Risiko- und Schwachstellen-Audit für IT-Architekturen

Matthias Mitze und Dirk Weidemann, OPITZ CONSULTING GmbH

IT-Infrastrukturen werden häufig unter einem hohen Druck aus dem Business ausgebaut. Vieles ist dabei kurzfristig auf Effizienz getrimmt – mitunter ohne Berücksichtigung mittel- und langfristig relevanter Faktoren wie Ausbaufähigkeit, Wartbarkeit und Sicherheit. Strukturierte IT-Audits bringen Licht ins Dunkel und zeigen mit Risikoanalyse und Handlungsempfehlungen einen technisch und betriebswirtschaftlich optimalen Weg auf.

IT-Infrastrukturen wachsen kontinuierlich und müssen immer größere Datenmengen in immer kürzerer Zeit verarbeiten. Jede Erweiterung oder Modifikation in Form von System-Updates oder Release-Wechseln kann dabei Implikationen auf die systemische Unterstützung zahlreicher Geschäftsprozesse haben. Umgekehrt stellen Letztere in Form von Compliance oder Hochverfügbarkeit auch immer wieder neue Anforderungen an die IT-Infrastruktur.

Zur Minimierung des Risikos von Systemausfällen und Sicherstellung einer skalierbaren IT-Infrastruktur, die den Unternehmensanforderungen gerecht wird, ist eine Transparenz unabdingbar – von der darauf aufsetzenden Daten- und Applikationsschicht bis hin zur Business-Perspektive. Nur auf Basis einer solchen Transparenz lässt sich eine Planungsgrundlage erstellen, mit der ein sicherer und wirtschaftlicher IT-Betrieb organisiert und dem Management gegenüber plausibel vertreten werden kann.

Zusammenhänge ermitteln, analysieren und bewerten

Die jeweiligen Zusammenhänge der Architektur-Ebenen in einem Unternehmen sollten die zuständigen Mitarbeiter gemeinsam ermitteln. Hier kann es in manchen Fällen von Vorteil sein, einen unabhängigen Berater hinzuzuziehen, der eine neutrale Vermittlerrolle übernehmen und außerdem auf Basis konkreter Erfahrungen aus erfolgreichen Projekten einen speziellen Fragenkatalog entwickeln kann. Eine hilfreiche Methode für die Analyse, Aufbereitung und Bewertung dieser Zusammenhänge stellt das sogenannte „Solution Engineering“ dar (siehe Abbildung 3).

Resultat der ersten Analyse ist ein Gesamtüberblick, der es ermöglicht, sowohl die einzelnen Artefakte als auch die Zusammenhänge aus jeweils unterschiedlichen Perspektiven (siehe Abbildung 1) zu betrachten und zu bewerten: Welcher Geschäftsbereich ist für welche Applikation verantwortlich? Welcher Server hostet wie viele Applikationen? Welche Auswirkungen hat ein Ausfall dieses Servers auf den Geschäftsbetrieb?

Audit: Erkenntnisse in Maßnahmen überführen

Zur systemischen Unterstützung dieses Vorgehens empfehlen die Autoren die Oracle BPA Suite sowie die ARIS-Methode (Architektur integrierter Informationssysteme). Damit lassen sich die Artefakte an sich sowie die direkten und indirekten Abhängigkeiten zwischen den einzelnen Architektur-Ebenen (siehe Abbildung 1) in einem zentralen Informations-Repository erfassen, durch Attribute detaillieren und nach nahezu beliebigen Kriterien in definierten Formaten (wie Microsoft Office, PDF oder HTML) auswerten. Spezialisten für IT-Architekturen, Datenbanken und Geschäftsprozesse sollten dann die erfassten Daten gemeinsam analysieren und in Form eines Auditberichts für das IT- und Unternehmens-Management aufbereiten.

Der Auditbericht beinhaltet in der Regel die Dokumentation der Stärken, Schwächen oder Risikofaktoren der IT-Infrastruktur – sowie darauf basie-

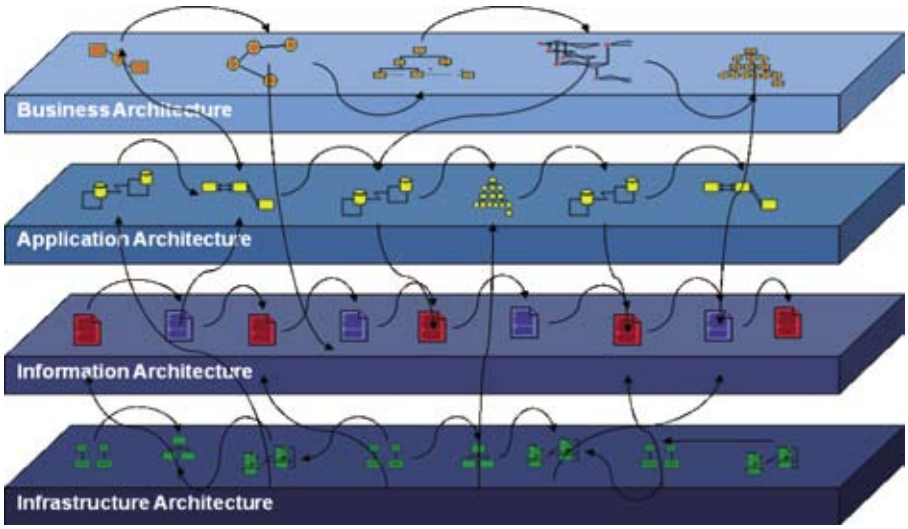

Abbildung 1: Architektur-Ebenen eines Unternehmens

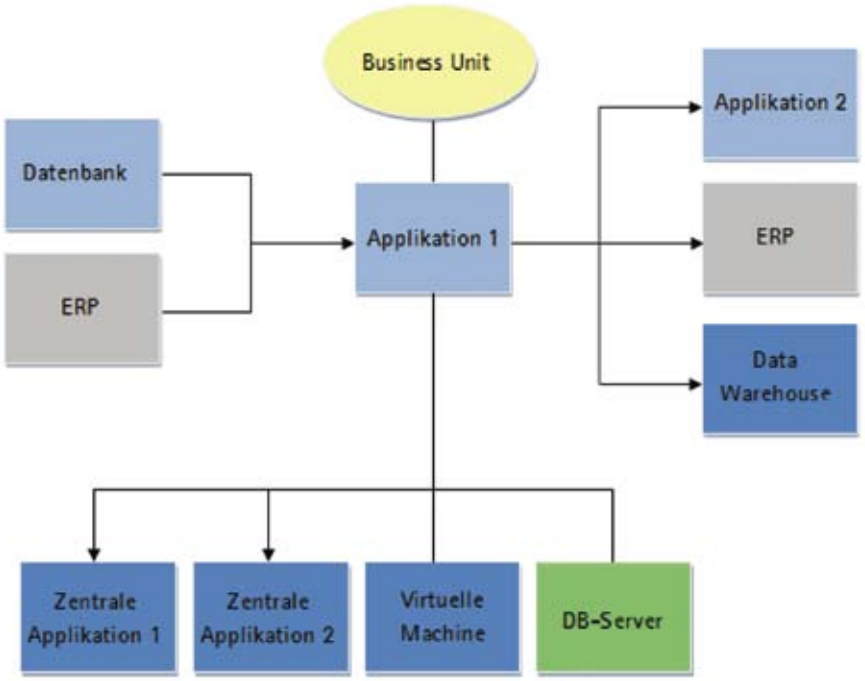

Abbildung 2: Zusammenhänge von Artefakten unterschiedlicher Architektur-Ebenen

rend – eine Handlungsempfehlung zur Durchführung von Optimierungsmaßnahmen oder von geplanten Änderungen der IT-Infrastruktur, die den Anlass für diese Analyse gegeben haben.

Strukturiertes Vorgehen in fünf Stufen

Zur Schaffung einer Transparenz hat sich in der Praxis ein mehrstufiges Audit-Vorgehensmodell bewährt, das von der Planung, über die Datenerhebung zur Analyse und Bewertung führt und in einer anschließenden Empfehlung mündet.

Stufe 1: Kick-off

Zu Beginn erfolgt im Kick-off eine detaillierte Planung und Zielfestlegung für das Projekt:

- Schaffung eines gemeinsamen Verständnisses für das anstehende Vorhaben
- Abstimmung einer gemeinsamen detaillierten Zieldefinition
- Festlegung der Informationsquellen
- Klärung der organisatorischen Rahmenbedingungen und des Rahmenterminplans

Stufe 2: Datenerhebung

Die Phase der Datenerhebung teilt sich in die Arbeitspakete „Dokumente sichten“, „Prozesse identifizieren“ und „IT-Objekte klassifizieren“.

- Dokumente sichten
  In diesem Aufgabenpaket geht es darum, alle vorhandenen Dokumente zu analysieren und für die spätere Verwendung aufzubereiten. Bestandteil dieses Arbeitspakets ist auch eine gemeinsame Fragerunde zur Klärung offener Punkte.
- Prozesse identifizieren
  Nach der ersten Sichtung der Dokumente geht es nun darum gemeinsam festzulegen, welche Prozesse für die weitere Analyse von Bedeutung sind. Dabei wird herausgearbeitet, in welcher Detaillierung die Prozesse erfasst und dokumentiert werden. Anschließend erfasst man die identifizierten Prozesse mit den notwendigen Informationen in einem Dokument.
- IT-Objekte klassifizieren
  In diesem Schritt gilt es die für die Analyse benötigten IT-Komponenten zu ermitteln und in entsprechende Objektgruppen einzuordnen. In einem Workshop wird diese Liste verifiziert und gegebenenfalls erweitert. Als zweiten Schritt in diesem Workshop ist vorgesehen, für jeden Objekttyp die für die Analyse und Dokumentation wichtigen Attribute festzulegen. Ergebnis des Workshops ist ein abgestimmtes Dokument zur nachfolgenden Pflege der Daten. Kernaufgabe in diesem Arbeitspaket ist die Füllung des zuvor erstellten Dokuments mit allen Daten. Input für die Pflege sind zum einen die verfügbaren Dokumente zum anderen das Know-how der zuständigen Mitarbeiter.

Stufe 3: Impact-Analyse

Auf Basis der nun vorhandenen Daten gilt es in dieser Phase zu dokumentieren, welche Zusammenhänge zwischen den einzelnen Objekten und Prozessen bestehen. Dabei unterteilt sich diese Phase ebenfalls in zwei Arbeitspakete:

- Zusammenhänge analysieren
  Im Rahmen eines Workshops wird in diesem Arbeitspaket gemeinsam

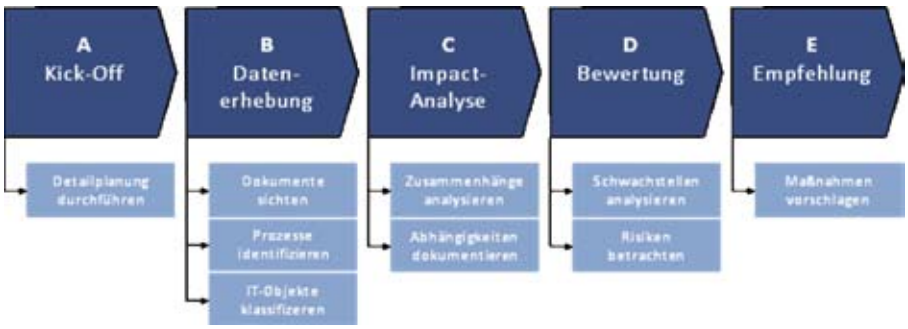

Abbildung 3: Vorgehensmodell (Solution-Engineering-Methode)

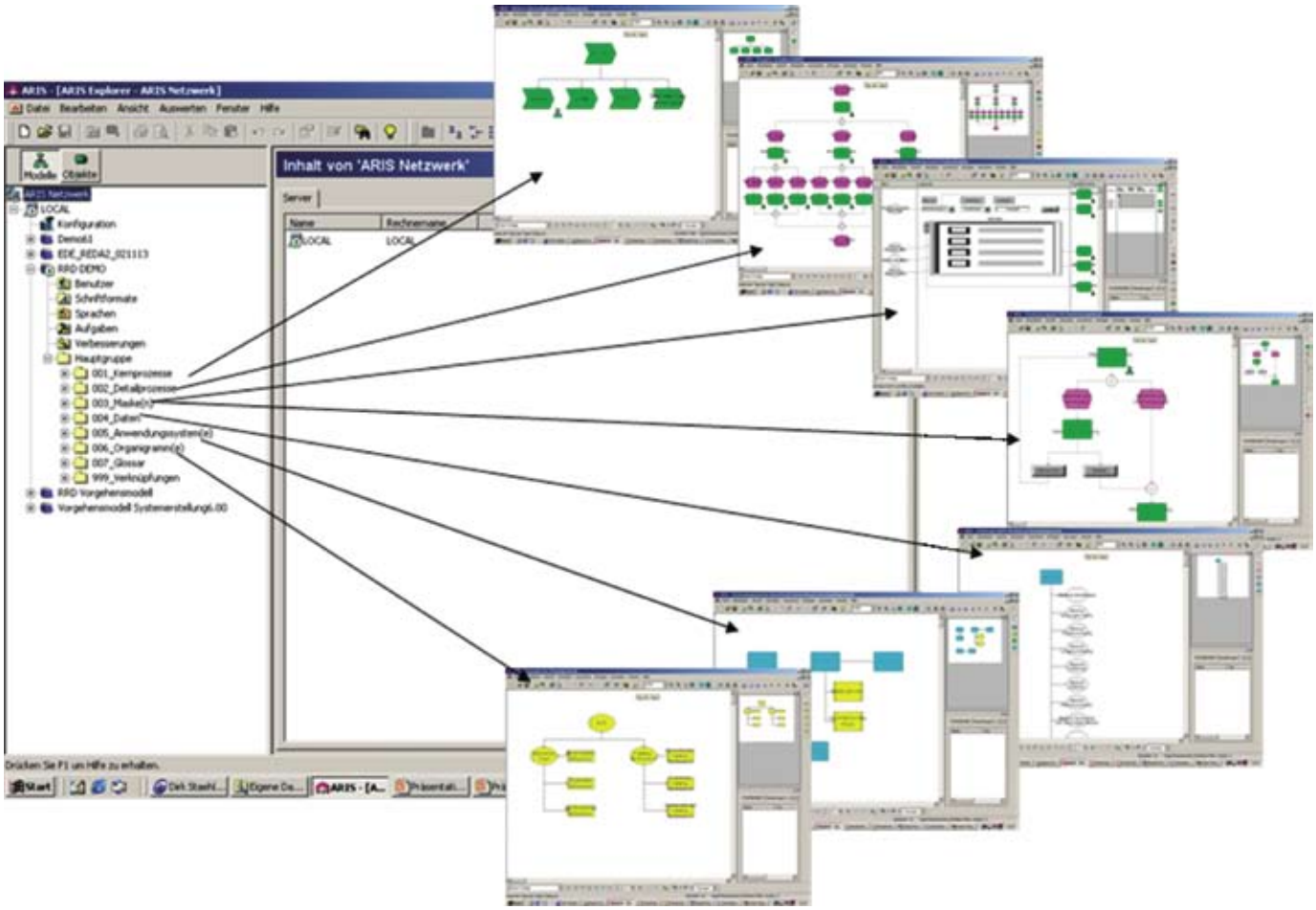

Abbildung 4: Beispiele für ARIS-Modelle

ermittelt, welche Zusammenhänge und Abhängigkeiten zwischen Prozessen und IT-Objekten bestehen. Diese Erkenntnisse erfasst man systematisch in einem strukturierten Dokument.

- Abhängigkeiten dokumentieren
  Die erfassten Zusammenhänge werden jetzt mit der Oracle BPA Suite in ARIS-Modellen dargestellt (siehe Abbildung 4).

Die Darstellung der Prozesse, IT-Objekte und deren Abhängigkeiten mit der ARIS-Methodik erlaubt eine genaue Analyse der Auswirkungen von Veränderungen und Ausfällen der IT-Komponenten auf die Prozesse. Dies ist Grundlage für nachfolgende Bewertungen und Analysen.

Stufe 4: Bewertung

Auf Basis der erstellten Dokumente und ARIS-Modellen werden vorhandene Schwachstellen und Risiken der IT-Infrastruktur bewertet:

- Schwachstellen analysieren
  In diesem Arbeitspaket prüft man, ob die eingesetzten IT-Objekte in der Lage sind, die notwendigen Anforderungen, die sich aus den Prozessen und Abhängigkeiten ergeben, zu erfüllen.
- Risiken betrachten
  Man betrachtet, wie wahrscheinlich das Auftreten von Störungen für die IT-Komponenten ist und welche Auswirkungen dies auf die vorhandenen Prozesse hat.

Stufe 5: Empfehlung

Die Ergebnisse der Schwachstellen und Risikoanalyse werden anschließend dokumentiert und fließen in die Abschlussdokumentation ein. Sie bilden die Grundlage für die auszusprechenden Empfehlungen.

Fazit

Mit diesem Vorgehen haben die Autoren in zahlreichen Projekten sehr positive Erfahrungen gemacht und bieten daher weiterhin regelmäßig ihre Unterstützung an, wenn es um die Analyse von IT-Infrastrukturen geht. Sie haben den Eindruck, dass der Optimierungsbedarf bei vielen Unternehmen derzeit besonders groß ist, und sich viele Firmen in Zeiten, wo die wirtschaftlichen Prognosen ungünstig und die weitere ökonomische Entwicklung unsicher scheint, noch rechtzeitig effizient aufstellen möchten.

Kontakte:
Matthias Mitze
matthias.mitze@opitz-consulting.de
Dirk Weidemann
dirk.weidemann@opitz-consulting.de