*, Pierre Audoin Consultants, München, 2003, S. 11.
- [19] **QSR (2002):** *Using NVivo In Qualitative Research*; QSR International, Melbourne, 2002.
- [20] **Löhr, R. (2004):** *Rechtliche Aspekte des Sourcing*; in: Scholtissek, S. (Hrsg.): *Sourcing: Die Toolbox: Wie Sie Ihre Wertschöpfungskette optimieren*, F.A.Z. - Institut für Management-, Markt- und Medieninformationen GmbH, Frankfurt am Main, 2004, S. 85 ff.
- [21] **Buchta, D./Eul, M./Schulte-Croonenberg, H. (2004):** *Strategisches IT-Management : Wert steigern, Leistung steuern, Kosten senken*; Gabler, Wiesbaden, 2004, S. 187.