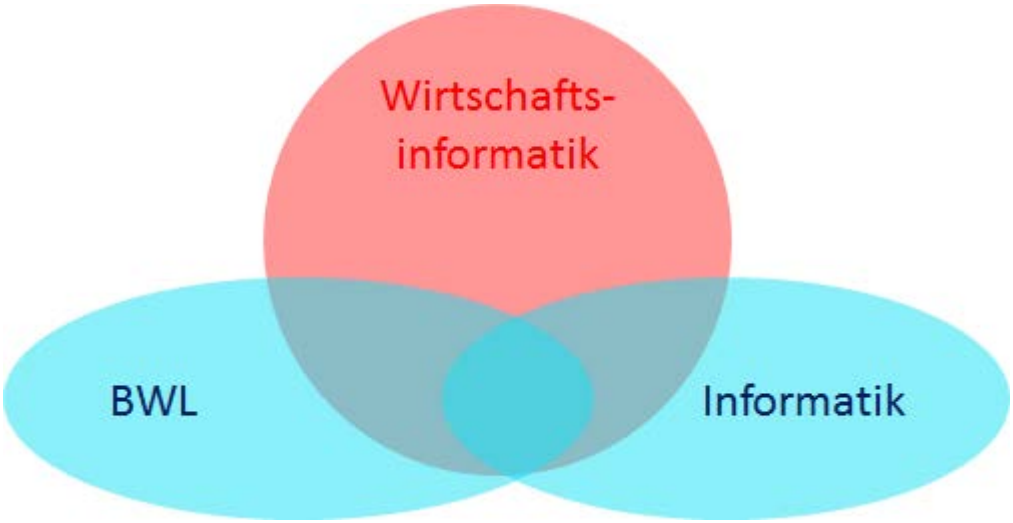
AK WI

Anwendungen und Konzepte der Wirtschaftsinformatik

Nummer 1 (2013)



Editorial


Christian Müller


Konrad Marfurt

Liebe Leserinnen und Leser,

vor Ihnen liegt die erste Ausgabe des E-Journals **Anwendungen und Konzepte in der Wirtschaftsinformatik (AKWI)**. Sie entstand aus aus den wissenschaftlichen Fachkonferenzen des Arbeitskreises Wirtschaftsinformatik an Fachhochschulen (AKWI). Dieser Arbeitskreis wurde 1988 als Diskussions- und Interessenvertretungs- Organ der Wirtschaftsinformatik- Studiengänge in Deutschland, Österreich und der Schweiz gegründet. Seit 2007 wurden die Jahrestagungen des AKWI um wissenschaftliche Fachkonferenzen erweitert, die jeweils einem speziellen Thema aus der Wirtschaftsinformatik gewidmet waren und sind. Die Beachtung der Fachkonferenzen ist in den letzten Jahren stark gestiegen, was sich an den Umfängen der Tagungsbände ablesen lässt. Dies war eine Motivation zur Gründung dieser Zeitschrift.

Diese Zeitschrift soll ein Diskussionsforum zu den aktuellen Entwicklungen in der Wirtschaftsinformatik aus der Sicht der angewandten Forschung an Fachhochschulen sein. Die Zeitschrift ist in die Rubriken Grundlagen, Trends, Praxis, Kurz erklärt, Bücher und Abschlussarbeiten gegliedert. In den ersten vier Rubriken berichten die Autoren über ihre Forschungen aus unterschiedlicher Perspektive und Detailliertheit. Die Rubrik Bücher enthält Buchbesprechungen und unter Abschlussarbeiten werden Zusammenfassungen oder Excerpts hervorragender Abschlussarbeiten veröffentlicht. Die Themen der Beiträge umfassen das ganze Portfolio der Wirtschaftsinformatik. Die Beiträge sind in deutscher oder englischer Sprache verfasst und werden vor der Publikation von zwei Gutachtern anonym und unabhängig bewertet.

Mit dieser ersten Ausgabe möchten wir Ihnen einen Eindruck vermitteln wie ein solches Heft künftig aussehen kann. Es umfasst nur die Rubriken Praxis und Trends und bei der Auswahl der Beiträge haben wir auf solche Beiträge zurückgegriffen, die schon auf den letzten Fachtagungen präsentiert wurden. Mit den Themen der Beiträge wollen wir die von uns intendierte Themenbreite der Zeitschrift darstellen. Der Zweck dieses ersten Heftes ist es, Sie zu motivieren bei unserer Zeitschrift sowohl als Autor als auch als Gutachter mitzuarbeiten. Beiträge können Sie jederzeit auf der Seite *http://akwi.hswlu.ch/index.php/AKWI* einreichen. Dort können Sie sich auch als Gutachter registrieren.

Die Zeitschrift erscheint als E-Journal und wird dankenswerter Weise an der Hochschule Luzern unter Federführung von Konrad Marfurt gehosted. Zur Zeit sind zwei Ausgaben pro Jahr geplant. Die Hauptredaktion haben Christian Müller (TH Wildau) und Konrad Marfurt (HS Luzern) übernommen. Uns können Sie über *redaktion@akwi.hswlu.ch* erreichen. Zum Reaktionsteam gehören außerdem: Thomas Barton (FH Worms), Burkhard Erdlenbruch (HS Augsburg), Andreas Heberle (HS Karlsruhe), Frank Herrmann (HS Regensburg), Rainer Neumann (HS Karlsruhe), Petra Schmidt (HS Mittweida) und Christian Seel (HS Landshut).

Wir hoffen mit diesem Heft Ihr Interesse an unserem Zeitschriftenprojekt geweckt zu haben und freuen uns auf Ihre Beiträge als Autor, Ihre Unterstützung als Gutachter und Ihre Meinung als Leser.

Ihr Christian Müller und Ihr Konrad Marfurt

PROZESSMETRIKEN FÜR DIE INFORMATIONSSICHERHEIT BETRIEBLICHER ANWENDUNGSSYSTEME

Carsten Dorrhauer
Haio Röckle
Institut für Wirtschaftsinformatik an der Hochschule Ludwigshafen
Ernst-Boehe-Str. 4, 67059 Ludwigshafen, Deutschland
E-mail: carsten.dorrhauer@hs-lu.de, haio.roeckle@hs-lu.de

EINLEITUNG

In vielen Unternehmen ist in den letzten Jahren die Informationssicherheit in den Fokus der Aufmerksamkeit gerückt, ihre Qualität wird aber kaum gemessen. Sicherheits-KPI wurden zwar vorgeschlagen (Jaquith 2007), haben sich aber in der Praxis bislang kaum durchgesetzt. (Schimpf und Röckle 2009). Im Gegensatz dazu werden die Prozesse des IT Service Management (ITSM) kontinuierlich evaluiert. In der Praxis haben Prozessframeworks, von denen ITIL das wichtigste ist, weite Verbreitung erfahren. ITIL sieht KPI zur Messung der Servicequalität für ITSM-Prozesse wie zum Beispiel Continuity Management und Incident Management vor. Allgemeiner betrachtet sind Prozess-KPI heutzutage weit verbreitet und akzeptiert, während Zustandskennzahlen – zumindest im Bereich der Informationssicherheit – offensichtlich schwieriger zu fassen sind.

Eine Ursache für die bemerkenswerte Vernachlässigung der Qualitätsmessung ausgerechnet bei Sicherheitsaspekten mag deshalb darin zu finden sein, dass die Vorgaben zur Informationssicherheit in den wichtigsten Standards nicht durchgängig prozessorientiert formuliert sind. So sind zwar die wesentlichen Vorgaben des Informationssicherheitsmanagements aus ISO 27001 prozessorientiert, nicht aber die Detailvorgaben nach ISO 27002. ITIL dagegen ist durchgängig prozessorientiert aufgebaut. KPI zur Messung der Qualität von ITIL-Prozessen sind bekannt und in vielen Fällen einfach zu implementieren und mit vertretbarem Aufwand zu erfassen.

Da aber die meisten Aufgaben der Informationssicherheit durchaus prozessorientiert durchgeführt werden, schlägt die vorliegende Arbeit eine prozessorientierte Sicht der Sicherheitsaufgaben vor, auf deren Grundlage prozessbasierte KPIs für die Informationssicherheit implementiert werden können. Dabei gibt es Kennzahlen, die

- den Prozess als solchen betreffen, z.B. „Welcher Anteil von sicherheitsrelevanten Zwischenfällen wird ohne Beteiligung des Servicedesk behoben?“ und solche, die
- seinen Output betreffen, z.B. „Welcher Anteil von sicherheitsrelevanten Zwischenfällen wird innerhalb einer vereinbarten Wiederherstellungszeit behoben?“

Die Unterscheidung zwischen diesen Kategorien ist fließend. Dem gegenüber stehen

- nicht-prozessbasierte Kennzahlen, die eindeutig rein technischer Natur sind, z.B. „Häufigkeit registrierter Portscans auf Webservern“.

Diese Arbeit konzentriert sich dabei auf Sicherheitsaufgaben im Zusammenhang mit betrieblichen Anwendungssystemen. Dadurch werden die Systeme erfasst, in denen die betrieblich relevanten Daten mit dem höchsten Schadenspotenzial verarbeitet werden, ohne sich in infrastrukturellen Details zu verlieren. Die Untersuchung erfolgt gegliedert nach den Lebenszyklusphasen betrieblicher Anwendungssysteme durch Betrachtung der jeweils relevanten Sicherheitsprozesse und der Anwendbarkeit prozessorientierter Sicherheitsmetriken. Bei der vorliegenden Arbeit handelt es sich um eine Neuauflage von Röckle und Dorrhauer 2011 mit einer knappen Reflektion über die Entwicklungen in den letzten Jahren.

INFORMATIONSSICHERHEIT UND IHRE MESSBARKEIT

Zu einem Managementsystem in einem Unternehmen gehören die Vorgabe von Zielen und ein Berichtswesen entlang der Unternehmensorganisation, das die Kontrolle der Ergebnisse ermöglicht. Nicht umsonst steht in Stellenbeschreibungen des Managements üblicherweise ein Passus wie „… berichtet an den CIO …“ oder „… berichtet direkt an den Vorstand …“.

Offensichtlich gibt es innerhalb eines Unternehmens mehrere Ebenen von Berichtsempfängern. Im Management der Informationssicherheit sind dies in der Regel der Informationssicherheitsmanager, häufig ISO oder CISO genannt, der IT-Leiter (CIO) und der IT-Vorstand, d.h. das Vorstandsmitglied in dessen Verantwortungsbereich die IT fällt. Jeder Berichtsempfänger hat unterschiedliche Informationsbedürfnisse:

- Der CISO interessiert sich für die einzelnen Sicherheitslücken, weil es zu seinen Aufgaben gehört, diese zu bewerten und ggfs. zu beheben.
- Der IT-Vorstand ist nur an Risiken interessiert, die für das Gesamtunternehmen relevant werden könnten oder die den Wertbeitrag der IT für das Unternehmen negativ beeinflussen könnten
- Der CIO interessiert sich für den qualitativen Gesamtzustand „seiner“ IT

Berichte können in unterschiedlichsten Formen und Formaten angefertigt werden. Grundsätzlich ist es wünschenswert, quantitative Kennzahlen zu haben, die aus Messungen gewonnen werden und die detaillierte Aussagen über Risikozustände, Fertigstellungsgrade, Qualitätszustände, etc. treffen. Der Managementvordenker Peter F. Drucker sagte z.B. nicht nur „If you can't measure it, you can't manage it", sondern auch "What gets measured gets managed" (Drucker 1974). Im Alltag sind solche quantitativen Kennzahlen leider häufig nicht vorhanden, so dass im Berichtswesen auf qualitative Informationen und subjektive Aussagen zurückgegriffen werden muss, dies ist aber nicht Thema dieser Arbeit.

Für das Management der Informationssicherheit wird vom wichtigsten Standard ISO 27001 ein „Maß für die Wirksamkeit der ausgewählten Maßnahmen…" gefordert (DIN2008a, Kap. 4.2.2, d), allerdings nicht weiter spezifiziert. Entsprechend findet sich im vertiefenden Standard ISO 27002 die Aussage „Das Messen von Informationssicherheit ist außerhalb des Geltungsbereichs dieses Standards" (DIN 2008a, Fußnote zu 0.7, j). Diese Lücke sollte geschlossen werden mit einem Standard ISO 27004, der nach einigen Jahren Entwicklungs- und Abstimmungsdauer im Dezember 2009 veröffentlicht wurde (ISO/IEC 2009), dessen praktische Verifikation aber noch aussteht (ISO/IEC 2011).

Bereits früher wurden zahlreiche IT Security Kennzahlen (Security Metrics) vorgeschlagen (Jaquith 2007). Die Menge an Kennzahlen ist allerdings gerade für Vorstände viel zu groß und die Relevanz der einzelnen Kennzahlen zu gering. Manche Kennzahlen sind auch aufgrund technischer Feinheiten für das höhere Management schlicht unverständlich. Dies sind Probleme, die auch mit dem Standard ISO 27004 weiterbestehen. Klassische Lösungsansätze bestehen darin, die Kennzahlen zu verdichten (aggregieren) und zu visualisieren, z.B. in Ampeldarstellungen oder in Dashboards („Management-Cockpit") bis hin zum Konzept einer „Balanced Security Scorecard". Weitere Ansätze des Security Reporting wurden in Schimpf und Röckle, Kap. 3 beschrieben.

Prinzipiell ist die Aggregation von Kennzahlen eine Aufgabe, die in jedem Unternehmensbereich in Angriff genommen werden muss. In Bezug auf das Management der Informationssicherheit gibt es aber zwei Besonderheiten:

- Gemäß den internationalen Standards zum Informationssicherheitsmanagement (BSI 2008, Funk 2011) soll der CISO direkt an den IT-Vorstand berichten, damit wird von der Aggregationslinie IT-Vostand – CIO – CISO abgewichen und es verstärkt sich die Gefahr, dass der IT-Vorstand mit einer Überzahl von Detailinformationen konfrontiert wird.
- Auch kleine Sicherheitslücken können große Auswirkungen haben. Jedes Detail, das bei der Aggregation der Informationen wegfällt, kann Basis eines fatalen Unfalls oder Angriffs werden und wäre damit – nachträglich betrachtet – durchaus Management-relevant gewesen.

Im folgenden Kapitel greifen wir die Idee aus Schimpf und Röckle, Kap. 3.6 auf und spezifizieren prozessorientierte Kennzahlen zur Informationssicherheit. Wir nutzen damit die folgenden Vorteile aus:

- Bei der Definition von Prozesskennzahlen handelt es sich um ein etabliertes Vorgehen,
- das speziell auch dem Management ad hoc verständlich ist.
- Viele Haftungsfragen bei IT-Unfällen können ausgeschlossen werden, wenn angemessen funktionierende Prozesse nachgewiesen werden.
- Durch die hierarchische Gliederung von Prozessen ergibt sich eine weitere Hierarchie, anhand der die Prozesskennzahlen aggregiert werden können.

Bei den folgenden Untersuchungen beschränken wir uns auf die Prozesse, die für den Lebenszyklus betrieblicher Anwendungssysteme relevant sind, einerseits weil dies dem Fokus der Jahrestagung entspricht, andererseits weil dadurch u.a. die Business-kritischen Anwendungen erfasst sind, die z.B. auch im Rahmen von Sarbanes-Oxley betrachtet werden müssen.

SICHERHEITSASPEKTE IN DEN LEBENSZYKLUSPHASEN BETRIEBLICHER ANWENDUNGSSYSTEME

Sicherheitsanforderungen für Betriebliche Anwendungssysteme nach ISO 27002

Die Stärke des Informationssicherheitsstandards ISO 27002 liegt darin, dass er die wesentlichen Bereiche der Informationssicherheit, speziell die wesentlichen Sicherheitsmaßnahmen für Unternehmen und andere Organisationen vollständig abdeckt, wobei absichtlich viele Freiheitsgrade bleiben. Zur Erfassung der speziellen Sicherheitsaspekte im Lebenszyklus betrieblicher Anwendungssysteme ist hier speziell das Kapitel (die „Domäne") 12: „Beschaffung, Entwicklung und Wartung von Informationssystemen" vorgesehen.

Allerdings berühren auch viele weitere Maßnahmenbereiche und Maßnahmen die Sicherheit der betrieblichen Anwendungssysteme, z.B. die Domäne „10 Betriebs- und Kommunikationsmanagement". Die folgende Tabelle gibt deshalb zunächst eine Übersicht über die Punkte des ISO 27002 Standards, die nach Ansicht der Autoren relevant für betriebliche Anwendungssysteme sind oder sein können. Da viele Punkte dieses Standards recht offen formuliert sind, könnten andere Betrachtungen aufgrund der Interpretationsspielräume auch zu anderen Ergebnissen kommen, dennoch sind wir der Ansicht, dass diese Aufstellung als Übersicht gut geeignet ist. Zur Übersichtlichkeit werden die Punkte häufig gekürzt dargestellt, für die vollständige Formulierung sei der Leser

auf den Originaltext des Standards verwiesen, ebenso wie auf die Inhalte der einzelnen Punkte.

Tabelle 1: Relevante Controls des ISO 27001 Standards

Punkt im ISO 27001	**Bezug zu betrieblichen Anwendungssystemen**
6.2.1 Sicherheitsanforderungen in Bezug auf externe Mitarbeiter	Anforderungen aus Sicht des Unternehmens, soweit externe Mitarbeiter in Entwicklung oder Betrieb mitarbeiten
6.2.2 Sicherheitsanforderungen bei Datenzugriff von Kunden	Anforderungen aus Sicht des Unternehmens, soweit Funktionen des Anwendungssystems von Kunden genutzt werden
6.2.3 Vereinbarungen mit Dritten	Verträge zur Unterstützung der o.g. Anforderungen
7 Klassifizierung von Informationen	Im Softwareentwicklungsprozess sollte der Sicherheitsbedarf des Programmcodes und der zu verarbeitenden Daten klassifiziert werden.
8.2.3 Zurücknahme von Zugangsrechten	Eigentlich bezieht sich Kapitel 8 des Standards auf „Personalsicherheit“ in Bezug auf Angestellte des Unternehmens. Speziell der Punkt 8.2.3 sollte aber auch auf externe Mitarbeiter angewandt werden.
9.1.2 Zutrittskontrolle 9.1.3 Sicherung von Büros, Räumen und Einrichtungen 9.1.5 Arbeit in Sicherheitszonen	Kapitel 9 des Standards bezieht sich auf physische Sicherheit. Bei geheimen Entwicklungen könnte es sinnvoll sein, die genannten Punkte auf Mitarbeiter in der Softwareentwicklung anzuwenden.
10.1.2 Änderungsverwaltung	Dieser Punkt des Standards wird vom ITIL Prozess Change Management abgedeckt.
10.1.3 Trennung von Verantwortlichkeiten	Dieser Punkt ist in Bezug auf betriebliche Anwendungssysteme noch komplexer als im ISO 27002, da er sich einerseits auf die Softwareentwicklung (vgl. „Analyse und Design“) und andererseits auf den ITIL Prozess beziehen kann.
10.1.4 Trennung von Entwicklung, Test und Produktion	Ist sowohl für die Code-Sicherheit als auch für die Sicherheit von Produktivdaten relevant.
10.2 Dienstleistungserbringung von Dritten 10.2.1 Vorgaben überwachen 10.2.2 Leistungen überprüfen 10.2.3 Change Mgmt. für Dienstleistungen von Dritten	Bezieht sich auf die Qualität der Leistungserbringung von externen Mitarbeitern im Gegensatz zu 6.2, wo es um „echte“ Sicherheitsanforderungen geht.
10.3.1 Kapazitätsplanung 10.3.2 Systemabnahme	Findet sich in den ITIL Prozessen *Capacity Management* und *Change Management*
10.4.1 Maßnahmen gegen Schadsoftware	Bezieht sich eigentlich auf Virenschutzmaßnahmen und wäre damit nicht relevant für betriebliche Anwendungssysteme. Kann aber auch darauf bezogen werden, dass der Code selbst entwickelter Software frei sein muss von Schadcode und fällt damit in den Bereich der Code Security
10.5.1 Backup von Informationen	Kann in Bezug auf betriebliche Anwendungssysteme so interpretiert werden, dass diese einen angemessenen Backup ermöglichen bzw. unterstützen. Dies kann in Bezug auf Softwareentwicklung aber auch in Bezug auf Auswahl und Implementierung von Software gesehen werden.
10.7.3 Umgang mit Informationen 10.7.4 Sicherheit der Systemdokumentation	In Bezug auf Softwareentwicklung ist zu beachten, dass der entwickelte Code und die Dokumentation einen angemessenen Umgang erlauben. Im Betrieb ist auf den Umgang mit Programmcode und -dokumentation zu achten.
10.8 Austausch von Informationen 10.8.1 Leitlinien und Verfahren 10.8.2 Vereinbarungen 10.8.3 Transport physischer Medien 10.8.4 Elektronische Mitteilungen 10.8.5 Geschäftsinformationssysteme	Ist in Bezug auf Softwareentwicklung in dem Sinne relevant, dass die entwickelte Software angemessene Sicherheit in den genannten Punkten erlaubt. Ist im Betrieb dahingehend relevant, dass die vorhandenen Möglichkeiten auch angemessen genutzt werden.

10.9 E-Commerce 10.9.1 E-Commerce 10.9.2 Online-Transaktionen 10.9.3 Öffentlich verfügbare Informationen	Analog zu den Anmerkungen zu 10.8
10.10 Überwachung (Audit) 10.10.1 Auditprotokolle 10.10.2 Überwachung der Systemnutzung 10.10.3 Schutz von Protokollinformationen 10.10.4 Admin. und Betreiberprotokolle 10.10.5 Fehlerprotokolle 10.10.6 Zeitsynchronisation	Analog zu den Anmerkungen zu 10.8
11 Zugangskontrolle 11.1 Geschäftsanforderungen 11.1.1 Leitlinie 11.6.1 Einschränkung von Informationszugriffen	Die Leitlinie muss sowohl bei der Entwicklung als auch im Betrieb von Anwendungen berücksichtigt werden. Es gelten die Anmerkungen zu 10.8
11.2 Benutzerverwaltung 11.2.1 Registrierung 11.2.2 Sonderrechte 11.2.3 Passwörter 11.2.4 Überprüfung 11.3.1 Passwortverwendung	Analog zu den Anmerkungen zu 10.8
11.5.4 Verwendung von Systemwerkzeugen	Im Betrieb soll der Zugriff auf administrative Funktionen der Software besonders geschützt werden, z.B. auf Betriebssystemebene. Bei der Softwareentwicklung muss darauf geachtet werden, dass die Anforderung im Betrieb erfüllt werden kann.
11.6.2 Isolation sensitiver Systeme	Ist eine Betriebsaufgabe für besonders sicherheitsrelevante Anwendungen

11.7.1 Mobile Computing und Kommunikation 11.7.2 Telearbeit	Generell gelten die Anmerkungen zu 10.8. Für Anwendungen auf mobilen Geräten sind ggfs. spezielle Schutzmaßnahmen zu treffen. Für Anwendungen, die per Telearbeit genutzt werden sollen, ist die entsprechende Kommunikationssicherheit zu gewährleisten. Beides gilt für die Entwicklung und für den Betrieb, vgl. die Punkte 10.8 und 10.9 des Standards.
12 Beschaffung, Entwicklung und Wartung von Informationssystemen 12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen	Generell gilt das Prinzip, dass Informationssicherheit in jedem Projekt bereits in Analyse und Design berücksichtigt werden muss.
12.2.1 Überprüfung von Eingabedaten 12.2.2 Kontrolle der internen Verarbeitung 12.2.3 Integrität von Nachrichten 12.2.4 Überprüfung von Ausgabedaten	Generell handelt es sich hier um typische Elemente der Code Sicherheit, die in der Softwareentwicklung zu berücksichtigen sind. Allerdings ist es auch denkbar, weitere Prüfungen im Betrieb vor- und nachzuschalten, um die Sicherheit zu steigern. Insbesondere die Integrität von Nachrichten könnte durch Mechanismen der Netzwerkverschlüsselung und –signatur unterstützt werden.
12.3.1 Leitlinie Kryptografie 12.3.2 Schlüsselverwaltung	Der Bedarf an Kryptografie muss in den einzelnen Projekten ermittelt werden. Falls Kryptografie genutzt wird, müssen die Schlüssel angemessen geschützt werden. Außerdem gelten die Anmerkung zu 10.8.
12.4.1 Kontrolle von Software im Betrieb 12.4.3 Zugangskontrolle zu Quellcode	Quell- und Programmcode müssen während der Entwicklung geschützt werden, insbesondere beim Übergang vom Entwicklungs- über das Test- ins Produktivsystem. Im Betrieb muss der Programmcode geschützt werden.
12.4.2 Sicherheit von Testdaten	Falls betriebliche Daten im Test verwendet werden, müssen diese dabei besonders geschützt werden.

12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen 12.5.2 Kontrolle nach Änderungen am Betriebssystem	Änderungen am Betriebssystem sowie die notwendigen Nacharbeiten gehören prinzipiell zum IT Betrieb.
12.5.3 Änderungen an Softwarepaketen	Bezieht sich auf die Änderung an Softwarepaketen, die von externen Anbietern geliefert werden. Sollten grundsätzlich sparsam verwendet werden.
12.5.4 Ungewollte Preisgabe von Informationen	Betriebliche Anwendungen von externen Lieferanten sollten – im Betrieb – auf unerwarteten Datenabfluss (Hintertüren) oder unsichere Datenspeicherung und –übertragung getestet werden.
12.5.5 Ausgelagerte Softwareentwicklung	Stellt eine Detaillierung von Punkt 10.2 dar, bei der es speziell um externe Softwareentwicklung geht.
12.6.1 Kontrolle technischer Schwachstellen	Hierunter versteckt sich u.a. der wichtige Sicherheitsprozess „Patch Management“. Für die Entwicklung und Wartung selbst entwickelter Software ergibt sich hieraus aber der Bedarf an einem Sicherheitssupport, der sehr kurzfristig Patches für bekanntgewordene Schwachstellen entwickelt und bereitstellt.
13 Umgang mit Informationssicherheitsvorfällen 14 Sicherstellung des Geschäftsbetriebs 15 Einhaltung von Vorgaben	Diese Prozesse beziehen sich zwar u.a. auch auf betriebliche Anwendungen, werden aber hier nicht vertieft behandelt, weil diese im ITIL wesentlich breiter behandelt werden.

Sicherheit Betrieblicher Anwendungssysteme im IT Service Management

Zur Auswahl Zu Untersuchender Prozesse

Entwicklung, Einführung und Betrieb betrieblicher Anwendungssysteme werden grundsätzlich in mehr oder weniger formalisierten Prozessen organisiert. Viele Unternehmen definieren diese Prozesse nicht grundlegend selbst, sondern nutzen ein Prozessframework als Vorlage. Besondere Bedeutung hat ITIL erlangt, das als Sammlung von Best Practices erwiesenermaßen praktisch erfolgreiche Prozesse miteinander kombiniert.

Im Folgenden sollen Prozesse, die im Lebenszyklus betrieblicher Anwendungssysteme eine Rolle spielen, auf die Messbarkeit von Sicherheitsqualität untersucht werden. Dazu könnten konkrete Prozesse in Unternehmen erfasst und analysiert werden; hier soll jedoch ein anderer Weg gewählt werden. Leider ist es schlechterdings unmöglich, die Gesamtheit in der Praxis vorkommender individueller ITSM-Prozesse zu erfassen. Eine empirische Analyse wäre deshalb entweder mit unverhältnismäßig großem Aufwand verbunden oder auf Einzelfälle beschränkt, deren Repräsentativität nicht feststellbar wäre.

Es bietet sich daher an, mit den ITIL-Prozessen die verbreitetesten Prozesse des IT Service Management auf diesen Aspekt hin zu untersuchen. Bei ihnen handelt es sich um bewährte Vorgehensweisen, die in vielen Fällen erfolgreich eingesetzt werden und die seit nunmehr zwei Jahrzehnten kontinuierlich den Rückmeldungen aus der Praxis und den technischen Entwicklungen angepasst werden.

Die ITIL-Kernveröffentlichungen des *Office of Government Commerce* nehmen vielfach Stellung zur Messbarkeit und zur Messung der Prozessqualität. Einige dieser Vorschläge haben Sicherheitsrelevanz – nicht nur jene zur Messung des ITIL-Prozesses *Information Security Management*, sondern auch solche zur Messung vieler anderer Prozesse, die in ihrer Gesamtheit den kompletten Lebenszyklus eines Anwendungssystems betreffen. Im Folgenden werden diese Empfehlungen aus der Sicherheitsperspektive betrachtet. Eine besondere Rolle nehmen dabei die Entwicklungs- und Testphase der Applikation ein, da ITIL diese zwar mit Prozessen wie *Release Management* und *Configuration Management* unterstützt, aber kein eigenes Vorgehensmodell für Softwareentwicklungsprojekte enthält. Die Projektmanagementmethode des OGC hat nicht dieselbe weite Verbreitung wie ITIL gefunden. Für diese Lebenszyklusphasen kommt daher den ISO-Normen 2700x (Kapitel „Sicherheitsanforderungen Für Betriebliche Anwendungssysteme Nach ISO 27002”) sowie den Methoden und Vorgehensweisen des Software Engineering (Kapitel „Sicherheit bei der Herstellung betrieblicher Anwendungssysteme”) ein spezieller Stellenwert zu.

Service Level Management

Vor der Einführung eines neuen IT-Service werden die Kundenanforderungen aufgenommen, analysiert und dokumentiert. Neben den funktionalen und nichtfunktionalen Anforderungen an die betriebliche Applikation werden dabei auch die Anforderungen an ihren Betrieb und den Support definiert. ITIL kennt dafür den Prozess des *Service Level Management* (OGC 2007b, S. 65ff.). In Zusammenarbeit mit dem Kunden wird der Service gestaltet; standardisierte Services werden aus einem Servicekatalog abgerufen. Neben vielen anderen Parametern wird dabei nach Kundenanforderung auch das

erforderliche Sicherheitsniveau festgelegt. ITIL schlägt zur Messung der Prozessqualität Kennzahlen vor (Ebel 2008, S. 225f.), von denen viele vor allem die Services als Output der Prozesse messen.

- Dazu zählen im Fall des *Service Level Management* die relative und absolute Häufigkeit von Service-Level-Verletzungen, was zunächst wenig Sicherheitsbezug zu haben scheint. An anderer Stelle fordert ITIL aber die besondere Erfassung von sicherheitsrelevanten Service-Level-Verletzungen. Es ist nur ein kleiner Schritt, die Kennzahlen zu Service-Level-Verletzungen ebenfalls separat für solche Fälle zu ermitteln, dann werden sie auch aus Sicherheitsperspektive relevant. Insbesondere ihre Entwicklung über mehrere Betrachtungsperioden gibt dann eine recht genaue Einschätzung, wie sich die Sicherheitsqualität entwickelt.
- Auch die Analyse, welche Service-Level-Verletzungen in welcher Häufigkeit auf Fehler von Subauftragnehmern zurückzuführen sind, gewinnt Relevanz für die Erhöhung des Sicherheitsniveaus, wenn die zusätzliche Kennzeichnung der Service-Level-Verletzungen als sicherheitsrelevant mit ausgewertet wird. Eine sich daraus unmittelbar ergebende Handlungsempfehlung könnte der Wechsel des Subauftragnehmers sein.
- Eine weitere ITIL-Kennzahl zum *Service Level Management* ist der Anteil der Services, für die es überhaupt keine SLA gibt, die also am offiziellen Prozess vorbei erbracht werden. Offensichtlich ist für Services ohne SLA auch kein Sicherheitsniveau definiert, das vom Kunden eingefordert werden könnte. Ihre Zahl sollte möglichst gering sein, was gleichbedeutend damit ist, für diese „Abdeckungsrate" des *Service Level Management* 100 Prozent als Zielgröße anzustreben. Sie hat somit zumindest zum Teil Sicherheitsbedeutung.
- Die Qualität des SLM-Prozesses kann darüber hinaus gemessen werden, indem man die Anzahl der SLA-Reviews und die der daraus abgeleiteten Maßnahmen analysiert. Damit wird deutlich, ob der Prozess „gelebt" wird, ob, wie schnell und in welchem Umfang also Änderungen der Kundenanforderungen oder neue Anforderungen vom SLM aufgegriffen werden. Auch dies betrifft mit allen anderen Anforderungen insbesondere die Sicherheitsanforderungen. Diese Kennzahl hat für sich alleine zwar keinen direkten Sicherheitsbezug, gibt aber Auskunft über die Aussagekraft der anderen erhobenen Kennzahlen.
- Über diese Kennzahlen hinaus sieht ITIL Kundenbefragungen zur Zufriedenheit mit dem SLM vor. Fragen zur Auswertung der Kundenzufriedenheit mit der Sicherheitsqualität könnten etwa lauten: Sind die Sicherheitsanforderungen an den IT Service mit Ihnen seitens des Service Providers zu Ihrer Zufriedenheit erörtert worden? Wurden Ihnen Alternativen aufgezeigt? Wurden Ihnen die Kosten dieser Alternativen genannt? Würden Sie die sicherheitsrelevanten Anforderungen in den SLA wieder genauso definieren? Sind die in den SLA mit Ihnen vereinbarten Sicherheitsanforderungen vom Service Provider in vollem Umfang erfüllt worden?

Availability Management

Zentrale Bedeutung bei der Einhaltung von SLA kommt der Verfügbarkeit der Services zu, um die sich der ITIL-Prozess *Availability Management* von der Definition der Verfügbarkeitsanforderungen bis zur Überwachung der tatsächlichen Verfügbarkeit kümmert (OGC 2007b, S. 97ff.). Zwischen Verfügbarkeit und Informationssicherheit besteht eine gegenseitige Abhängigkeit:

- Aus Sicherheitsperspektive setzt sich Informationssicherheit zusammen aus Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
- Aus der Perspektive des *Availability Management* ist die Sicherheit einer von vielen Faktoren, die die Verfügbarkeit bedingen. Andere sind z.B. Redundanz, Hardwareersatzteillager, aktuelle und gepflegte Konfigurationsdaten.

Selbstverständlich müssen Sicherheitsmaßnahmen auf die vereinbarte Verfügbarkeit abgestimmt werden. Ein niedriges Sicherheitsniveau impliziert ein gesteigertes Risiko ungeplanter Serviceausfälle aufgrund von Sicherheitszwischenfällen. Dieses wiederum senkt die maximale Verfügbarkeit, zu der sich der Service Provider in einem SLA verpflichten kann.

Die Messung der Leistungsfähigkeit dieses Prozesses gibt leider recht wenig für die prozessbasierte Messung der Sicherheitsqualität her. Die wichtigsten KPI sind die Verfügbarkeiten der Services und der zu ihrer Erbringung verwendeten Komponenten sowie die zur Wiederherstellung eines Service nach einem Ausfall im Mittel benötigte Zeit. Auch hier gibt es natürlich einen Zusammenhang zur Sicherheitsqualität. Er lässt sich aber nicht isolieren, es sei denn, man wollte eine theoretische Verfügbarkeit bei Vernachlässigung nicht sicherheitsinduzierter Ausfälle konstruieren. Eine solche Kennzahl wäre nicht nur sehr weit hergeholt, sie mäße auch nicht primär den Prozess selbst, sondern seinen Output und erfüllte damit eben nicht den eingangs erhobenen Anspruch der prozessorientierten Messung von Sicherheitsqualität. Gleiches gilt für den Versuch, Wiederherstellungszeiten nach sicherheitsrelevanten Zwischenfällen zu isolieren. Schließlich hängt die Wiederherstellungszeit nach einem Ausfall von technischen und organisatorischen Faktoren ab, nicht primär vom Grund des Ausfalls.

IT Service Continuity Management

Der Prozess *IT Service Continuity Management* kümmert sich um Katastrophenfälle. Er soll das Risiko bestimmter katastrophaler Ereignisse vermindern und die Organisation auf den Fall vorbereiten, daß sie dennoch eintreffen. Neben Ereignissen wie Erdbeben, Feuer oder Hochwasser können auch manche sicherheitsrelevante

Angriffe zu berücksichtigen sein (OGC 2007b, S. 125ff.). ITIL schlägt zur Messung prozessbasierte Maßstäbe vor:

- Der Anteil der Service Level Agreements, die auf Katastrophenschutz Bezug nehmen. Damit wird gemessen, wie weit der Service Continuity-Gedanke die Organisation durchdrungen hat. In leicht abgeänderter Form könnte man messen: "Welcher Anteil der SLA nimmt Bezug auf die Vorbeugung und Notfallplanung für Katastrophenfälle durch interne oder externe Angriffe?"
- Die Anzahl der Audits im Zeitverlauf und der Anteil der erfolgreichen Audits misst, wie sehr der Prozess "gelebt" wird und wie gut die Organisation auf den Katastrophenfall vorbereitet ist. Eine Eingrenzung nach Katastrophen durch Angriffe ist auch hier möglich und gäbe der Kennzahl zusätzliche Sicherheitsbedeutung.

Supplier Management
Die Lieferanten und Subunternehmer, die der Service Provider engagiert, um mit ihrer Unterstützung seine Serviceversprechen zu halten, bestimmen die Qualität der Services ebenso wie er selbst. Mit Ihrer Auswahl und der Pflege der Lieferantenbeziehungen beschäftigt sich der Prozess *Supplier Management* (OGC 2007b, S. 149ff.). Da eine von einem Zulieferer verursachte Sicherheitslücke ebenso folgenschwer wie eine selbstverschuldete sein kann, die Kontrolle und Steuerung sich aber schwieriger als bei eigenen Mitarbeitern gestalten, ist auch dieser Prozess sicherheitsrelevant.

Die Qualität des *Supplier Management* wird gemessen, indem man die Abdeckung der Lieferantenbasis durch gemäß diesem Prozess verwaltete Beziehungen oder die Anzahl und Entwicklung der Lieferantenreviews erhebt. Primär den Output des Prozesses messen Anzahl, Anteil und Entwicklung der von Lieferanten verschuldeten SL-Verletzungen. Letzteres ließe sich dank separater Erfassung sicherheitsrelevanter SL-Verletzungen auch sicherheitsbezogen spezialisieren.

Information Security Management
Der ISM Prozess ist der ITIL-Prozess, der Sicherheit im Namen trägt und der unmittelbar für Sicherheit zuständig ist. ITIL beschreibt nicht technische Lösungen, sondern die sie verwendende Ablauforganisation (OGC 2007b, S.141ff.).

Zur Messung der Prozessqualität wird z.B. vorgeschlagen, die Menge der Angriffe und Infektionen im Zeitverlauf zu erfassen. Dieser Kennwert misst allerdings sowohl die Qualität ihrer Erkennung (je mehr desto besser) als auch die Qualität der Vorbeugung (je weniger, desto besser) und ist damit insgesamt wenig aussagekräftig.

Weitere in diesem Zusammenhang vorgeschlagene Kennzahlen sind auch in der Sicherheitsbranche bekannt aber in vielen Fällen nicht prozessbasiert. Der ISM-Prozess als solcher ist in ITIL allerdings so allgemein formuliert, dass es schwierig ist, ihn anhand von Kennzahlen zu messen. Anhaltspunkte, die dennoch dafür sinnvoll sein könnten, sind z.B. die Frequenz der Überarbeitung von Richtlinien, Analysen und Evaluationen.

Change Management
Sämtliche Änderungen an der Infrastruktur haben definierte Prozesse zu durchlaufen. Im Rahmen des *Change Management* wird über sie entschieden (OGC 2007a, S. 42ff.). Zu den Prüfungen, denen eine potentielle Änderung im Genehmigungsprozess unterzogen wird, gehören auch solche, die ihre Konsequenzen für die Angriffssicherheit der Infrastruktur abschätzen. Nur ein konsequent umgesetzter Change Management Prozess bietet einen wirksamen Schutz vor unbedacht aufgerissenen Sicherheitslücken in der Infrastruktur. Um ihn zu messen, kann man seinen Abdeckungsgrad erheben, also die Anzahl der nicht genehmigten Änderungen, die im Idealfall Null sein sollte. Mit der Anzahl der Störungen, die unmittelbar durch Änderungen verursacht wurden, misst man die Sorgsamkeit des Genehmigungsprozesses (Ebel 2008, S. 394). Zum wiederholten Mal zahlt sich hierbei die Kennzeichnung von Störungen als sicherheitsrelevant aus, wenn man den Sicherheitsbeitrag des Prozesses zu erfassen beabsichtigt.

Event Management, Incident Management und Problem Management
Drei Prozesse sorgen für einen möglichst reibungslosen Systembetrieb. *Incident Management* befasst sich mit der Behandlung von Störungen, (OGC 2007c, S. 46ff.) *Problem Management* mit den hinter den Störungen liegenden Ursachen (OGC 2007c, S. 58ff.) und *Event Management* mit Vorfällen, z.B. aus automatisiertem Monitoring, die ein Eingreifen erforderlich machen (OGC 2007c, S.35ff.). Die Prozesse arbeiten eng zusammen und können alle drei auch sicherheitsrelevante Fälle betreffen. Ein Event kann ein Hinweis auf einen Systemeinbruchsversuch sein, ein Incident kann aus einem erfolgreichen Systemeinbruch resultieren, ein Problem kann eine offene Sicherheitslücke sein, die diesen Systemeinbruch ermöglicht. Erkennt man sicherheitsrelevante Events, Störungen und Probleme als solche und kennzeichnet man sie für die spätere Auswertung als solche, so kann man nicht nur an ihrer Anzahl, Erfolgsquote, Bearbeitungsdauer und Entwicklung im Zeitverlauf den Sicherheitsbeitrag dieser operativen Prozesse messen. Die erhobenen Daten liefern auch das Material zur Messung anderer Prozesse, wie bereits beschrieben wurde.

Weitere Prozesse
Weitere Prozesse zu Erstellung, Inbetriebnahme und Betrieb betrieblicher Anwendungssysteme haben mittelbare Sicherheitsrelevanz. So definiert das *Capacity Management* Kapazitätsanforderungen, die bei der Definition von Sicherheitsmaßnahmen zu berücksichtigen sind.

Der *Demand Management* Prozess sorgt u.a. dafür, dass die Kundenorganisation ein Sicherheitskonzept bekommt, das ihren Anforderungen entspricht und berät bei technischen Fragen. Der Prozess *Release Management* kümmert sich u.a. um die Verteilung von Sicherheitspatches auf die Client-PCs der Mitarbeiter. Das *Service Asset and Configuration Management* dokumentiert die aus Hardware, Software und Dokumenten bestehende Konfiguration. Seine gewissenhafte Durchführung ist Grundlage praktisch aller anderen Prozesse eines IT Service Providers und damit auch der oben aufgeführten.

Diese Prozesse zur Messung von Sicherheit heranzuziehen, ist möglich, aber u.E. wenig zweckdienlich, da sie Sicherheit entweder nur mittelbar betreffen oder diese nur einen kleineren Teil ihrer Aufgabe ausmacht.

Sicherheit bei der Herstellung Betrieblicher Anwendungssysteme

Projekt Kick-Of
Zum Start eines Softwareentwicklungsprojekts oder eines neuen Software-Releases gehören neben der allgemeinen Projektplanung auch der Aufbau des Entwicklungsteams und die Festlegung des Entwicklungsprozesses. Hierzu gehören auch die sicherheitsrelevanten Punkte

- Sicherheits- und Qualitätsanforderungen an externe Mitarbeiter
- Anforderungen von Räumen und IT-Ressourcen sowie die Vergabe der notwendigen Zugangs-, Zutritts- und Zugriffsrechte für interne und externe Mitarbeiter, idealerweise nach einem formalen, dokumentierten Verfahren, das zum Projektabschluss auch die Zurücknahme der Rechte erlaubt (vgl. „Projektabschluss")
- Ggfs. Einrichtung von Sicherheitszonen oder speziellen Büros, Räumen und Einrichtungen und die entsprechenden Zutrittsrechte
- Prozess zur Überwachung der (internen und) externen Mitarbeiter sowie zur Überprüfung von deren Leistungen
- Prozesse zur Verwaltung von Quellcodes und Programmcodes sowie Dokumentation, speziell zur Gewährleistung der Integrität bei der Übergabe zwischen Entwicklungs-, Test- und Produktivsystemen. Diese Prozesse können sich je nach der Sicherheitsrelevanz der zu entwickelnden Software deutlich unterscheiden.

Mit der Gewährleistung der Integrität der Quell- und Programmcodes kann sowohl eine Manipulation des Codes durch Dritte als auch eine Infektion mit Schadcode ausgeschlossen werden. Natürlich sind auch die Vertraulichkeit und Verfügbarkeit von Code sicherheitsrelevant, aber hier nur von untergeordneter Bedeutung. Dasselbe gilt für die Versionierung, die zwar innerhalb des Entwicklungsprozesses wichtig ist, aber nicht in Bezug auf die Sicherheit.

Im Rahmen eines einzelnen Projektes scheinen Kennzahlen in Bezug auf diese Aufgaben nicht zweckmäßig zu sein. Sofern aber innerhalb des Unternehmens eine Vielzahl solcher Projekte durchgeführt wird, können Kennzahlen definiert werden, die jeweils die Anzahl oder den Anteil an Projekten angeben, in denen der entsprechende Punkt nicht berücksichtigt wurde.

Im Zusammenhang mit der Sicherheit von Quell- und Programmcodes können außerdem Kennzahlen des *Incident Management* verwendet werden, z.B. die Anzahl von Sicherheitsvorfällen in Folge fehlerhaften Codes.

Analyse und Design
Zur Analysephase innerhalb eines Softwareentwicklungsprojektes gehören alle Überlegungen und Festlegungen, die eine generelle Bedeutung für das System haben und nicht auf der Basis technischer Überlegungen erledigt werden können. Aus Sicherheitssicht sind dies:

- Benutzerkreis für die Anwendung: Nur interne Benutzer / Partner des Unternehmens / öffentlicher Zugriff
- Art der von der Anwendung verarbeiteten Daten, speziell im Hinblick auf eine notwendige Klassifizierung der Daten
- Geschäftliche Bedeutung der Anwendung und der verarbeiteten Daten
- Art der Benutzerverwaltung: Registrierung, Rechtevergabe, Sonderrechte, Passwörter
- Bedarf an einer funktionalen Trennung bestimmter Verantwortlichkeiten (Separation of Duties)
- Bedarf an Kommunikationsmechanismen wie elektronische Nachrichten oder externe Zugriffe, die eine Verschlüsselung erfordern

In der Designphase sind die Ergebnisse der Analysephase aufzugreifen und außerdem weitere Punkte zu berücksichtigen, die soweit technischer Natur sind, dass sie für die Analyse nicht relevant waren. Technische Entscheidungen der Designphase betreffen die folgenden Punkte:

- Backup-freundliche Datenspeicherung oder Bereitstellung spezieller Backup-Mechanismen
- Erzeugung von Auditprotokollen (Benutzer-, Administrations- und Fehlerprotokolle) der Anwendung, die Datenschutz-konform gespeichert und ausgewertet werden können. Idealerweise unterstützt die Anwendung die elektronische Auswertung und ggfs. die Anonymisierung oder Pseudonymisierung der Protokolle.
- Sicherheitsmechanismen nach Kapitel 12.2 des ISO 27002: Überprüfung von Ein- und Ausgabedaten, Kontrolle der internen Verarbeitung sowie Gewährleistung der Integrität von Nachrichten.

Alle Sicherheitsanforderungen sind dabei als „sicherheitsrelevant" zu dokumentieren. Als Kennzahl schlagen wir die Anzahl sicherheitsrelevanter Anforderungen vor.

Dies dokumentiert einerseits die Durchführung des Prozesses, andererseits – wenn auch nur sehr grob – den Prozessoutput. Vorteilhaft ist, dass diese Kennzahl als Benchmark dienen kann für den Anteil nicht oder fehlerhaft umgesetzter Sicherheitsanforderungen (vgl. „Test" und „Support"). Detailliertere Kennzahlen wären außerdem nach Ansicht der Autoren für Managementebenen nicht verständlich.

Softwareentwicklung
Getreu des Paradigmas, dass nach sorgfältigen Analyse- und Designphasen in der Entwicklung praktisch keine Freiheitsgrade mehr bestehen, bestehen keine zusätzlichen Sicherheitsanforderungen für die eigentliche Softwareentwicklung.

Da es aber üblich ist, dass einzelne Anforderungen während der Entwicklung aus Gründen von Zeit und Aufwand wieder gekippt oder zumindest zurückgestellt werden, ist es sinnvoll, die Anzahl und den Anteil (in %) der nicht implementierten Sicherheitsanforderungen als Kennzahlen zu verwenden.

Test
Grundsätzlich kann sorgfältiges Softwaretesten die Qualität und die Sicherheit von Software massiv erhöhen. Zum allgemeinen Thema „Testing" wurden aber bereits seit vielen Jahren zahlreiche Arbeiten verfasst (Myers 2001, Sommerville 2011), so dass wir dieses Thema hier nicht allgemein vertiefen wollen.

Die (weiteren) sicherheitsrelevanten Aspekte des Softwaretests entsprechen den Punkten 12.2.1 bis 12.2.4 sowie 12.4.1 bis 12.4.3 und – falls externe Mitarbeiter beteiligt sind – den Punkten 6.2, 10.2 und 12.5.5 des ISO 27002 (vgl. „Sicherheitsanforderungen Für Betriebliche Anwendungssysteme Nach ISO 27002"). Im Testprozess betrifft dies die folgenden Schritte

Tabelle 2: Kennzahlen für Softwaretests

Prozessschritte	**Mögliche Kennzahlen**
Sicherstellen der Zuverlässigkeit und Qualität externer Mitarbeiter (falls zutreffend)	▪ Anzahl der beteiligten externen Mitarbeiter ▪ Anteil der nicht bekannten / geprüften Personen
Übernahme der zu testenden Programmmodule aus der Entwicklungsumgebung und Prüfung, dass die Module unverändert übernommen wurden (Integrität)	▪ Anteil der ohne Integritätsprüfung übernommenen Module (in %) ▪ Anteil der fehlgeschlagenen Prüfungen (in %)
Generierung oder Übernahme von Testdaten und Testfällen. Falls hierbei produktive Daten verwendet werden Genehmigung und besonderer Schutz	▪ Anteil der Testabläufe, bei denen Produktivdaten verwendet wurden (in %) ▪ davon Anteil ohne Genehmigung oder besonderen Schutz
Durchführung von Sicherheitstests nach 12.2.1 bis 12.2.4 des ISO 27002	▪ Anteil von Tests, bei denen auf die Sicherheitstests verzichtet wurde (in %) ▪ Anteil von Tests, bei denen die Sicherheitstests fehlgeschlagen sind (in %) ▪ Anteil an Sicherheitsanforderungen (vgl. „Softwareentwicklung"), die nicht verifiziert werden konnten
Durchführung weiterer funktionaler und nichtfunktionaler Tests (entsprechend dem oben stehenden Absatz nicht im Scope unserer Betrachtungen)	
Behandlung der Testergebnisse und ggfs. unveränderte Weitergabe der getesteten Programmmodule	Hängt von der konkreten Ausgestaltung des Prozesses ab.

Support
Der Sicherheitssupport für in Betrieb genommene Anwendungen hat die Aufgabe, bekanntgewordene Sicherheitslücken möglichst schnell zu schließen, indem Patches bereitgestellt werden, die dann dem ITIL Prozess *Change Management* zur Verfügung gestellt werden, damit sie in die Produktivsysteme eingespielt werden.
Mögliche Kennzahlen hierzu wären

- Bedarf an Patches pro Jahr (absolute Anzahl)
- Anteil an Patches, die nicht in einem vorgegebenen Zeitraum zur Verfügung stehen (in %)
- Anteil an Patches, die im Systemtest oder im Produktivsystem Probleme bereiten (in %)

Weitergehender Support im Sinne der Bereitstellung zusätzlicher Softwarefunktionen stellt keine Sicherheitsaufgabe dar, ist also hier nicht zu betrachten.

Projektabschluss
Zum Projektabschluss, der in der klassischen Softwareentwicklung verschiedene interessante Punkte enthält, gehört aus Sicherheitssicht auch

- Das De-Provisioning bzw. die Zurücknahme spezieller Zugangs-, Zutritts- und Zugriffsrechte für interne und externe Mitarbeiter

Wenn die Vergabe der Rechte durchgängig nach einem formalen Prozess durchgeführt wurde, sollte dies auch für die Zurücknahme der Rechte gelten. Innerhalb eines einzelnen Prozesses erscheint eine Kennzahl, die über ein „wurde durchgeführt / wurde nicht durchgeführt" hinausgeht, nicht zweckmäßig. Über viele Prozesse eines Unternehmens hinweg ist – analog zu „Projekt Kick-Off" – eine Kennzahl denkbar, die die Anzahl oder den Anteil der Prozesse ohne explizite Zurücknahme von Rechten angibt.

ZUSAMMENFASSUNG UND AUSBLICK

Es zeigt sich, dass die Sicherheit von Applikationen auch abseits von großen Anhäufungen technischer Parameter messbar ist, wenn man nicht nur die Hard- und Softwarekomponenten, sondern auch die Qualität der sicherheitsunterstützenden Prozesse ins Auge fasst. Man misst dann nicht mehr nur das Erreichen eines Zieles, sondern auch, wie gut es verfolgt wurde.

Bezüglich einiger IT-Service-Management-Prozesse hat sich ein recht einfaches Muster wiederholt:

- Man misst den Abdeckungsgrad eines sicherheitsrelevanten Prozesses. Die Zielgröße ist 100%.
- Berücksichtigt man bei der Datenerfassung die Sicherheitsrelevanz, erfasst man also z.B. sicherheitsrelevante Störungen oder sicherheitsrelevante SLA-Klauseln separat, so ist es ein Leichtes, gängigen Kennzahlen zur Messung der Prozessqualität ihre Pendants zur Seite zu stellen, die über den Sicherheitsbeitrag des jeweiligen Prozesses Auskunft geben.

Die Autoren sprechen sich dafür aus, prozessorientierte Kennzahlen zur Messung der Sicherheit heranzuziehen. Da das Informationsbedürfnis auf verschiedenen Hierarchieebenen unterschiedlich ist, ersetzen diese aber technische Sicherheitsparameter nicht. Technische Größen behalten ihre Wichtigkeit insbesondere für die Analyse von Einzelfällen und die Erarbeitung technischer Verbesserungsmaßnahmen durch Sicherheitsverantwortliche der IT. Sie eignen sich aber weit schlechter als prozessorientierte Kennzahlen als strategisches Instrument der Unternehmensführung auf den darüber liegenden Hierarchieebenen.

AKTUELLE ENTWICKLUNGEN

Da in den letzten Jahren kein neuer ITIL-Standard veröffentlicht wurde – aktuell ist immer noch der ITIL-Standard V3 von 2007 – beschränkt sich unsere Betrachtung der Entwicklungen hier auf die Entwicklung der ISO 27xxx Standardfamilie.

Der Messbarkeit der Informationssicherheit wird in den Standardsierungsgremien mehr und mehr Bedeutung zugerechnet. Dabei gehen die aktuellen Ansätze dahin, Metriken prozessorientiert zu bilden und in einem PDCA-Zyklus zu managen (ISO/IEC 2011, ISO/IEC 2013). Dieser Ansatz entspricht den gängigen Mechanismen auch zum Management der Informationssicherheit selbst und steht nicht im Widerspruch zu den dargestellten Vorschlägen dieser Arbeit.

Für die Bildung der Metriken selbst ist aber immer noch wenig Hilfestellung vorhanden. Der Ansatz der Autoren, wonach Sicherheitsmetriken – zumindest für betriebliche Anwendungssysteme – entlang deren Lebenszyklusprozesse gebildet werden sollten, könnte damit die noch offenen Aufgaben zur Bildung der notwendigen Sicherheitsmetriken unterstützen.

LITERATURVERZEICHNIS

BSI (Hrsg.). 2008. *IT-Grundschutz-Kataloge, M 2.193: Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit.* https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m02/m02193.html, Abruf am 29.06.2011

DIN. 2008a. *DIN ISO/IEC 27001: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005)*

DIN. 2008b. *DIN ISO/IEC 27002: Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informations-Sicherheitsmanagement (ISO/IEC 27002: 2005)*

Drucker, P.F. 1974. *Management*. New York, 5. Auflage

Ebel, N. 2008. *ITIL-V3-Basis-Zertifizierung*, Addison-Wesley, München

Funk, W. 2011. *Rollen für Informationssicherheit in einer Best-Practice-Organisation*. The Bulletin Security Management, BSM Anwender Nr. 202-1.0, http://www. security-management.de/de/publikationen/20100109_BSM_Anwender_202_1.0_Rollen_Informationssicherheit.pdf, Abruf am 29.06.2011

ISO/IEC. 2009. ISO/IEC 27004*:2009 Information technology. Security techniques. Information security management. Measurement*

ISO/IEC. 2011. *ISO27001 Security*: *ISO/IEC 27004*, http://www. iso27001security.com/html/27004.html, abgerufen am 21.06.2011

ISO/IEC. 2013. *ISO27034 Information Technology – Security Techniques – Application Security*: http://www.iso27001security.com/html/27034.html, abgerufen am 24.06.2013

Jaquith, A. 2007. *Security Metrics – Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley, Amsterdam

Myers, G.J. 2001. *Methodisches Testen von Programmen*, Oldenbourg, München

OGC (Hrsg.). 2007a. *Service Transition: ITIL*, TSO, London

OGC (Hrsg.). 2007b. *Service Design: ITIL*, TSO, London

OGC (Hrsg.). 2007c. *Service Operation: ITIL*, TSO, London

Röckle, H. und Dorrhauer, C. 2011. *Messbarkeit der Sicherheitsqualität im Lebenszyklus betrieblicher Anwendungssysteme*, in: Herausforderungen an die Wirtschaftsinformatik: Betriebliche Anwendungssysteme, News & Media, Berlin, S. 155-174

Schimpf, G. und Röckle, H. 2009. *Security Reporting in großen Unternehmen*, in: Horster, P./ Schartner, P. (Hrsg.) D.A.CH Security 2009, syssec, S. 240-252

Sommerville, I. 2011. *Software Engineering*, Boston, Pearson

Data-Mining Routinen in SAP BI 7.0

Norbert Ketterer
Fachbereich Angewandte Informatik
Hochschule Fulda
36039 Fulda
E-mail: norbert.ketterer@informatik.hs-fulda.de

STICHWORTE
Data-Mining, SAP-BI 7.0, Klassifikation, Neuronale Netzwerke, Benchmarking, RapidMiner.

ABSTRACT

In der vorliegenden Arbeit werden ausgewählte klassifizierende Data-Mining-Verfahren aus SAP BI 7.0 und RapidMiner an Hand etablierter Benchmarks analysiert. Schließlich wird eine Implementierung eines alternativen Data-Mining-Verfahrens in SAP-BI vorgestellt, welches auf neuronalen Netzen basiert.
Dieses Paper ist im Wesentlichen eine Wiedergabe der bereits 2012 im Rahmen der AKWI-Tagung in Pforzheim erschienenen Arbeit von Augustin und Ketterer durch einen der Autoren (Augustin& Ketterer 2012).

EINLEITUNG

Die SAP AG bietet bereits seit geraumer Zeit in deren Business-Intelligence-Produkt SAP-BI eine Auswahl von Funktionen an, die Standardmethoden des Data-Mining implementieren. Die Methode der „Klassifikation“ wird dabei in der aktuellen Version von SAP-BI durch eine Data-Mining-Funktion implementiert, die im Wesentlichen entropiebasiert einen Entscheidungsbaum erzeugt (SAP 2007) – die Funktionsweise ist ähnlich dem bekannten C 4.5 Algorithmus; alternative Klassifikationsverfahren – etwa neuronale Netze - sind dagegen nicht Teil des von SAP-BI bereitgestellten Funktionsumfangs. Weitere wesentliche Data-Mining-Verfahren – speziell in Anlehnung an die Verfahrensübersicht aus (Ester& Sander 2009)– sind in SAP-BI: Clusteranalyse über ein Verfahren ähnlich dem „K-Means-Algorithmus“, Assoziationsanalyse über ein Verfahren ähnlich dem „A-Priori-Algorithmus“ sowie eine Regressionsanalyse.
RapidMiner deckt dagegen eine größere Bandbreite von Klassifikationsverfahren ab; hier stellt etwa der C 4.5-Algorithmus nur eine Alternative zwischen einer Reihe von Verfahren dar, die u.a. auch auf neuronalen Netzen basieren.

Das Ziel dieser Arbeit besteht zum einen darin, die SAP-BI Data-Mining-Lösung zur Klassifikation auf Basis etablierter, veröffentlichter Benchmarks bezüglich seiner Klassifikationsgenauigkeit zu bewerten; eine ähnliche Analyse wird zudem für RapidMiner – hier für den C 4.5 Algorithmus sowie ein neuronales Netz mit einem verborgenen Layer – durchgeführt.
Zum anderen wird die Implementierung eines alternativen Verfahrens des Data-Mining in SAP-BI skizziert, welches ebenfalls auf neuronalen Netzen mit einem verborgenen Layer basiert. Das Benchmarking dieser Implementierung wird hier wiederum detailliert dokumentiert.

KLASSIFIZIERNDE DATA-MINING-VERFAHREN IN SAP-BI UND RAPIDMINER

Bei Anwendung eines Klassifikationsverfahrens sind, anders als etwa beim Clusterverfahren, die Klassen bereits bekannt. Es ist Aufgabe des Klassifikationsverfahrens, Objekte auf Basis von Attributwerten den Klassen zuzuordnen. Hierbei ist ein Klassifikationswissen aufzubauen, welches die Klassenstruktur beschreibt (Ester& Sander 2009).
Der Klassifikationsprozess besitzt anfangs eine Trainingsphase, die dem Aufbau des Klassifikationswissens dient; nach der Trainingsphase soll das Wissen ausreichen, neue Objekte selbständig in das Klassenschema einzuordnen. Das Training erfolgt dabei auf Basis historischer Daten für die die Klassenzuordnung bereits bekannt ist, die Trainingsdaten sollten dabei eine ähnliche Klassenverteilung besitzen wie die zu analysierenden Daten.

Bekannte Klassifikationsverfahren stellen der C4.5 Algorithmus von Quinlan (Quinlan 1986) sowie sein Vorgänger ID3 dar. Bei diesen Algorithmen wird versucht, die Ausgangsmenge schrittweise in Klassen aufzuteilen, wobei in jedem Schritt der maximale Informationsgewinn erzielt werden soll. Ein bei diesen Schritten generierter Entscheidungsbaum repräsentiert dann das Klassenwissen. Eine frühe Darstellung der Idee findet sich beispielsweise in Quinlans Veröffentlichung (Quinlan 1986) eine grundlegende Darstellung im Buch von Ester und Sander (Ester& Sander 2009) ein Vergleich von C4.5 mit dem Vorgänger ID3 und dem Nachfolger C5 in der Arbeit von Shahnaz (Shahnaz 2006).

Für die Entropie und den Informationsgewinn werden bei diesen Verfahren typischerweise Definitionen wie folgt verwendet (Ester& Sander 2009):

$$Entropie(T) = -\sum_{i=1}^{k} p_i log_2 p_i \quad (1)$$

$$Informationsgewinn\ (T,\ A) = Entropie(T) - \sum_{i=1}^{m} \frac{|T_i|}{|T|}\ Entropie(T_i) \quad (2)$$

Weitere Klassifikationsverfahren basieren neben Entscheidungsbäumen auf - siehe etwa (Maimon, 2010) - Bayes'schen Netzen, Support Vector Maschinen und Neuronalen Netzen.
Während in SAP BI 7.0 lediglich ein Verfahren zur Klassifikation – nämlich ein entropiebasiertes Entscheidungsbaumverfahren - implementiert wurde, finden sich in RapidMiner neben dem klassischen Entscheidungsbaum nach C4.5 unter anderem auch verschiedene entscheidungsbaumbasierte Modelle – neben C 4.5 und dem älteren ID3 auch CHAID, Bayes'sche Modelle, Support-Vektor-Modelle, Regelbasierte Modelle wie „Ripper" – siehe hier zu Cohen (Cohen 1995) - sowie Neuronale Netzwerke. Es kann hier neben einem einschichtigen Perzeptron auch ein Multi-Layer Netzwerk aufgebaut werden.

BENCHMARKS FÜR KLASSIFIKATIONSROUTINEN

Das UCI-Repository listet eine Reihe von Benchmarks, die sich bezüglich der Art der Daten (etwa „stetig", „diskret" und dem „Grad der Separierbarkeit") stark unterscheiden. Diese Benchmarks bilden die Referenz für eine Vielzahl von Veröffentlichungen, von denen pro Benchmark eine Reihe von Referenzen im Repository angegeben werden (UCI 2012).

Name in UCI (Name in Ref)	Elemente	Klassen
IRIS-Data-Set (IRIS) (Opitz 1999)	**150**	**3**
Congressional Voting Records Data Set (House-Votes-84) (Opitz 1999)]	**435**	**2**
Heart Disease Data Set (Heart-Cleveland) (Opitz 1999)]	**303**	**2**
Chess (King-Rook vs. King-Pawn) Data Set (kr-vs-kp) (Opitz 1999)]	**3092**	**2**
Wine Data Set (Wine) (Rokach 2008)	**178**	**3**
Census Income (Adult) (Kohavi 1996)	**32561**	**2**
Zoo (Zoo) (Rokach 2008)	**101**	**7**

Tabelle 1: Untersuchte Benchmarks des UCI-Repositories (UCI 2012) – Referenzname in Literatur in Klammern

Name in UCI (Name in Ref)	Bemerkung
IRIS-Data-Set (IRIS) (Opitz 1999)	Klassifikation der IRIS-Blumen basierend auf der Länge der Kelch/ Kronblätter. Eine Klasse ist linear separierbar von den übrigen, die anderen zueinander nicht. Daten sind stetig.
Congressional Voting Records Data Set (House-Votes-84) (Opitz 1999)]	Klassen unterscheiden "Republikaner" und "Demokraten" abhängig von 16 Einzelthemen[3], die verschiedenen Entscheidungsmöglichkeiten wurden dabei verdichtet. Daten sind diskret.
Heart Disease Data Set (Heart-Cleveland) (Opitz 1999)]	Der Datensatz besitzt 76 Parameter[4], die Literatur verwendet oft nur eine Teilmenge (etwa 13 oder 14) – (Opitz 1999) verwendet 13 Parameter. Klassen sind „krank" Ja/ Nein. Daten sind gemischt stetig/ diskret.
Chess (King-Rook vs. King-Pawn) Data Set (kr-vs-kp) (Opitz 1999)]	Entscheidung, ob der weiße Spieler ein Schachspiel auf Basis einer gegebenen Situation gewinnen kann – ein Bauer steht dabei bereits auf A7. Die Feldsituation wird durch 36 diskrete Merkmale beschrieben[5].
Wine Data Set (Wine) (Rokach 2008)	Unterscheiden von 3 Weinen an Hand von 13 Merkmalen, wie Phenolgehalt. Die Merkmale sind stetig.
Census Income (Adult) (Kohavi 1996)	Entscheidung an Hand einer Reihe von Kriterien, ob das Einkommen >50K ist. Die Merkmale sind diskret./ stetig.
Zoo (Zoo) (Rokach 2008)	Tiere werden anhand von 17 – größtenteils boolschen Merkmalen – in 7 Klassen eingeordnet[6]. Die Merkmale sind alle diskret.

Tabelle 2: Untersuchte Benchmarks des UCI-Repositories (UCI 2012) – Referenzname in Literatur in Klammern

BEWERTUNG DER EXISTIERENDEN VERFAHREN

Für sämtliche Benchmarks wurde ein Klassifikationslauf auf Basis von Entscheidungsbäumen in RapidMiner (C 4.5) sowie SAP-BI (Entscheidungsbäume) durchgeführt und mit den Benchmarks der in Tabelle 2 und Tabelle 2 referenzierten Quelle verglichen.

Methoden zum Vergleich von Klassifikatoren

Aus einer Trainingsmenge können sehr unterschiedliche Klassifikatoren gelernt werden - siehe hierzu auch wieder (Ester& Sander 2009). Ein typisches Verfahren zum Vergleich der Klassifikatoren bei einer vergleichsweise kleinen Anzahl von Objekten mit bekannter Klasse stellt die „Kreuzvalidierung" dar. Die k-fache Kreuzvalidierung teilt die Menge der Daten in k gleich große Teilmengen, von denen jeweils k-1 Teilmengen zum Training und die verbleibende Teilmenge zum Test verwendet wird.
Der Klassifikationsfehler wird in Anlehnung an die Methode in der Arbeit von Opitz und Maclin (Optiz&Maclin 1999) als Mittelwert einer 5-maligen Wiederholung einer 10-fachen Kreuzvalidierung gebildet (was einem k = 10 entspricht).

Klassifikationsalgorithmen auf den Datensätzen

Die Entscheidungsbäume sind gemäß Benchmark einem Pruning zu unterziehen – es ergeben sich die in Abbildung 1 dargestellen Abweichungen.

Datensatz	*Rapidminer C4.5*	*SAP-BI DT*	*Benchmark C4.5*
Iris	8% (+ 2.8%)	13.33% (+ 8.13%)	5.2%

Abbildung 1: IRIS Daten, klassifiziert via Entscheidungsbaum, Abweichung von RapidMiner und SAP-BI Entscheidungsbaum (DT) zum Benchmark

Ein Beispiel einer Fehlermatrix direkt aus dem Analyseprozessdesigners des SAP BI zeigt Abbildung 3; für diese spezifische Instanz aller Validierungsschritt wurde eine Genauigkeit von 86% erreicht, den zugeordneten Entscheidungsbaum zeigt Abbildung 2. Zu beachten ist, dass die Anzahl der Sätze aufgrund des Validierungsverfahrens mit k = 10 nur „15“ beträgt und das es sich hier nur um eine Instanz aller Validierungen handelt, wobei der Klassifikationsfehler in diesem Fall auch dem durchschnittlichen Fehler entspricht.

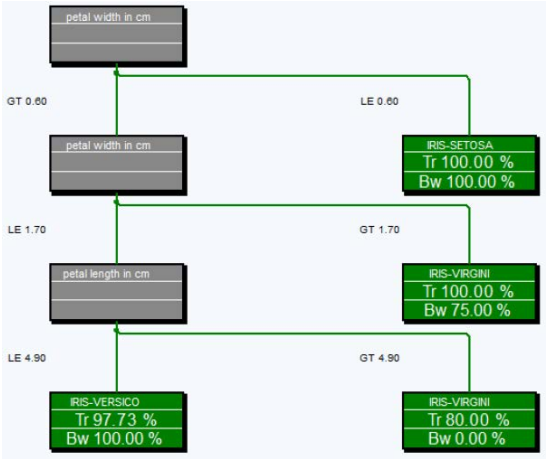


Abbildung 2: Entscheidungsbaum für IRIS-Datensatz (pruned) aus SAP-BI

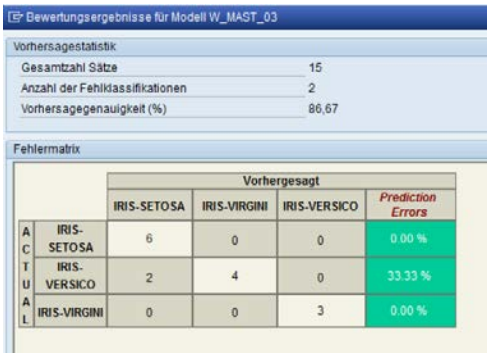


Abbildung 3: Ergebnis eines Validierungslaufes für IRIS

Gemäß der Vorgaben der Benchmark-Literatur ist der Entscheidungsbaum bei den „Voting-“, „Herzerkrankungs-“ und „Schach-Daten“ ebenfalls einem “Pruning” zu unterziehen. Der SAP-Entscheidungsbaum besitzt einen Entscheidungsfehler, der der Benchmark sehr nahe kommt.

Datensatz	*Rapidminer C4.5*	*SAP-BI DT*	*Benchmark C4.5*
House-Votes-84	6.45% (+ 2.85%)	4.6% (+ 1%)	3.6%
Heart-Cleveland	21.14% (- 3.16%)	25.81% (+ 1.51%)	24.3%
Kr-vs-Kp	0.31% (- 0.29%)	0.94% (+ 0.34%)	0.6%
Census-Income	16.51% (+ 1%)	15.38% (- 0.16%)	15.54%
Wine	6.14% (- 7.9%)	11.11% (- 2.93%)	14.04%
Zoo	3.91% (-3.02%)	10% (+ 3.07%)	6.93%

Abbildung 4: übrige Beispieldaten, klassifiziert via Entscheidungsbaum (DT)

ERWEITERUNG VON SAP-BI 7.0 UM EIN NEURONALES NETZ

Erweiterungsmöglichkeiten von SAP BI 7.0 für Hochschulen

Hochschulen und Universitäten betreiben ein SAP BI 7.0 typischerweise beim UCC gemäß Preislistenposition „F2“ oder „F3“ (UCC 2012) – dieses sind „Shared Systeme“, die keine Entwicklungsberechtigung besitzen, sondern lediglich ermöglichen, ein Data-Warehouse über die DW-Modelling-Workbench zu modellieren, sowie Data-Mining-Prozesse mit Hilfe des Analyse Prozess Designers (APD) aufzusetzen.
Innerhalb der Definition eines Analyseprozesses kann jedoch trotzdem eine einfache ABAP-Routine eingebunden werden, die mit Hilfe eines externen Remote Function Call (RFC) in ein anderes System – etwa einem SAP-Entwicklungssystem der Preislistenpostion „G“ – zeigt, welches ABAP-Entwicklungen erlaubt. Somit können komplexe Erweiterungen in das Entwicklungssystem ausgelagert und vom APD über einen RFC referenziert werden. Werden Daten des neuronalen Netzwerks direkt im Data-Warehouse – etwa in einem DSO - gespeichert und muss auf diese im Rahmen des Analyseprozesses zugegriffen werden, kann das mit Hilfe eines BAPIs (BAPI_ODSO_READ_DATA_UC) aus dem Entwicklungssystem erfolgen. Die Spezifikation des RFC kann als Codefragment direkt in die APD-Routine eingebunden werden, die zugehörigen ABAP-Objekte werden direkt von SAP-BI verwaltet; dies gilt nicht als Entwicklungstätigkeit (siehe Abbildung 5 und Abbildung 6).

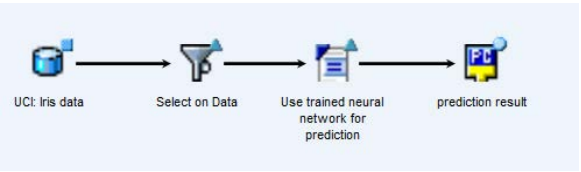


Abbildung 5: Einbindung einer Routine in den APD

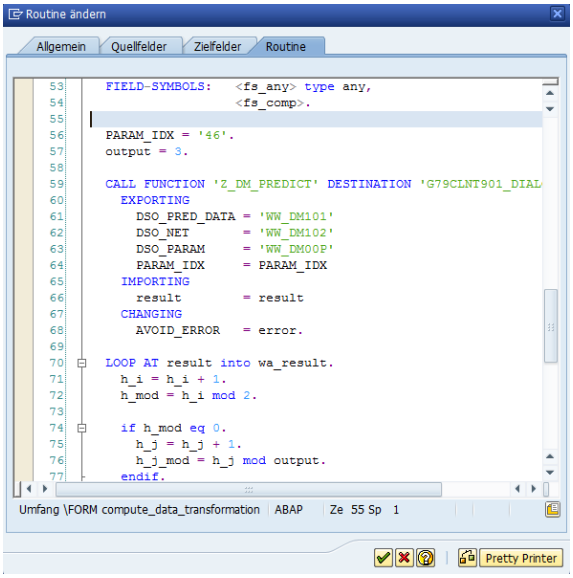


Abbildung 6: Eingebundene Routine in APD

Dieses Konzept der Einbindung erlaubt auch Hochschulen unter den gegebenen Restriktionen des Lizenzabkommens eine Einbindung beliebiger Data-Mining-Routinen; beispielsweise kann eine Data-Mining-Routine nun auch komplett außerhalb von SAP realisiert und mit dem Business-Connector oder Netweaver-Funktionen in das ABAP-System eingebunden und dann per RFC aus dem APD angesprochen werden.

Struktur des Netzwerks und verwendete Algorithmen

Ein neuronales Netz besteht aus einer Menge von Knoten, die über Kanten miteinander verbunden sind. Das Netz besteht aus einer Input-Schicht, einer Reihe verborgener Schichten und einer Output-Schicht, welche mit Kanten, denen Gewichte zugeordnet sind verbunden sind. Es existieren eine Reihe von Aktivierungs- und Ausgabefunktionen in Knoten, die typischerweise die Form einer „Squashing"-Funktion besitzen (Ester& Sander 2009)

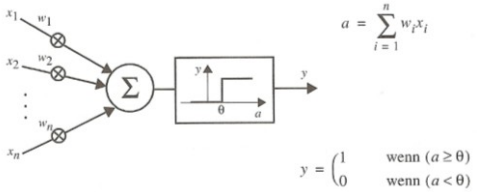


Abbildung 7: Gewichtete Eingangskanten eines Neurons aus (Ester& Sander 2009)

Ein Knoten kann mit Hilfe genau einer Hyperebene die Eingangsdaten separieren - siehe beispielsweise (Ester& Sander 2009) - durch weitere Schichten können weitere Hyperebenen gelernt werden.

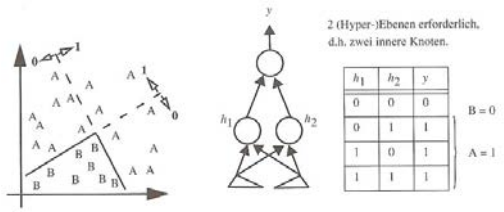


Abbildung 8: Skizze eine Neuronalen Netzwerks sowie der separierbaren Datenklassen - beides aus (Ester& Sander 2009)

Die Klassifikation wird durch die Belegung der Kantengewichte des Netzes gesteuert. Ist die Klassifikation anzupassen, müssen bei einem mehrstufigen Netzwerk eine Reihe von Kanten-gewichten angepasst werden, einen typischen Algorithmus hierfür stellt der „Backpropagation-Algorithmus" dar (Es handelt sich bei diesem Algorithmus i.W. um ein Gradientenabstiegsverfahren). Ein Backpropagation-Algorithmus wurde auch hier implementiert – er wurde dabei um eine Flat-Spot-Elimination und einen Momentum-Term ergänzt. Die Speicherung der Netzstruktur erfolgte in einer DSO – für Details bezüglich der Implementierung sei auf (Augustin 2011) verwiesen.

Das Netz ist – in Anlehnung an die Vergleichsbenchmarks einen Feed-Forward-Netz mit einem verdeckten Layer; es wurden die folgenden Parameter für das neuronales Netz/ den Lernalgorithmus gewählt:

Parameter	Belegung
Lernrate	$0.1 < \alpha < 0.6$
Momentum	$0.2 < \eta < 0.99$
Epochen	$20 < Epochen < 80$
Sigmoid. T.	0.2
FSE	$0.05 < \tau < 0.1$
Input	Anzahl Attribute in D ohne Klassen
Hidden	$5 < hidden < 25$
Output	Anzahl an Klassenattribute in D
Gewicht-Bias	$-0.5 < w_{bias} < 0.5$
Gewicht-Normal	$-0.5 < w_{ij} < 0.5$
Aktivierungsfunktion	$\frac{1}{1+e^{-x/T}}$
Ausgabefunktion	$O_i = id(f_{act}) = f_{act}(net_j)$

Abbildung 9: Parameter des neuronalen Netzes/ des Trainings

Der Grund für diese Parameter liegt in der Vergleichbarkeit mit den Benchmarks (Opitz & Maclin 1999) sowie genereller Vorgaben aus Zell (Zell 2003).

BEWERTUNG DER ERWEITERUNG
Ergebnisse der Literatur

Für die ausgewählten Benchmarks existieren Ergebnisse in der Literatur – speziell die Arbeit von Opitz& Maclin (Optiz&Maclin 1999) stellt für neuronale Netze Ergebnisse für die verwendeten Benchmarkdatensätze vor, in denen auch die Parameter der neuronalen Netze vorgegeben sind.
Für die übrigen drei Benchmarks liegen keine Details bezüglich neuronaler Netze aus der Literatur vor, so dass alleine die Ergebnisse des mehrlagigen neuronalen Netzes aus RapidMiner und den Entscheidungsbäumen der Literatur als Benchmarks verwendet wurden. Schließlich wird das Ergebnis mit dem durch Agustin implementierten (Augustin 2011) für SAP-BI entwickelten neuronalen Netz verglichen. Basis des Vergleiches ist wiederum eine 5 malige Kreuzvalidierung mit Faktor 10. Das Feed-Forward-Netz besaß in den Tests die folgenden Parameter:

Datensatz	Instanzen	Eingabeneuronen	Ausgabeneuronen	verdeckte N.	Epochen
Iris	150	4	3	5	80
House-Votes-84	435	16	1	5	40
Heart cleveland	303	12	1	5	40
Kr-vs-Kp	3196	74	1	15	20
Wine	178	13	3	15*	20*
Census-Income	32561	14	1	15*	20*
Zoo	101	17	7	15*	20*

Abbildung 10: Parameter des Benchmarks – mit „*" gekennzeichnete Parameter waren nicht in der Literatur dokumentiert

Neuronale Netz auf den Datensätzen
Der Iris-Datensatz stellte sich mit dem gegebenen Parametersatz in RapidMiner als ähnlich gut lösbar durch das neuronale Netz dar, wie im Benchmark; unser („das Fuldaer") neuronale Netz lag dagegen bei vorgegebener verdeckten Neuronen Anzahl der Klassifikationsfehler weit über der Benchmark (> 20%).

Datensatz	Rapidminer NN	Fulda-NN @ SAP-BI	Benchmark NN
Iris	4.67% (- 0.37%)	25% (+ 20.7%)	4.3%

Abbildung 11: Vergleich „Fulda NN“ mit Benchmark für IRIS Daten

Die Klassifikationsgenauigkeit konnte nur durch das Einfügen weiterer verdeckten Neuronen erhöht werden – ein Hinzufügen zwei weiterer verdeckter Neuronen erhöht die Genauigkeit in einem Masse, dass das Ergebnis von RapidMiner ungefähr erreicht werden konnte. Im Fulda-NN trat somit ein klares „Underfitting“ aus, welches durch Erhöhen der verdeckten Neuronen behoben werden konnte.

Für das „Congressional Voting“ ergaben sich die Ergebnisse von Abbildung 12 – RapidMiner erreicht die Benchmark gut, die eigene Routine weicht um > 3% ab. In diesem Fall wurde durch die Erhöhung der Anzahl der Neuronen im eigenen Netz nur leichte Verbesserungen, teilweise sogar Verschlechterungen erreicht .

Datensatz	Rapidminer NN	Fulda-NN @ SAP-BI	Benchmark NN
House-Votes-84	5.53% (- 0.63%)	8.22% (+ 3.32%)	4.9%

Abbildung 12: Vergleich Rapidminer-NN, mit „Fulda-NN“ mit Benchmark für Voting-Daten

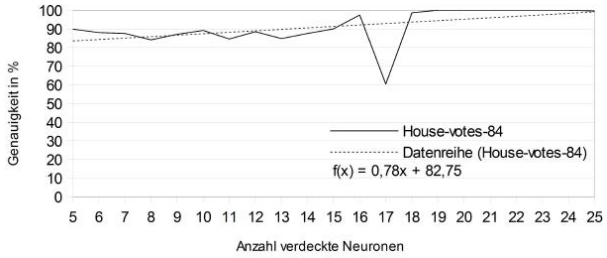


Abbildung 13: Abhängigkeit des Klassifizierungsfehlers von Anzahl der verdeckten Neuronen

Abbildung 14 zeigt die Ergebnisse für die Herz-Daten – es fällt die Nähe von RapidMiner zur Benchmark auf. Für vergleichbare Ergebnisse im eigenen neuronalen Netz war eine Erhöhung der verdeckten Neuronen notwendig. Eine Erhöhung von 5 auf 6 Neuronen erhöhte die Genauigkeit um > 5% (absolut). Wie im Falle des „Iris-Datensatzes“ lag ein „Underfitting“ vor.

Datensatz	Rapidminer NN	Fulda-NN @ SAP-BI	Benchmark NN
Heart-Cleveland	18.56% (- 0.04%)	36% (+ 17.4%)	18.6%

Abbildung 14: Vergleich Rapidminer-NN, mit „Fulda-NN“ mit Benchmark für Herz-Daten

Zur Abbildung des Schach-Problems wurde experimentell versucht, die 36+1 diskreten Attribute des Problems in nominelle Werte umzuwandeln. Aufgrund der im neuronalen Netz vorhandenen schlechten semantischen Trennung war die Klassifizierung unbefriedigend. Die bei Optiz und Maclin (Optiz&Maclin 1999) vorgeschlagene binäre Darstellung in 74 Attributen liefert das folgende sehr gute Ergebnis.

Datensatz	Rapidminer NN	Fulda-NN @ SAP-BI	Benchmark NN
Kr-vs-Kp	1.97% (- 0.33%)	1.95% (- 0.35%)	0.6%

Abbildung 15: Vergleich Rapidminer-NN, mit Fulda-NN mit Benchmark für Schach-Daten

Für die übrigen Benchmarks wurden keine Vergleichszahlen auf Basis neuronaler Netze gefunden, so dass als Benchmark das Klassifikationsverfahren nach C4.5 herangezogen wird; die Daten hierfür stammen von Rokach (Rokach 2008), es wurden 15 verdeckte Neuronen verwendet. Benchmark zur Bewertung des „Fulda-NN“ ist somit lediglich RapidMiner.

Datensatz	Rapidminer NN	Fulda-NN @ SAP-BI	Benchmark C4.5
Wine	3.95% (- 10.09%)	0.68% (- 13.36%)	14.04%
Census-Income	15.61% (+ 0.07%)	0.37 (- 15.17)	15.54%
Zoo	6.91% (+ 0.02%)	8.41% (- 1.48%)	6.93%

Abbildung 16: Vergleich Rapidminer-NN, mit Fulda-NN mit C4.5 Benchmark für übrige Daten

Eine Erhöhung der verdeckten Neuronen für die problematischen Modelle (etwa IRIS) auf 15 führt schließlich zu folgenden Ergebnissen:

Datensatz	Rapidminer NN	Fulda-NN @ SAP-BI	Benchmark NN	Benchmark C 4.5
Iris	4.67% (- 0.37%)	2.67% (- 1.63%)	4.3%	5.2%
House-Votes-84	5.53% (- 0.63%)	6.12% (- 1.22%)	4.9%	3.6%
Heart-Cleveland	18.56% (- 0.04%)	7.62% (- 17.4%)	18.6%	24.3%
Kr-vs-Kp	1.97% (- 0.33%)	1.95% (- 0.35%)	2.3%	2.3%
Datensatz	**Rapidminer NN**	**Fulda-NN @ SAP-BI**	**Benchmark C 4.5**	
Wine	3.95% (- 10.09%)	0.68% (- 13.36%)	14.04%	
Census-Income	15.61% (+ 0.07%)	0.37 (- 15.17)	15.54%	
Zoo	6.91% (+ 0.02%)	8.41% (- 1.48%)	6.93%	

Abbildung 17: Ergebnisse des Benchmarkings bei erhöhter Neuronenanzahl („SAP-NN“ bezeichnet dabei das Fuldaer-NN in SAP-BI)

RapidMiner besitzt – zumindest in der verwendeten Community-Edition – eine deutlich geringere Abhängigkeit von der Anzahl der verdeckten Neuronen, als das eigene Netz.

ZUSAMMENFASSUNG

Die Evaluation zeigt, dass die entscheidungsbaumbasierten Verfahren in SAP und RapidMiner vergleichbare Ergebnisse zum Benchmark liefern.

Es wurde ein Prototyp erstellt, in dem SAP-BI mit einfachen Routinen direkt im APD um neuartige Klassifikationsroutinen erweitert werden kann.

Diese Klassifikationsroutinen wurden mit verschiedenen etablierten Benchmarks evaluiert – aktuell basieren diese Routinen jedoch lediglich auf sehr grundlegenden Standardverfahren der Literatur; es besteht eine weite Bandbreite der Verbesserung dieser Verfahren.

Abhängig vom Datensatz (etwa bei „Wine“ oder „Heart Cleveland“) ergeben sich bereits jetzt deutliche Verbesserungen des Klassifikationsresultats gegenüber den entscheidungsbaumbasierten Verfahren.

Es wurde zudem ein Verfahren implementiert, welches auch Hochschulen erlaubt beliebige Data-Mining-

Routinen in SAP- BI zu implementieren – bis hin zu einer Einbindung externer Routinen.

LITERATUR

Y. Augustin, N. Ketterer: Data-Mining Routinen in SAP BI 7.0, *Management und IT, Tagungsband zur AKWI-Fachtagung 2012*, S.41-54, News & Media 2012

Y. Augustin: Design und Implementierung von Klassifikationsroutinen auf Basis neuronaler Netze in SAP BI 7.0, *Master-Thesis am FB-AI*, HS Fulda 2011

W. W. Cohen: Fast Effective Rule Induction, *Machine Learning 12*, 1995

M. Ester, J. Sander: Knowledge discovery in databases: Techniken und Anwendungen, Springer, 2009

R. Kohavi: A study of cross-validation and bootstrap for accuracy estimation and model selection, *International Joint Conference on Artificial Intelligence 14*: S.1137–1145, 1995

R. Kohavi: Scaling up the accuracy of naive-bayes classifiers: a decision-tree hybrid., *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining*, 1996

O. Maimon, L. Rokack: Data Mining and Knowledge Discovery Handbook, 2nd ed. Springer, 2010

D. Opitz, R. Maclin: Popular ensemble methods: an empirical study, *Journal of Artificial Intelligence Research* 11, S.169–198, 1999

J.R. Quinlan: Induction of Decision Trees, *Machine-Learing 1*, S. 81-106, Kluwer 1986

RapidMiner: Deutschsprachiger Internetauftritt unter: http://rapid-i.com/content/view/181/190/lang,de/

L. Rokach: Genetic algorithm-based feature set partitioning for classification problems, *Pattern Recognition*. 41, S.1676–1700, May 2008

SAP AG: Training-Material for Course BW380, 2007

F. Shahnaz: Decision Tree based Algorithms, in Lecture-Notes in Data-Mining von M.W. Berry, M. Browne, World Scientific, 2006

SAP UA EMEA Portal: Preisliste des SAP-UCC von 2012, https://portal.ucc.uni-magdeburg.de/irj/portal/anonymous

UCI Machine Learning Repository: Classification Data-Sets, retrieved 2012, http://archive.ics.uci.edu/ml/datasets.html (Default-Task = "Classification")

Zell: Simulation neuronaler Netze, Oldenbourg, 2003

KONTAKT

Norbert Ketterer lehrt seit Ende 2008 Wirtschaftsinformatik an der Hochschule Fulda. Sein Hauptinteresse liegt in dem Bereich „Betriebliche Anwendungssysteme", insbesondere deren Unterstützung von betrieblichen Geschäftsprozessen.

BERECHNUNG DES IT-WERTBEITRAGS

Martin Kütz
Fachbereich Informatik und Sprachen
Hochschule Anhalt
D-06366 Köthen, Deutschland
E-Mail: m.kuetz@inf.hs-anhalt.de

SCHLÜSSELWORTE

Barwert, Kapitalbedarf, Residualgewinn, Transferpreise, Wertbeitrag

EINLEITUNG

Seit Längerem wird intensiv diskutiert, welchen Beitrag die IT zum Wert oder zur Wertsteigerung eines Unternehmens leistet. In der Regel sind die Aussagen von eher qualitativer Natur oder die dargestellten Quantifizierungen messen eher die Wertbeitragsfähigkeit einer IT-Organisation (Bearing Point 2011). In diesem Beitrag wird ein Rechenmodell vorgestellt, dass direkt einen finanziellen Wertbeitrag der IT im Sinne der wertorientierten Unternehmensführung ermittelt.

FRAGESTELLUNG UND ZIELSETZUNG

IT ist in Unternehmen und anderen Organisationen unverzichtbar (Krcmar 2010, S. 1 - 4). Obgleich der Anteil der IT-Kosten an den gesamten Kosten einer Organisation eher gering ist, so ist doch die Abhängigkeit von der Funktionsfähigkeit, Verfügbarkeit und Leistungsfähigkeit der IT-Systeme enorm. Nicht zuletzt aufgrund gesetzlicher Anforderungen, z.B. Meldepflichten, ist eine geregelte Geschäftstätigkeit ohne den Einsatz von IT nicht (mehr) möglich.
Vor diesem Hintergrund stellt sich die Frage, in welchem Maße die IT zum Unternehmenserfolg beiträgt, insbesondere den Markt- oder Börsenwert des Unternehmens (positiv) beeinflusst. Kurz: Wie trägt IT zum Wert des Unternehmens / der Organisation bei?
Um diese Frage zu beantworten, muss man klären, wie der Wert eines Unternehmens oder einer Organisation zu bestimmen ist. Geeignete Methoden bietet die wertorientierte Unternehmensführung in Form des Residualgewinns (oder: Economic Value Added (EVA), vergleiche (Stiefl und von Westerholt 2008)). Ziel dieses Beitrages ist es, die Ansätze der wertorientierten Unternehmensführung auf die IT eines Unternehmens oder einer Organisation zu übertragen.
Da in diesem Beitrag zwei verschiedene Ansätze zur Ermittlung des IT-Wertbeitrages vorgestellt werden, ergibt sich als weiteres Ziel, die Verbindung zwischen den beiden Verfahren bzw. die Unterschiede zwischen ihnen herauszuarbeiten.

METHODEN ZUR BERECHNUNG DES IT-WERTBEITRAGES

Begriffliche Grundlagen

Unternehmen müssen Gewinne erwirtschaften, sonst sind sie nicht (über-) lebensfähig. Die wertorientierte Unternehmensführung hat erkannt, dass das aber nicht ausreicht. Die Gewinne müssen sogar eine bestimmte Größenordnung erreichen und überschreiten. Ursache dieser Forderung ist das Kapital, dass die Unternehmen von externen Personen oder Organisationen erhalten. Die Kapitalgeber erwarten für das bereitgestellte Kapital eine bestimmte Rendite. Die Gewinne eines Unternehmens müssen daher so groß sein, dass die Renditeerwartungen der Kapitalgeber befriedigt werden können. Die entsprechenden Auszahlungen an die Kapitalgeber müssen also aus den Gewinnen finanziert werden können, weil sie sonst (auf Dauer) die (finanzielle) Substanz des Unternehmens aufzehren.
Bleibt nach den Auszahlungen an die Kapitalgeber noch ein Teil des Gewinns übrig, so bezeichnet man diesen Residualgewinn als "Übergewinn" oder auch "Economic Value Added" (EVA) - je nach gewählter Berechnungsmethode (Stiefl und von Westerholt 2008).

Das Prinzip des Residualgewinns

Um einen Wertbeitrag der IT im vorgenannten Sinn zu ermitteln, sind vier Komponenten zu ermitteln:

- den durch IT erzielten Erlös oder ein Erlösäquivalent
- die entstandenen IT-Kosten
- den Kapitalbedarf der IT
- die Renditeerwartung der Kapitalgeber

Für den erzielten Erlös einer IT-Organisation kann man im Falle einer innerbetrieblichen Leistungsverrechnung den Verrechnungserlös ansetzen; das ist Grundlage des serviceorientierten Ansatzes. Der projektbasierte Ansatz bezieht sich auf IT-Projekte und betrachtet als Erlös den durch die Projekte erzielten oder erzielbaren Nutzen.
Die Ermittlung der IT-Kosten ist begrifflich am einfachsten abzugrenzen. Jedoch ist sicherzustellen, dass sie vollständig einbezogen werden (können). Bei der Betrachtung von IT-Bereichen sind das (natürlich) nur die Kosten der Leistungserstellung, nicht die Kosten der Leistungsverwendung; es geht hier also nicht um Kosten im Sinne der TCO (Fröschle und Kütz 2011, S. 368).
Der Kapitalbedarf der IT ergibt sich aus zwei Komponenten, zum einen dem im Anlagevermögen der IT gebundene Kapital und zum anderen dem betriebsnotwendigen Kapital der IT, das sie benötigt, um den laufenden Betrieb aufrechterhalten zu können.
Zur Ermitlung des ersten Teilbedarfs muss man die Restbuchwerte des IT-Anlagevermögens ermitteln. Das sollte über die Anlagenbuchhaltung möglich sein. Um die Kon-

sistenz zum Wertbeitrag des Unternehmens zu erhalten, sollte man mit den bilanziellen Abschreibungen arbeiten (Das ist methodisch allerdings nicht zwingend). Bei der Berechnung ist zu entscheiden, ob man das IT-Anlagevermögen zu bestimmten Zeitpunkten erhebt oder mit einem Jahresmittelwert arbeitet. Der Anwender sollte dieselbe Betrachtungsweise wählen, die in der Organisation auch an anderen Stellen genutzt wird.

Zur Ermittlung des zweiten Teilbedarfs geht man davon aus, dass das Unternehmen einen bestimmten branchen- und unternehmensspezifischen Cash-to-Cash-Cycle (CCC) aufweist. Der CCC beschreibt die Zeitspanne, die ein Unternehmen benötigt, bis die in Material und Vorleistungen gebundenen finanziellen Mittel durch Umsatzerlöse wieder freigesetzt werden. Diese Zeitspanne wird hier als Anteil an der Dauer einer Planungsperiode angesehen (Krause und Arora 2008, S. 105 – 106). Dementsprechend müssen auch die IT-Kosten des laufenden Betriebs (ohne Abschreibungen!) durch Kapital vorfinanziert werden. Dieses betriebsnotwendige Kapital entspricht demzufolge demjenigen Anteil der IT-Kosten einer Planungsperiode, den der CCC als Zeitspanne an der Länge der Planungsperiode aufweist. Hat das Unternehmen also einen CCC von 6 Monaten, so hat das betriebsnotwendige Kapital (der IT) ein Volumen von 50% der gesamten IT-Kosten des Jahres.

Um schließlich die Renditeerwartungen der Kapitalgeber zu bestimmen, sind mehrere Fragen zu beantworten:

- Wer sind die Kapitalgeber?
- Was sind Ihre Erwartungen?
- Wie kann man den entsprechenden finanziellen Wert ermitteln?

Bei den Kapitalgebern ist zwischen Eigenkapitalgebern und Fremdkapitalgebern zu unterscheiden. Der Eigenkapitalgeber hat ein bestimmtes Kapital in das Unternehmen investiert, das sich in den Bilanzpositionen zum Eigenkapital manifestiert. Auf dieses Kapital erwartet er eine bestimmte Verzinsung. Der Fremdkapitalgeber hat der Organisation ebenfalls Kapital überlassen, z.B. in Form eines Kredites. Er erwartet ebenfalls eine bestimmte Verzinsung dieses Kapitals, die er sich aber vertraglich gesichert hat.

Insgesamt hat die Organisation eine bestimmte Kapitalstruktur und aus den unterschiedlichen Renditeerwartungen der verschiedenen Kapitalgeber ergibt sich über die spezifische Kapitalstruktur ein mittlerer Zinssatz. Da Zinsen auf Fremdkapital als Kosten in der Gewinn- und Verlustrechnung (GuV) geführt werden dürfen, reduzieren sie die steuerliche Belastung. Diese Steuereffekte werden in den mittleren Zinssatz eingerechnet. Der solchermaßen angepasste mittlere Zinssatz auf das eingesetzte Kapital ist die WACC = weighted average cost of capital (Stiefl und von Westerholt 2008, S. 31 – 34). Da man das in einem Fachbereich eingesetzte Kapital üblicherweise nicht danach unterscheiden kann, aus welcher Quelle es stammt, insbesondere nicht, ob Eigenkapital oder Fremdkapital eingesetzt wurde, werden die Kapitalkosten, also die Zinsen auf das eingesetzte Kapital, durch die Multiplikation des entsprechenden Kapitalbetrages mit dem WACC bestimmt.

Damit hat der Residualgewinn folgende Struktur:

$$RG = E - K - AS - RBW \cdot WACC - K \cdot CCC \cdot WACC$$

Dabei bedeutet RG den Residualgewinn, E das Erlösäquivalent, K die Kosten (ohne Abschreibungen), AS die Abschreibungen, RBW den Restbuchwerrt, CCC den (relativen) Cash-to-Cash-Cycle und WACC die Weighted Average Cost of Capital.

Auf der Unternehmensebene werden noch Gewinnsteuern abgezogen, da durch Steuerzahlungen Liquidität und somit Kapital abfließen. Für die Betrachtung interner Wertbeiträge sei das ausgeklammert, weil dies z.B. bei der Investitionsrechnung meistens in gleicher Weise praktiziert wird. Man muss sich aber darüber im Klaren sein, dass der interne Wertbeitrag letztlich so groß sein muss, dass er auch einen Deckungsbeitrag zu den Gewinnsteuern der Gesamtorganisation leisten kann.

Residualgewinne von IT-Projekten

Zunächst sei ein einzelnes Projekt betrachtet. Im Rahmen der Investitionsrechnung werden die durch das Projekt verursachten Liquiditätsflüsse periodenweise für einen bestimmten, vorgegebenen Zeitraum betrachtet. In vielen IT-Organisationen sind 3 Jahre plus Projektlaufzeit üblich. Daraus wird in der Investitionsrechnung der Barwert ermittelt, also der durch das Projekt in der zugrundegelegten Zeitspanne erzielte Vermögenszuwachs der Organisation (Götze 2006, S. 71). sind. Der Barwert des Projektes kann auch als Summe der Periodenbarwerte dieses Projektes dargestellt werden. Dabei wird zugrundegelegt, dass die erzielten Nutzeffekte alle finanziell bewertbar und unmittelbar gewinnrelevant sind.

In der Praxis wird gerne argumentiert, dass viele Nutzenanteile von IT-Projekte nicht finanziell bewertbar seien. Daraus müsste man dann schließen, dass die hier vorgestellte Vorgehensweise nicht praktikabel ist. Aus der Entscheidungstheorie weiß man jedoch, dass (unter gewissen Randbedingungen) jeder beliebige Nutzeffekt ein finanzielles Äquivalent haben muss, wenn man über die Durchführung oder Nichtdurchführung eines Projektes entscheiden will (Laux 2007, S. 82 – 89). Denn es lässt sich stets ein Projekt konstruieren, so dass alle Projektdaten bis auf die Nutzeffekte identisch sind und das konstruierte Projekt einen finanziellen Nutzen derart ausweist, dass sich der Verantwortliche nicht mehr zwischen den beiden Projekten entscheiden kann. Beide Projekte sind (für ihn) äquivalent. Der Barwert berücksichtigt zudem die Kosten, die in Form von Abschreibungen auftreten, da er den gesamten Projektaufwand enthält.

Die hier vorgetragenen Überlegungen orientieren sich an der statischen Investitionsrechnung (Wöhe und Döring 2010, S. 530 – 536). Das hat seine Ursache darin, dass Diskontierungen bei der Übertragung von der Projektebene auf die Gesamt-IT-Ebene wieder eliminiert werden müssten (siehe weiter hinten). Diese Vorgehensweise beruht auch auf der Tatsache, dass bei den in der IT üblichen 3-jährigen Einsatzzeiträumen, die man der Investitionsrechnung zugrundelegt, die Diskontierungseffekte minimal und in der Praxis nicht entscheidungsrelevant sind. Außerdem vereinfacht sich so der Rechenaufwand...

Der Barwert des Projektes muss nun noch um die (kumulierten) Kapitalkosten reduziert werden. Wenn man weiß, welcher Anteil des Projektaufwandes aktiviert wird, ergeben sich daraus sofort die (üblicherweise linearen) Abschreibungen. Der nicht aktivierte Anteil des Projektaufwandes wird als Kosten der Projektperiode geführt. Die jährlichen Betriebskosten sind aus der Investitionsrechnung bekannt und können unmittelbar in die Kapitalkostenermittlung eingesetzt werden. Damit zeigt sich der kumulierte Projektwertbeitrag als Erweiterung oder Modifikation des Barwertes.

Ableitung eines projektbasierten IT-Wertbeitrags

Wie lassen sich nun die Einzeldaten von Projekten nutzen, um einen Wertbeitrag der Gesamt-IT zu errechnen? Betrachtet man die aktuelle Planungsperiode, so kennt man mehrere Projekte, die entweder in dieser Periode durchgeführt werden, in der letzten Periode durchgeführt wurden, in der vorletzten Periode durchgeführt wurden usw.
Mit der in der Investitionsrechnung üblicherweise genutzten Indizierung der Perioden ergibt sich daraus Folgendes: Die aktuell laufenden Projekte sind in Periode 0, die im Vorjahr gelaufenen Projekte sind in Periode 1, die im vorletzten Jahr gelaufenen Projekte sind nun in Periode 2, usw. Für die betrachteten Projekte kennt man aus der Investitionsrechnung die jeweiligen periodenspezifischen Effekte:

- Nutzeffekte in der aktuellen Periode
- IT-Kosten (inkl. Abschreibungen) in der aktuellen Periode
- Restbuchwerte des Projektes in der Anlagenbuchhaltung

Daraus kann man für jedes betrachtete Projekt einen periodenspezifischen Wertbeitrag ermitteln. Dieser Wertbeitrag kann für ein einzelnes Projekt positiv sein, muss es aber nicht sein. Bei aktuell laufenden Projekten wird der Periodenwertbeitrag sogar negativ sein, denn üblicherweise zeigen Projekte in der Projektperiode noch keine Nutzeffekte. Die Vorgehensweise für ein einzelnes Projekt zeigt Tab. 1.

	WACC	10%	CCC	0,5
Periode	0	1	2	3
Projektaufwand, aktivierbar	90			
Projektaufwand, nicht aktivierbar	50			
Projektfolgekosten		80	50	50
Abschreibungen		30	30	30
Nutzeffekte (Erlösäquivalent)		100	150	150
Restbuchwert	90	90	60	30
Kapitalkosten auf Restbuchwert	9	9	6	3
Kapitalkosten auf Projektfolgekosten	0	4	2,5	2,5
Periodenwertbeitrag	-59	-23	61,5	64,5

Tab. 1: Berechnung der Periodenwertbeiträge eines Projektes (Beispiel)

Jetzt werden über alle betrachteten Projekte die periodenspezifischen Größen aufaddiert. Dabei wird vereinfachend angenommen, dass die Projektperioden mit den Planungsperioden vollständig synchronisiert sind. Das ist natürlich in der Praxis nicht der Fall. Insofern wären (eigentlich) entsprechende Abgrenzungsrechnungen erforderlich.
Und man stellt fest, dass die periodenspezifischen Kosten der betrachteten Projektgruppe einen bestimmten Anteil an den Gesamtkosten der IT haben. Jetzt muss man vom Modell her eine entscheidende Annahme machen, nämlich die, dass die gesamte aktuell vorhandene IT das Ergebnis einer (unendlichen) Kette von Projekten ist. Die Effekte von Projekten, die vor sehr langer Zeit durchgeführt werden, sind inzwischen stark "verblasst", wirken aber in schwacher Konzentration immer noch. Das gilt sowohl für die Nutzeffekte als auch für die Projektfolgekosten. Diese Betrachtung ist eine Anwendung des Prinzips der ewigen Rente, wie es z.B. bei Unternehmensbewertungen eingesetzt wird, jetzt aber nicht als Projektion der Zukunft auf die Gegenwart, sondern als Projektion der Vergangenheit auf die Gegenwart (Wöhe und Döring 2010, S. 664). Daher müssen in den aktuellen Kosten der IT sämtliche Folgekosten früherer IT-Projekte enthalten sein.
Jetzt kommt eine weitere Annahme des Modells zum Tragen: Wenn die Kosten der betrachteten Projekte einen Anteil X an den Gesamtkosten der IT-Organisation haben, dann hat der von den betrachteten Projekten erzeugte Nutzen ebenfalls einen Anteil X an dem von der IT insgesamt erzeugten Nutzen. Ggf. muss oder will man den Wert X auf der Nutzenseite geeignet anpassen.
So hat man nun für den Wertbeitrag eigentlich alle erforderlichen Daten zusammen:

- einen Schätzwert für den in der Periode erzeugten Nutzen
- die IT-Kosten
- den Wert des IT-Anlagevermögens

Daraus kann man den IT-Wertbeitrag ableiten.
Unter Umständen müssen die vorliegenden Werte noch korrigiert werden:

IT-fremder Aufwand
Wenn in den Projektwerten Projektaufwände und Projektfolgekosten enthalten sind, die nicht in der IT, sondern außerhalb der IT entstehen, dann müssen diese Werte herausgerechnet werden. Dementsprechend müssen auch die Nutzeffekte der Projekte angepasst werden. Hier wird man üblicherweise, wenn keine besonderen Argumente vorliegen, die Nutzeffekte (auf Projektebene) proportional zum Kostenanteil der IT reduzieren.

IT-Anlagevermögen
Das gilt analog für das IT-Anlagevermögen. In der Praxis wird es oftmals so sein, dass Anlagevermögen auf Kostenstellen außerhalb der IT aktiviert wird und zunächst nicht als IT-spezifisch zu erkennen ist. Hier müssen dann die IT-Restbuchwerte geeignet (nach oben) korrigiert werden.

Interne IT-Projekte
In der IT werden in erheblichem Umfang interne Projekte durchgeführt, die die Leistungsfähigkeit der IT oder die

Effizienz der IT steigern sollen. Von diesen Projekten darf nur die Aufwandsseite einbezogen werden, weil sich die Nutzeffekte in der allgemeinen Kostenlage der IT manifestieren.
Solche Abgrenzungen machen die Anwendung dieses Ansatzes schwieriger, sind aber nicht zu umgehen. Das Vorgehen zeigt Tab. 2 exemplarisch.

IT-Kosten (ohne Abschreibungen)	1.200,0	WACC
Abschreibungen	340,0	0,1
Projektaufwand der Periode, gesamt, nicht aktivierbar	75,0	
Projektaufwand der Periode, gesamt, aktivierbar	125,0	CCC
Projektfolgekosten (ausgewähltes Portfolio)	375,0	0,5
Restbuchwert IT-Anlagevermögen (aus Vorperiode)	700,0	
periodenspezifische Nutzeffekte (ausgewähltes Portfolio)	675,0	
Nutzeffekte der Periode (hochgerechnet)	1.800,0	
IT-Kosten (inkl. Abschreibungen)	1.540,0	
Wert IT-Anlagevermögen, gesamt	825,0	
Kapitalkosten auf Anlagevermögen	82,5	
Kapitalkosten auf betriebsnotwendiges Kapital	60,0	
Periodenwertbeitrag der IT	117,5	

Tab. 2: Berechnung des projektbasierten Periodenwertbeitrages der IT (Beispiel)

Residualgewinne von IT-Services

Die bislang diskutierte Methode zur Ermittlung eines IT-Wertbeitrages orientierte sich (über die IT-Projekte) am Nutzen der Projekte im Sinne einer Auswirkung auf den Erlös der Gesamtorganisation. Dabei hat man stets das Problem der Abgrenzung zwischen dem durch IT erzeugten Nutzenvolumen und dem durch andere Kräfte erzeugten Nutzenvolumen. Diese Abgrenzung ist konkret nicht möglich, da es sich um Gemeinnutzen handelt.
Die nun betrachtete Methode geht von der bewerteten IT-Leistung aus, indem sie nämlich annimmt, dass sämtliche Leistungen der IT für die Gesamtorganisation definiert und verrechenbar sind. Es muss also einen vollständigen IT-Servicekatalog geben (Scholderer 2011, S. 7 – 9). Die Bewertung des von der IT erbrachten Servicevolumens in Form von Verrechnungserlösen entspricht dem Erlös auf Unternehmensebene.
Wie bei allen anderen Methoden muss man auch hier Kosten und Kapitalkosten von diesem Leistungswert abziehen. Und die verbleibende Differenz sollte positiv sein.

Ableitung eines servicebasierten IT-Wertbeitrages

Analog zur projektbasierten Methode müssen Leistungswert, Kosten und Kapitalkosten der IT ermittelt werden. Der Nutzen sind die Verrechnungserlöse. Insofern hat man es hier einfacher als bei der projektbasierten Methode. Allerdings darf man nicht die normalen Verrechnungspreise verwenden, sondern muss zur (finanziellen) Bewertung der erbrachten IT-Leistungen die entsprechenden Marktpreise bzw. Marktpreisäquivalente nutzen. Denn würde die Organisation diese Leistungen nicht von der eigenen IT beziehen, müsste sie die benötigten IT-Leistungen am externen Markt kaufen.
Als Argument gegen diese Vorgehensweise wird man ins Feld führen, dass viele Leistungen der IT-Organisation nicht am Markt erhältlich sind und daher auch keine Marktpreise verfügbar seien. Dagegen ist einzuwenden, dass im Falle eines Outsourcings diese Leistungen sehr wohl von einem externen Dienstleister bezogen werden und insofern dann auch ein Preis angegeben werden kann. Außerdem haben viele Unternehmen die Herausforderung schon heute im Rahmen von Verrechnungen zwischen verschiedenen Unternehmen der Unternehmensgruppe, insbesondere dann, wenn sie international tätig sind. Hier müssen dann Transferpreise ermittelt werden und dafür gibt es etablierte und praxiserprobte Ansätze (Abdallah 2004). Es kann also angenommen werden, dass jeder IT-Service mit einem Marktpreisäquivalent bewertet werden kann. Der Wert der IT-Leistung ergibt sich damit aus der Summe der Leistungsmengen, die man mit den Transferpreisen der einzelnen Leistungen gewichtet.
Bei den IT-Kosten kann man wieder auf die üblichen Betriebskosten einschließlich der (bilanziellen) Abschreibungen zurückgreifen. Ein Problem ergibt sich für den Projektaufwand. Wird er aktiviert, dann können die daraus entstehenden Abschreibungen in den Folgeperioden bestimmten Services zugeordnet werden. Wird er nicht aktiviert, dann kann man diesen Aufwand möglicherweise einem bereits definierten Service zuordnen, aber das muss nicht so sein. Dann müssen diese Kosten aber einem zukünftigen Service zugeordnet werden können, für den es in der betrachteten Periode dann eben noch keine Verrechnungserlöse gibt. Schließlich ermittelt man die Kapitalkosten wie gehabt über Restbuchwerte im Anlagevermögen, betriebsnotwendiges Kapital der IT und WACC. Das Vorgehen zeigt exemplarisch Tab. 3.

IT-Kosten (ohne Abschreibungen)	1.200,0	WACC
Abschreibungen	340,0	0,1
Projektaufwand der Periode, gesamt, aktivierbar	125,0	
Restbuchwert IT-Anlagevermögen (aus Vorperiode)	700,0	CCC
		0,5
Verrechnungserlöse zu Transferpreisen	1.700,0	
IT-Kosten (inkl. Abschreibungen)	1.540,0	
Wert IT-Anlagevermögen, gesamt	825,0	
Kapitalkosten auf Anlagevermögen	82,5	
Kapitalkosten auf betriebsnotwendiges Kapital	60,0	
Periodenwertbeitrag der IT	17,5	

Tab. 3: Berechnung des servicebasierten Periodenwertbeitrages der IT (Beispiel)

Eigentlich müsste man den so ermittelten Wertbeitrag noch korrigieren:

Ersparte Transaktionskosten
Dadurch, dass die Organisation einen internen IT-Dienstleister hat, muss sie die benötigtern IT-Leistungen nicht am freien Markt beziehen und erspart sich so Transaktionskosten (Picot et al. 2003, S. 27 – 29). Der ermittelte Wertbeitrag müsste also um diese ersparten Transaktionskosten erhöht werden. Allerdings dürfte es schwierig sein, die Höhe dieser Transaktionskosten abzuschätzen. Man könnte dazu Vergleichswerte nutzen von Organisationen, die keine eigene IT-Organisation (mehr) haben. Diese benötigen eine "retained IT organisation", deren

Kosten man angeben kann. Jedoch ist es fraglich, ob solche Informationen zur Verfügung stehen.

Ersparte Kapitalkosten
Dadurch, dass die Organisation einen internen IT-Dienstleister hat, muss sie die benötigten Leistungen nicht am freien Markt beziehen und erspart sich die Kapitalkosten auf dieses Leistungsvolumen. Entsprechend ist der Wertbeitrag zu erhöhen.

Ersparter Vertriebsaufwand
Die IT-Organisation, die ihre Leistungen innerhalb der eigenen Organisation absetzt, muss keinen oder nur einen geringen Vermarktungs- und Vertriebsaufwand treiben. Die Marktpreise müssen jedoch einen entsprechenden Aufwand beinhalten und insofern muss man den ermittelten Wertbeitrag um diesen ersparten Vertriebs- und Marketingaufwand reduzieren. Auch hier müsste man auf entsprechende Vergleichswerte zurückgreifen können, um diesen Effekt bewerten zu können.

Interner Leistungsbezug
Werden zur Leistungserstellung der IT Leistungen anderer Teilorganisationen bezogen, so müssen diese (intern) bezogenen Leistungen ebenfalls mit Marktpreisäquivalenten bewertet werden, denn wäre ein interner Bezug nicht möglich, müssten man diese Leistungen vom externen Markt zukaufen (Kütz 2012). Allerdings stellt sich die Frage, ob der entsprechende Aufwand durch den Gewinn an Genauigkeit gerechtfertigt werden kann.

Vergleich der Methoden

Beide Methoden, das projektbasierte Vorgehen und das servicebasierte Vorgehen, nutzen den gleichen Berechnungsmechanismus, gehen aber von unterschiedlichen Nutzenbegriffen aus. Die projektbasierte Methode betrachtet den für die Organisation insgesamt durch IT-Einsatz erzielten Wertbeitrag. Die servicebasierte Methode betrachtet nur den originär von der IT erzeugten Wertbeitrag. Ihr Ergebnis muss (eigentlich) niedriger sein als der projektbasierte Wertbeitrag.
Dieser Wertbeitrag ist in Analogie zur Bereitstellungswirtschaftlichkeit ein Bereitstellungswertbeitrag. Der projektbasierte Wertbeitrag enspricht der Gesamtwirtschaftlichkeit der IT, insofern ist die Differenz bei Wertbeiträgen ein Analogon zur Verwendungswirtschaftlichkeit der IT.
Begrifflich hat man also folgende Situation:

- servicebasierter Wertbeitrag ≅ Bereitstellungswertbeitrag
- projektbasierter Wertbeitrag ≅ Gesamtwertbeitrag
- Verwendungswertbeitrag ≅ Gesamtwertbeitrag minus servicebasierter Wertbeitrag

Der servicebasierte Wertbeitrag hat mehrere Vorteile: Die finanzielle Bewertung der IT-Leistungen ist relativ gut objektivierbar. Die bei der projektbasierten Methode auftretenden Abgrenzungsprobleme gibt es hier nicht. Dieser Ansatz hat große Analogien zum EVA auf Unternehmensebene. Die Einbeziehung von Steuereffekten wäre relativ leicht möglich. Der Wertbeitrag kann servicespezifisch ermittelt werden. Es können die bekannten Instrumentarien der Kostenrechnung i.S. der flexiblen Plankostenrechnung genutzt, also Plan-Wertbeitrag, Soll-Wertbeitrag und Ist-Wertbeitrag ermittelt werden.

EINSATZ IN DER PRAXIS

Erfahrungen

Die vorgestellten Ansätze wurden bereits in mehreren Fällen in der Unternehmenspraxis prototypisch erprobt. Die Unternehmen entschieden sich stets für die projektbasierte Methode - trotz der theoretisch schwierigeren Ausgangslage. Das mag daran liegen, dass das Konzept aufgrund der Nähe zur klassischen Barwertberechnung eingängiger ist. Außerdem ist es in vielen Organisationen offenbar so, dass gerade der "Wert" vieler IT-Projekte in Frage gestellt wird, sodass hier wohl ein höherer Rechtfertigungsdruck vorliegt. Zudem bereitet das Denken in Transferpreisen vielen Verantwortlichen offenbar größere Schwierigkeiten als das Denken in Barwerten und Nutzeffekten.
Erfahrung 1: In einem Fall ergab sich zunächst ein negativer Wertbeitrag. Nachdem ein "Jahrhundertprojekt" aus der Berechnung herausgenommen wurde, ergab sich ein positives Ergebnis.
Erfahrung 2: Die Organisation hatte für die vergangenen Jahre eine vollständige Dokumentation aller IT-Projekte mit sämtlichen erforderlichen Daten. Das Berechnungsergebnis war positiv.
Kritisch wurde stets angemerkt, dass das Ergebnis der Projektmethode natürlich durch geschickte Auswahl der einbezogenen Projekte "optimiert" werden könnte. Dieser Einwand lässt sich jedoch stets damit entkräften, dass die Selektion der Projekte transparent ist und die Berechnungen ohne großen Aufwand für modifizierte Projektportfolios wiederholbar sind. Allerdings spricht auch das eigentlich für die Wahl des servicebasierten Ansatzes.

Anwendungsempfehlungen

Der Wertbeitrag von IT ist modellhaft rechenbar und die erforderlichen Methoden sind mit einfachen Werkzeugen wie z.B. Tabellenkalkulation zu unterstützen. Die projektbasierte Methode sollte dann gewählt werden, wenn die Projektinitiierung bereits gut formalisiert ist und entsprechende Dokumentationen vorliegen. Es sollte darauf geachtet werden, dass das zugrundegelegte Projektportfolio "repräsentativ" ist und von allen Beteiligten klar erkannt, nachvollzogen und akzeptiert werden kann.
Die servicebasierte Methode sollte dann gewählt werden, wenn eine IT-Leistungsverechnung vorhanden ist und man auf Mengendaten der Services zurückgreifen kann. Man sollte das Modell eher einfach halten und ohne Korrekturfaktoren einsetzen.
Obgleich der Wertbeitrag eine finanzielle Größe ist, handelt es sich nicht um einen realen Geldbetrag. Insofern sollte mehr Wert auf Plausibilität als auf scheinbare Genauigkeit gelegt werden. Auch mit den vorgestellten Verfahren muss man praktische Erfahrungen sammeln; insofern ist eine längere Erprobung (über mehrere Perioden) anzuraten.

FAZIT

Zusammenfassung und Bewertung

Die hier vorgestellten Verfahren zur Berechnung eines IT-Wertbeitrages gehen vom Residualgewinn der wertorientierten Unternehmensführung aus und übertragen das Konzept auf den IT-Bereich. Für den projektbasierten Ansatz muss der Nutzeffekte von Projekten vollständig finanziell dargestellt werden. Das ist ggf. schwierig, aber grundsätzlich immer möglich.
Für den servicebasierten Ansatz müssen alle IT-Leistungen mit Marktpreisen oder Marktpreisäquivalenten bewertet werden. Das ist ebenfalls schwierig, aber auch möglich.
Die dargestellten Verfahren sind nicht IT-spezifisch, sondern können auf beliebige interne Dienstleister von Unternehmen und Organisationen übertragen werden.

Erweiterungen und Varianten

Hier wurden keine Steuereffekte einbezogen, die Verfahren könnten entsprechend erweitert werden. Es wurde stets nur die aktuelle Periode betrachtet; die Verfahren können auf zukünftige Perioden bzw. auf mehrere Perioden im Verbund angewandt werden.

Offene Fragen

Das Verfahren wurde bislang nur prototypisch eingesetzt. Zu untersuchen wäre ein operativer Einsatz über einen längeren Zeitraum:

- Wie verändert sich das Selbstverständnis der IT?
- Wie verändert sich die Wahrnehmung der IT?
- Kann im Mittel ein positiver Wertbeitrag realisiert werden?
- Falls das nicht der Fall ist, können die Ursachen festgestellt werden?
- Kann der Wertbeitrag im hier vorgestellten Sinne für die strategische Steuerung von IT-Organisationen eingesetzt werden?
- Verbessert oder erleichtert er die strategische Steuerung von IT-Organisationen?

LITERATUR

Abdallah, W. M. 2004. *Critical Concerns in Transfer Pricing and Practice*. Westport (USA) 2004. ISBN 978-1-56720-561-9.

Bearing Point GmbH. 2011. *IT-Wertbeitrag – Messbare Realität oder Illusion?* CIO Snapshot / Studie IT-Wertbeitrag. Frankfurt (Main) 2011.

Fröschle, H.-P. und M. Kütz. *Lexikon IT-Management*. Düsseldorf 2011. ISBN 978-3-939707-72-1.

Götze, U. *Investitionsrechnung*. Heidelberg 2006 (5., überarbeitete Auflage). ISBN 978-3-540-28817-6.

Krause, H.-U. und D. Arora. 2008. *Controlling-Kennzahlen*. München 2008. ISBN 978-3-486-58207-9.

Krcmar, H. 2010. *Informationsmanagement*. Heidelberg 2010 (5., vollständig überarbeitete und erweiterte Auflage). ISBN 978-3-642-04285-0.

Kütz, M. 2012. „Methoden zur Berechnung des IT-Wertbeitrags“. In: Bartsch, Oliver; Lindinger, Markus (Hrsg.): *IT-Servicemanagement*. Köln 2012 (6. Aktualisierung). ISBN 978-3-8249-1492-0.

Laux, H. 2007. *Entscheidungstheorie*. Heidelberg 2007 (7., überarbeitete und erweiterte Auflage). ISBN 978-3-540-71161-2.

Picot, A.; R. Reichwald und R.T. Wigand. 2003. *Die grenzenlose Unternehmung*. Wiesbaden 2003 (5., aktualisierte Auflage). ISBN 978-3-409-52214-4.

Scholderer, R. 2011. *Management von Service-Level-Agreements*. Heidelberg 2011. ISBN 978-3-89864-702-1.

Stiefl, J. und K. von Westerholt. 2008. *Wertorientiertes Management*. München 2008. ISBN 978-3-486-58323-6.

Wöhe, G. und U. Döring. 2010. *Einführung in die Allgemeine Betriebswirtschaftslehre*. München 2010 (24., überarbeitete und aktualisierte Auflage). ISBN 978-3-8006-3795-9

OPTIMIERUNG BESTEHENDER GESCHÄFTSPROZESSE DURCH DEN EINSATZ MOBILER APPLIKATIONEN AM BEISPIEL EINES MITTELSTÄNDISCHEN UNTERNEHMENS MIT DISKRETER FERTIGUNG

Prof. Dr. Frank Morelli
Fakultät Wirtschaft und Recht /
Wirtschaftsinformatik, Studiendekan
Master Information Systems (M.Sc.)
Hochschule Pforzheim
Tiefenbronnerstr. 65
75175 Pforzheim
E-Mail: frank.morelli@hs-pforzheim.de

Mathias Schröder
M.Sc. Information Systems
Technology Consultant /
Master Data Services
SAP Deutschland AG & Co.KG
Hasso-Plattner-Ring 7
69190 Walldorf
E-Mail: mathias.schroeder@sap.com

KEYWORDS
Mobile Applikationen, Geschäftsprozesse, ERP-Systeme, Mittelstand, diskrete Fertigung

ABSTRACT

Mobilität und internetbasierte Kooperation gewinnen zunehmend auch für mittelständische Unternehmen an Bedeutung, um ihre Geschäftsprozesse zu optimieren. Die vorgestellte generische Methodik zeigt auf, wie man zugehörige Lösungsansätze in praxisgerechter Art und Weise identifizieren kann. Als Analysegrundlage für die Anwendungsbeispiele fungieren die SAP Best Practices (BP) im Rahmen der diskreten Fertigung.

Mobilität und App-Einsatz

Im Jahr 2011 wurden in Deutschland 11,8 Millionen Smartphones verkauft. Das entspricht einem Anstieg von 31 Prozent im Vergleich zum Vorjahr (Bitkom 2012) und bedeutet, dass es sich bei fast jedem zweiten neu erworbenem Handy um ein Smartphone handelt. Im Gegensatz zu konventionellen Mobiltelefonen werden Smartphones in der Regel über ein berührungsempfindliches Display gesteuert und unterstützen mobiles Breitband-Internet. Mit einem weltweiten Marktanteil von 19 Prozent im Jahr 2011 ist das iPhone von Apple das am weitesten verbreitete Smartphone (Restivo 2012). Hingegen erweist sich bei den mobilen Betriebssystemen Android von Google, das zum Jahresende 2011 einen Anteil von ca. 50 Prozent verzeichnete, als führend. Im Gegensatz zu iOS dem mobilen Betriebssystem von Apple, das sich ausschließlich auf Apple-Geräten installiert lässt, kann Android von unterschiedlichen Hardware-Herstellern eingesetzt werden.
Zum Erfolg verhalfen diesem Marktsegment, neben technischen Innovationen, insbesondere mobile Applikationen, sogenannte „Apps“. Hierbei handelt es sich um fertige Anwendungen, die im Alltag Verwendung finden sollen. Die erforderliche Infrastruktur zur Bereitstellung ist für den Benutzer nicht transparent: Beim Starten einer App muss er nicht auf (Netz-)Laufwerken zu seinen Dateien navigieren, sondern bekommt diese in personalisierter Form angezeigt. Das Frontend repräsentiert die einzige Schnittstelle, mit der ein Benutzer kommuniziert. Mit Hilfe einer Internetverbindung können Apps über ein herstellerspezifisches Online-Portal bezogen und innerhalb kürzester Zeit installiert werden.
Das Spektrum der möglichen Anwendungen reicht von einfachen Inhalten (aktuelle Nachrichten, Zeitungsartikel etc.) und Datenbanken bis hin zu Programmpaketen mit jeweils umfangreicher Funktionalität. Aktuell werden im Apple Store über eine halbe Millionen Apps angeboten, von denen allein pro Monat über eine Millionen Apps heruntergeladen werden (Grothaus 2011). Die große Anzahl und Vielfalt von Apps ist durch ein weiteres Konzept begründet: Die Betreiber der Online-Portale beteiligen die Entwickler am Gewinn der App. Dies motivierte in der Vergangenheit neben professionellen Softwareentwicklern eine hohe Anzahl von Hobby-Programmierern Apps zu entwickeln. Zwei Entwicklungskonzepte sind dabei besonders populär. Apps die speziell für ein mobiles Betriebssystem entwickelt werden, bezeichnet man als native Apps. Diese Art von Apps wird direkt auf dem Endgerät installiert, ausgeführt und bietet eine optimale Integration der jeweiligen Hardware. Der Einsatz auf einem fremden Betriebssystem erfordert allerdings eine erneute Entwicklung und der Wartungsaufwand nimmt zu. Das zweite Konzept umgeht dieses Problem. Der Einsatz von Web-Technologien wie HTML5, CSS3 und JavaScript ermöglicht die Entwicklung von Web-Apps ohne direkte Abhängigkeit vom jeweiligen Betriebssystem oder Endgerät. Die Ausführung erfolgt mit Hilfe des mobilen Browsers, der Eindruck eine eigenständige App zu starten bleibt erhalten. Entwicklung und Wartung werden hierdurch lediglich an einer App durchgeführt.

Aus betriebswirtschaftlicher Perspektive bietet die Kombination von Apps und Smartphones ein erhebliches Chancenpotenzial, bei gegebener globaler Vernetzung und Mobilität, auf der Grundlage permanenter Konnektivität Informationen unabhängig von Zeit und Ort sofort abzurufen bzw. zu versenden. Hinzu kommen Aspekte der Personalisierung (Anpassung der Nutzerbedürfnisse) und der Kontext-sensitivität (z.B. in Form von Location Based Services). (Bulander 2008, S. 26 ff)

Im B2C Bereich erfreuen sich Apps bereits großer Beliebtheit und für die Betreiber der Online-Portale, insbesondere Apple, erweisen sie sich als umsatz-steigernd. Apps schließen im privaten Umfeld die Lücke zwischen dem Möglichkeitsspektrum des Internets einerseits und einem effizienten Zugriff andererseits. Auch im B2B-Sektor wird das Potenzial des App-Einsatzes zur Effizienzsteigerung diskutiert: In einer aktuellen Studie (Signorino 2011) erhoffen sich 48 Prozent der befragten Unternehmen eine Verbesserung der Kundenbeziehung durch die Einführung mobiler Lösungen. Auf dem zweiten Platz mit 41 Prozent der Stimmen steht die Steigerung der Mitarbeiter-Produktivität. Die Auswahl an aktuell angebotenen Applikationen wird der unternehmensseitigen Nachfrage jedoch nur bedingt gerecht: Insbesondere mangelt es noch an branchenspezifischen Lösungen. Generell bieten viele der derzeit angebotenen Applikation nicht den Nutzen, der eine Investition in teure Endgeräte und die hierfür notwendige IT-Infrastruktur für mittel-ständische Unternehmen rechtfertigen würde. Wissenschaft und Praxis stehen daher gleichermaßen vor der Herausforderung, Bereiche für die Optimierung durch mobile, passgerechte Lösungen zu identifizieren und zu evaluieren. Nur so lässt sich sicherstellen, dass eine mobile Applikation den erwünschten Erfolg auf dem Markt erzielt und dem Unternehmen einen Mehrwert liefert. Der Beitrag stellt anhand zweier Beispiele dar, wie sich mit Hilfe von mobilen Applikationen Geschäftsprozesse systematisch optimieren lassen. Das Beispiel basiert auf den Geschäftsprozessen der SAP Best Practices (BP) die im weiteren Verlauf näher erläutert werden.

Motivation von mittelständischen Unternehmen für den Einsatz mobiler Lösungen

In der jüngeren Vergangenheit litten vor allem kleinere und mittlere Unternehmen (KMU) unter den Folgen der Weltwirtschaftskrise, die 2007 mit dem Zusammenbruch des US-Immobilienmarktes (Subprime-Krise) begann. Im Gegensatz zu großen Unternehmen sind die negativen Auswirkungen solcher Störungen für kleine und mittelständische Unternehmen meist stärker und länger spürbar. Die Gründe hierfür liegen in den vergleichsweise geringeren Rücklagen, dem schlechteren Zugang zu Krediten und den sinkenden Kundenzahlen. Als Reaktion nimmt in Krisenzeiten die Reduktion von Kosten zur Sicherung der Unternehmung oberste Priorität ein. Dies geschieht beispielsweise durch Kurzarbeit oder durch die Aufschiebung von Investitionen in neue Maschinen und/ oder in die IT Infrastruktur. Zwischenzeitlich haben sich die Situation und die Lagebewertung bei den deutschen Unternehmen verbessert. Dies ermöglicht Investitionen, bei der die IT für die Schaffung von Effizienz- und Wettbewerbs-vorteilen zunehmend an Bedeutung gewinnt. Als Motor für diese Entwicklung fungieren mehrere IT-Trends: Hierzu zählen neben den App-basierten Mobility-Lösungen insbesondere der Anstieg des Datenaus-tauschs, die weltweite Vernetzung durch Social-Media sowie die Auslagerung von IT-Infrastruktur in die sogenannte Cloud. Diese Trends repräsentieren den Wunsch einer skalierbaren IT-Landschaft, die es Unternehmen und Mitarbeitern ermöglicht sich effektiver zu vernetzen und beliebige Informationen in Echtzeit unabhängig von Ort und Zeit auszutauschen.

Als charakteristisch für die mittelständische Unternehmenskultur gilt eine hohe Kommunikationsrate, die sich aufgrund der schwächer ausgeprägten Arbeitsteilung gegenüber großen Firmen als kritischer Erfolgsfaktor erweist. Ein weiterer Aspekt im bestehenden Mobilitäts-kontext ist die flexible Handhabung von Geschäfts-prozessen im operativen Management. App-basierte Lösungen haben das Potential, Flexibilitäts-, Kosten- und Zeitvorteile zu steigern und den Bedürfnissen der zukünftigen Arbeitnehmer gerecht zu werden.

Mobility Lösungen im Unternehmensumfeld am Beispiel von SAP Business All in One

Die SAP AG eröffnete Ende 2011 als erstes Unternehmen eine Plattform, ähnlich dem Apple App Store und dem Android Market, die Geschäftskunden Zugang zu mobilen Applikationen ermöglicht. Der SAP Store beinhaltet derzeit 82 Apps (Stand 15. Mai 2012), entwickelt von Partnerunternehmen und der SAP selbst. Der Zugang zum Portal kann sowohl über eine Webseite als auch über eine App („SAP Mobile Apps“) erfolgen. Auf der Bitkom kündigten Hewlett-Packard, Deutsche Telekom, Atos und Fujitsu an, in naher Zukunft ebenfalls eine Plattform dieser Art für Apps und Cloud Applikationen zu eröffnen (Hackmann 2012). Im Vergleich zur hohen Verfügbarkeit von Apps für den privaten Gebrauch mangelt es wie bereits angesprochen noch an Lösungen für den Einsatz in Unternehmen unterschiedlicher Branchen. Hierfür zeichnet insbesondere die Komplexität verantwortlich, die anhand von zwei Aspekten erläutert werden soll:

- Als Ausgangspunkt für eine Mobility Lösung im Unternehmen fungiert typischerweise das vor-handene ERP-System mit seinen betriebswirt-schaftlich orientierten Transaktionen im Sinne eines „Backbones“. Im Mittelstand trifft man hierbei auf eine hohe Bandbreite an verfügbaren Alternativen (vgl. Sontow 2011).

- Die Anforderungen im B2B-Sektor sind vielfältiger und höher als im B2C-Bereich. Es gilt in diesem Kontext sowohl unterschiedliche Geschäftsprozesse und IT-Systeme zu berücksichtigen als auch hohe Sicherheitsanforderungen zu erfüllen.

App-Entwickler und Unternehmen müssen demnach beiderseits bestrebt sein, die für den jeweiligen Einsatzweck optimale Lösung zu identifizieren. Die innovativen Bestrebungen der SAP rechtfertigen es aus Sicht der Autoren, auf der Basis vorhandener Lösungen dieses Softwareherstellers ein Konzept zur Identifizierung mobiler Lösungskonzepte im B2B-Bereich zu erarbeiten. Im Folgenden wird aufgrund zugehöriger Einsatzerfahrungen der SAP und des bestehenden BP Konzepts die ERP Lösung Business All in One als Grundlage für das Anwendungsbeispiel herangezogen. Die konzeptionelle Ausgestaltung lässt sich auf andere ERP-Softwarehersteller übertragen.

SAP Business All in One repräsentiert neben SAP Business One und Buiness ByDesign eine Lösungsoption für KMU. Im direkten Vergleich zu den beiden anderen ERP-Produkten handelt es sich bei SAP Business All in One um das umfassendste Lösungsangebot, das auf dem klassischen SAP ERP System und der SAP Netweaver Technologie basiert: Um die Implementierung zu beschleunigen und die Total Cost of Implementation (TCI) zu senken hat die SAP in Zusammenarbeit mit Partnern und Kunden sogenannte „Best Practices“ entwickelt. Bei SAP All in One ermöglichen diese BP den Einsatz vorgefertigter Standard-Geschäftsprozesse, anstatt diese unternehmensindividuell in einem SAP ERP System einstellen zu müssen. Der Customizing-Aufwand wird hierdurch erheblich reduziert.

BP existieren sowohl in branchenspezifischen Ausprägungen (wie beispielsweise Automotive, Banking oder High-Tech) als auch in Form von branchenübergreifenden Paketen wie Business Intelligence (BI), Customer Relationship Management (CRM), Supply Chain Management (SCM) oder Product Lifecycle Management (PLM). Sie enthalten grundsätzlich drei Komponenten (strukturiertes Einführungsverfahren, Dokumentation mit Konfigurationsleitfaden sowie vorkonfigurierte Inhalte), um zentrale Geschäftsprozesse "schlüsselfertig" lauffähig zu machen.

Die Dokumentation zweier Kernprozesse für die diskrete Fertigung dient im Rahmen dieses Artikels als Ausgangspunkt für die Identifizierung neuer mobiler Lösungskonzepte. In den nachfolgenden Kapiteln wird die eigens in Kooperation mit dem Softwarehersteller entwickelte Vorgehensweise anhand zweier Beispiele erläutert.

Identifizierung und Einbindung mobiler Lösungskonzepte anhand von SAP Best Practices (BP) der diskreten Fertigung

Für die Veranschaulichung der Methodik werden Beispiele der SAP BPs aus der diskreten Fertigung als Grundlage verwendet. Diese bestehen aus 103 Szenarien in den Bereichen Materialwirtschaft, Produktionsplanung und –steuerung, Vertrieb, Logistik, Qualitätsmanagement sowie Rechnungswesen und Controlling (Stand: V1.605). Im Rahmen der Dokumentation werden die einzelnen Prozesse innerhalb der Szenarien mit Hilfe von Schwimmbahn-Diagrammen visuell dargestellt. Diese Diagramme geben Aufschluss über die Beteiligten (Rollen), Tätigkeiten und Abläufe.

Unternehmen der diskreten Fertigung zeichnen sich dadurch aus, dass ihre Produkte als abzählbare Einheiten hergestellt werden und damit im Kontrast zur Prozessfertigung stehen. Hierzu zählt u.a. die Produktion von Automobilkomponenten. Unternehmen innerhalb dieser Branche agieren in einem globalen, kostenorientierten Markt und stehen vor der Herausforderung, bei den sich weiter verkürzenden Produktlebenszyklen, Kundenbindung durch hohe Qualität und exzellentem Service langfristig zu forcieren. Diese Umgebung erfordert einen kontinuierlichen Verbesserungsprozess. Die wesentlichen Herausforderungen und Treiber für zugehörige Aktivitäten liegen in der kontinuierlichen Optimierung der Prozesseffizienz sowie in der Unterstützung unternehmensinterner, standortübergreifender Zusammenarbeit sowie der Zusammenarbeit mit externen Partnern und Zulieferern. Einer Verkürzung der „Time-to-Market“ kommt dabei eine zentrale Bedeutung zu. Hier sehen die Autoren entsprechendes Potential für den Einsatz mobiler Lösungen im Mittelstand.

Die Identifizierung neuer mobiler Lösungen anhand der BP-Prozesse vollzieht sich in drei Schritten: Zunächst erfolgt eine Zuordnung der Rollen aus den BPs zu einem generischen Rollenmodell eines mittelständischen Betriebes. Als Ergebnis fungiert ein vereinfachtes Rollenmodell, aus dem man ersehen kann, welche Rollen in welchen Szenarien involviert sind. Im Anschluss werden die Szenarien detailliert untersucht und fünf Mobility-relevante Sachverhalte (vgl. Abb. 1) bestimmt, die man aus den Szenarien heraus einer Rolle zuordnen kann.

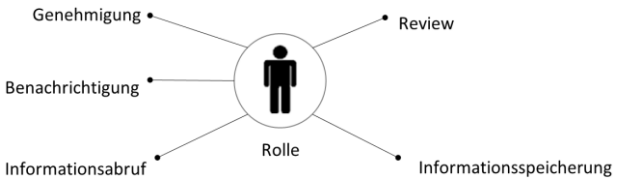


Abbildung 1: Rollenmodell für die Analyse der SAP Best Practices

Die entsprechenden Aufgabenstellungen, Informationen bzw. Aktivitäten lassen sich wie folgt kategorisieren:

- *Genehmigung*: Genehmigungsaktivitäten verwendet man, wenn die Zustimmung einer Führungskraft oder eines Vorgesetzten zur Fortführung des Geschäftsprozesses bzw. zum Anlegen bestimmter

Belege (z. B. Bestellungen) im IT-System erforderlich ist. Genehmigungen lassen sich aufgrund der geringen Komplexität verhältnismäßig leicht auf Apps übertragen. Das zeitliche Verbesserungspotenzial erweist sich als hoch, da eine Genehmigung meist den Prozessverlauf so lange blockiert, bis sie von der verantwortlichen Person oder dessen Stellvertreter erteilt wurde.

- *Benachrichtigung*: Eine Benachrichtigung informiert eine Person über einen definierten Status bzw. ein Ereignis (z.B. „Bestellung eingegangen", „Wareneingang erfolgt"). In zeitkritischen Prozessen mit mehreren Beteiligten lassen sich Benachrichtigungen einsetzen, um die erforderlichen Tätigkeiten zu beschleunigen, da die jeweils verantwortliche Person schneller informiert wird. Auch kritische Situationen wie beispielsweise der Ausfall einer Maschine oder ein Qualitätsproblem kann man mit Hilfe von Benachrichtigungen schneller beheben. Das automatische Senden von Nachrichten auf ein mobiles Endgerät erfordert in diesem Zusammenhang Push-Funktionalität im Backend-System.
- *Informationsabruf*: In der Kategorie Informationsabruf werden Prozessschritte gesammelt in denen eine Person Information aus dem ERP System abruft (z.B. Liefertermin, Status, …).
- *Review*: Bei einem Review handelt es sich um einen Vorgang, bei dem Informationen in gebündelter Form zur Begutachtung übermittelt werden. Eine nachfolgende Handlung ist nicht zwingend erforderlich.
- *Informationsspeicherung*: Alle Vorgänge, bei denen Belege im ERP System aktiv vom menschlichen Bearbeiter abgespeichert werden, gehören in die Kategorie Informationsspeicherung.

Nach der initialen Analyse der Rollen und der Zuordnung Mobility-relevanter Sachverhalte erfolgt als zweiter Schritt die Optimierung der Geschäftsprozesse auf Grundlage der SAP BPs. Innerhalb dieses Artikels werden im weiteren Verlauf zur Illustration ein Verkaufsprozess und ein Einkaufprozess herangezogen. Für die Darstellung der BPs verwendet die SAP eine Swimlane-Diagrammtechnik. Das jeweilige Modell enthält Informationen über die beteiligten Rollen, Tätigkeiten, Ereignisse und Dokumente.

Die ganzheitliche Abbildung von mobilen Realisierungspotenzialen innerhalb der Beispiele erfolgt mit Hilfe der Modellierungssprache Business Process Model and Notation (BPMN), da sich diese zunehmend in Wissenschaft und Praxis etabliert: BPMN stellt Symbole zur Verfügung, mit denen Experten aus den Fachbereichen und IT-Spezialisten Geschäftsprozesse abbilden können. Als Modellierungssprache basiert sie darüber hinaus auf syntaktischen und semantischen Regeln (Metamodellen) zur Verknüpfung der Symbole. Diese Formalisierung, die innerhalb der menschlichen Sprache einer Grammatik entspricht, ermöglicht im Idealfall die automatisierte Transformation der Prozessmodelle in ablauffähige Workflows.

Beispiel Verkaufsprozess

Der Geschäftsprozess „Kundenauftragsabwicklung - Verkauf ab Lager" ist in seiner ursprünglichen Fassung aus Abbildung 2 ersichtlich. Er umfasst sämtliche Schritte vom Anlegen eines Auftrags bis hin zum Ausgleichen eines Kundenkontos nach Eingang der Zahlung.

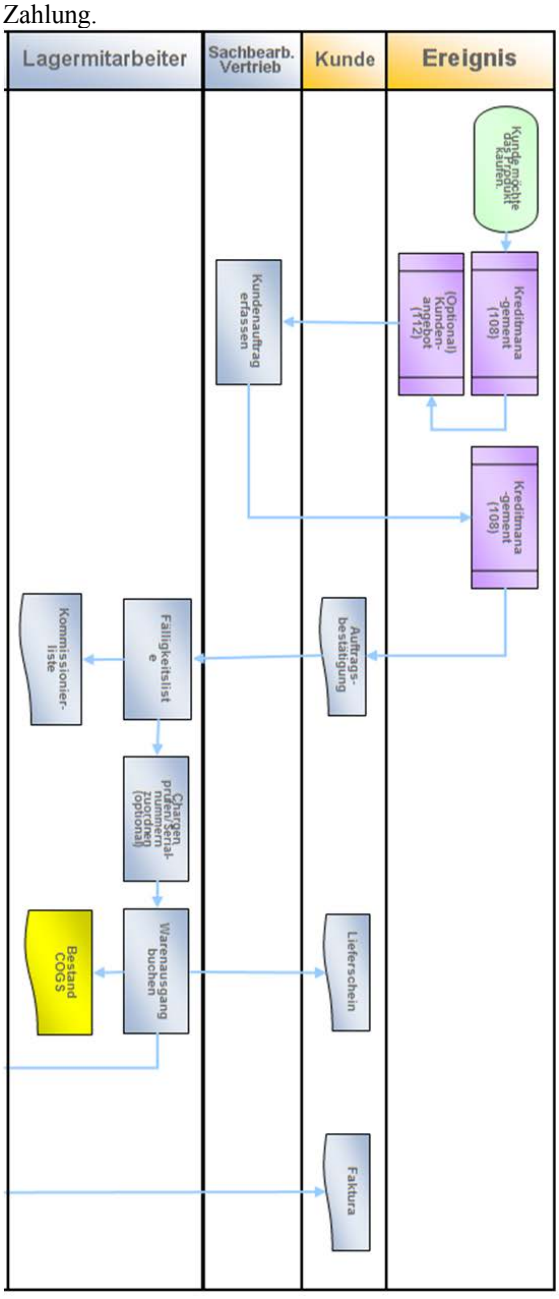


Abbildung 2: SAP Best Practice Kundenauftragsabwicklung – Verkauf ab Lager [SAP 2012a]

Der Ausgangsprozess beginnt mit dem Anlegen eines Standardkundenauftrags. Je nach Kunde und Material werden während der Auftragserfassung verschiedene spezifische Schritte durchgeführt, wie z. B. die Preis-

findung für den Kunden und/oder das Material, das Gewähren anwendbarer Rabatte, die Überprüfung der Materialverfügbarkeit sowie die Überprüfung der Kredithistorie des Kunden. Im Anschluss an die Kommissionierung erfolgt die Erfassung die gelieferte Materialmenge im ERP System. Nach Abschluss der Kommissionierung muss der Lagermitarbeiter den Bestand systematisch ausbuchen. Diese Bestandsausbuchung stellt die eigentliche Erfassung der an den Kunden gelieferten physischen Menge dar. Sobald dies erfolgt ist, lässt sich die Lieferung fakturieren und der Erlös wird zusammen mit den Umsatzkosten im Rechnungswesen erfasst. Mit diesem Schritt endet das Beispiel für den Verkaufsprozess.

Der ausgewählte Geschäftsvorfall besitzt aus Sicht der Autoren ein hohes Potential für die Optimierung mit Hilfe von mobilen Lösungen. Wie in (Ellwood 2008) publiziert verbringen Vertriebsmitarbeiter durchschnittlich 13 Prozent ihrer Zeit mit Reisetätigkeiten und nur 22 Prozent mit Verkaufsaktivitäten. Weitere 12 Prozent fallen für die Verarbeitung von Bestellungen und 23 Prozent für administrative Aufgaben an. Entsprechende Optimierungsüberlegungen stützen sich auf folgende Aspekte:

- Während der Reise verfügen die Vertriebsmitarbeiter nur über eingeschränkten Zugriff auf ein Notebook oder einen PC. Durch die Ausführung von Geschäftsprozessaktivitäten auf mobilen Endgeräten ist eine Steigerung der Produktivität währenddessen möglich.
- Die Funktionalität von CRM-Systemen ermöglicht es den Vertriebsmitarbeitern einen größeren Kundenkreis zu betreuen. Gleichzeitig ist der Aufwand an administrativen Tätigkeiten stark gestiegen. Auch hier haben mobile Lösungen das Potential den Aufwand für Tätigkeiten wie beispielsweise die Absatzplanung oder die Kampagnenplanung zu minimieren. Der Mitarbeiter profitiert hierbei vor allem von der Möglichkeit Information direkt am Ort des Geschehens auf sein Smartphone und Daten aktiv in das ERP-System zu übertragen. Mehraufwände und Fehler können dadurch reduziert werden.
- Darüber hinaus ermöglicht der Zugriff auf Informationen aus dem ERP-System eine Verbesserung der Antwortzeit gegenüber dem Kunden. Ferner kann ein Vertriebsmitarbeiter über kritische Vorfälle schneller informiert und hierdurch zeitnah (Gegen-)Maßnahmen eingeleitet werden.

Für das neue Lösungskonzept (siehe Abbildung 3) werden drei Elemente der Rolle Vertriebsmitarbeiter kombiniert: Informationsspeicherung (Kundenauftrag erstellen), Informationsabruf (Kundenreport, Kundenauftragsstatus /-sperre prüfen, Kreditlimitprüfung durchführen) und Benachrichtigung (Auftragserteilung, ATP-Prüfungsergebnis.

Der Vertriebsmitarbeiter wird nach Auftragseingang per App über eine Nachricht informiert. Er hat nun frühzeitig die Möglichkeit die Bearbeitung der Anfrage zu planen oder direkt auf seinem mobilen Endgerät auszuführen. Die dafür notwendigen Informationen sind im ERP System abgelegt und lassen sich im Sinne einer Pull-Funktion über die App abrufen bzw. analog zur Meldung des Auftrageingangs als Push-Funktionalität aktiv IT-seitig bereitstellen.

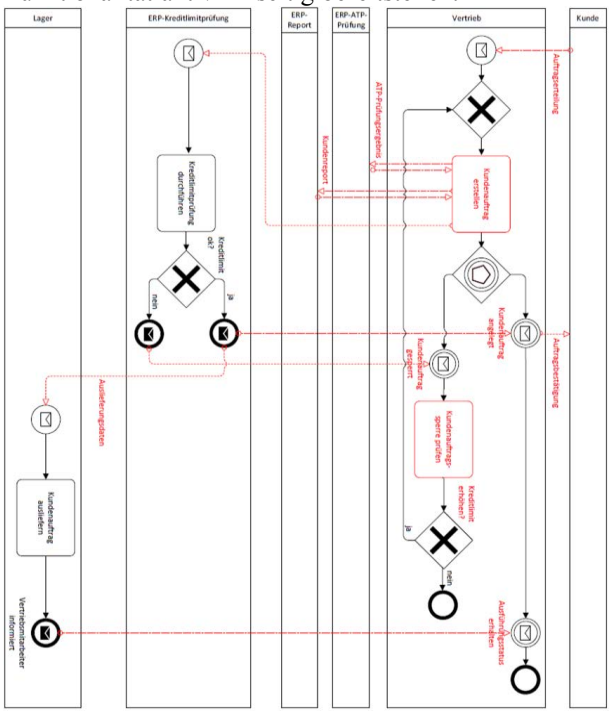


Abbildung 3: Lösungskonzept für die Auftragsbearbeitung aus Sicht des Vertriebsmitarbeiters

Beispiel Einkaufsprozess

Im Rahmen dieses Geschäftsprozesses (vgl. Abbildung 4) werden Bestellanforderungen entweder über die Materialbedarfsplanung (MRP) oder manuell von einem Anforderer im Unternehmen generiert. Alternativ kann eine Bestellung auch manuell vom Einkäufer angelegt werden. Ein Sachbearbeiter im Einkauf prüft die Bestellanforderung auf Fehler und setzt sie zu gegebener Zeit in eine Bestellung um.

Bevor die Bestellung an einen Lieferanten versendet wird, muss sie in Abhängigkeit von der Höhe des Betrags ggf. der Leiter des Einkaufs genehmigen. Nach erfolgtem Ausdruck wird die Bestellung an den Lieferanten versendet. Der hiernach erfolgende Wareneingang mit Bezug auf die Bestellung ist nicht mehr Gegenstand der weiteren Betrachtung.

Ein Sachbearbeiter im Einkauf verfügt z.B. aufgrund von Besprechungen oder Meetings nicht zwangsweise über permanenten Zugriff auf ein Notebook oder einen PC. Dies gilt in noch verstärktem Maße für den Einkaufsleiter im Unternehmen, der weiterhin für Genehmigungsprozesse nur eingeschränkt Zeit aufbringen kann. Entsprechend besitzt auch dieses Prozessbeispiel aus Sicht der Autoren Optimie-

rungspotenzial durch den Einsatz mobilen Lösungen.

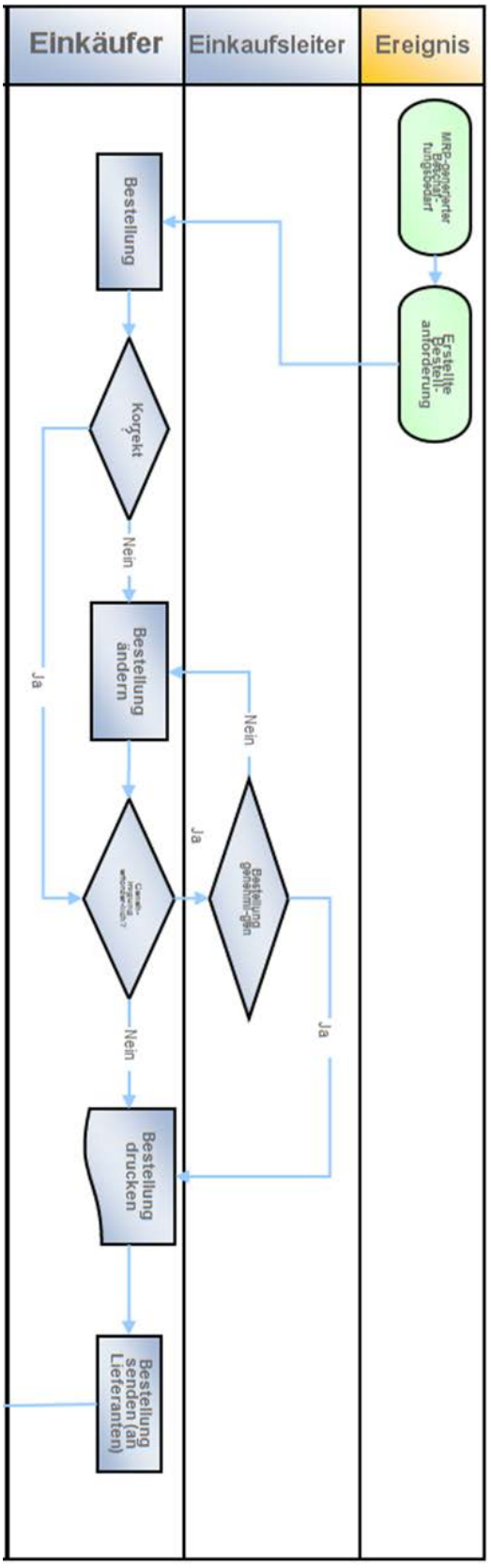


Abbildung 4: SAP Best Practice Beschaffung von Materialien [SAP 2012b]

Für das neu gestaltete Konzept (vgl. Abbildung 5) werden für den Sachbearbeiter im Einkauf folgende Mobility-relevante Sachverhalte identifiziert: Informationsspeicherung (BANF in Bestellung umwandeln, Bestellung ändern, Bestellung versenden), Review (Bewilligungsantrag) und Benachrichtigung (manuell erzeugte BANF von einem Antragsteller aus einer Fachabteilung, maschinell erzeugte BANF über die Materialbedarfsplanung sowie genehmigte bzw. abgelehnte Bestellung durch den Einkaufsleiter). Der Leiter des Einkaufs wird seinerseits per App vom Sachbearbeiter über die zu genehmigende Bestellung benachrichtigt (Push-Funktion). Nach Durchführung des Arbeitsschrittes erfolgt die Unterrichtung (im Sinne einer Benachrichtigung) des Sachbearbeiters wiederum automatisch per App über das Ergebnis des Genehmigungsvorgangs.

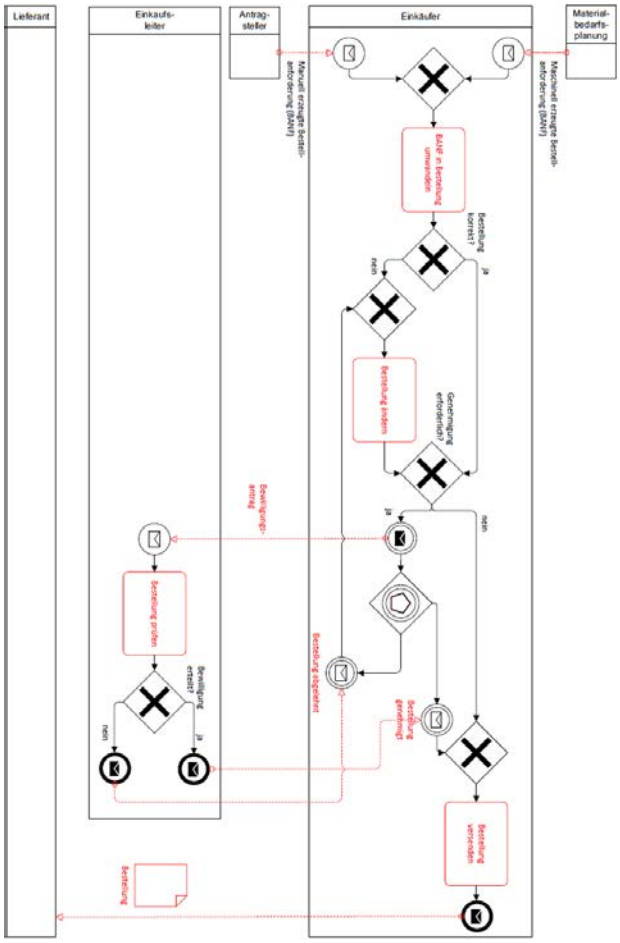


Abbildung 5: Lösungskonzept für die Beschaffung von Materialien aus Sicht des Einkäufers

Fazit

Die Bedeutung von neuen IT-Technologien, die sich mit Mobilität und der internetbasierten Zusammenarbeit beschäftigen, nimmt mehr und mehr zu. Für mittelständische Unternehmen mit begrenztem IT-

Budget ist die Auswahl der richtigen Technologie von großer Bedeutung.

Mobile Lösungen bieten ein vielfältiges Möglichkeitsspektrum, um Ziele im Unternehmen positiv zu beeinflussen: Entsprechende Optimierungspotenziale bestehen von der internen Beschleunigung von Geschäftsprozessen durch die Mobilisierung von Genehmigungsabläufen bis hin zur Verbesserung des Kundenservices mit Hilfe von multifunktionalen Apps für Vertriebsmitarbeiter. Aufgrund der Komplexität von vorhanden System(infrastruktur)en, Geschäftsprozessen und Technologien sind eine systematische Vorgehensweise sowie der Einsatz von adäquaten Werkzeugen unerlässlich. Dies unterscheidet Entwicklungen im Unternehmensumfeld von denen im privaten Bereich und repräsentiert einen wichtigen Grund für die jeweils stark unterschiedlichen Entwicklungen im Hinblick auf die App-Portal-Nutzung.

Die vorgestellte generische Methodik wurde mit dem Ziel entwickelt, auf Grundlagen bestehender Geschäftsprozesse mobile Lösungsansätze zu identifizieren und deren Ausgestaltung visuell darzustellen. Zur Illustration der Vorgehensweise wurde auf die SAP BP als Analysegrundlage zurückgegriffen. Diese basieren auf langjährigen Erfahrungen der SAP und beteiligter Kunden und repräsentieren einen empfohlenen Implementierungsansatz. Aus Sicht der Autoren zeigen die beiden ausgewählten Beispiele, dass es möglich ist, auf der Basis von Geschäftsprozessdokumentationen zugehörige Optimierungspotenziale zu identifizieren und konzeptionelle Lösungen auszugestalten. Die Verwendung der standardisierten Geschäftsmodellierungssprache BPMN vereinfacht einen globalen Austausch über entsprechende Sachverhalte. Die Ergebnisse sollten im praktischen Einsatz als Ausgangspunkt für den Dialog mit relevanten Stakeholdern (z.B. betroffenen Mitarbeitern, Kunden und Nutzern) dienen, um einen nachhaltigen Wertbeitrag im Unternehmen zu liefern.

LITERATUR

Bulander, R. 2008: Customer-Relationship-Management-Systeme unter Nutzung mobiler Endgeräte, Dissertation, Universitätsverlag Karlsruhe, Karlsruhe

Bitkom. 2012: Presseinformation: Smartphone Umsatz steigt rasant, http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Smartphone-Absatz_09_01_2012.pdf. Abruf am 10.04.2012

Grothaus, M. 2011: More than 18 billion apps downloaded from App Store, http://www.tuaw.com/2011/10/04/more-than-18-billion-apps-downloaded-from-app-store/. Abruf am 06.04.2012

Hackmann, J. 2012: B2B-App-Stores krempeln den Markt um, www.computerwoche.de/management/cloud-computing/2506188/. Abruf am 15.04.2012

Ellwood, M. 2008: How Sales Reps Spend Their Time, www.paceproductivity.com/files/How_Sales_Reps_Spend_Their_Time.pdf Abruf am 03.05.2012

Restivo, K. 2012: Mobile Phone Tracker February 6 2012, IDC Corporate USA, S. 2

SAP AG. 2012a: Best Practices Discrete Manufacturing, SAP AG, Walldorf, http://help.sap.com/saap/sap_bp/BB Library/Documentation/109_ERP606_Process_Overview_DE_XX.ppt Abruf am 08.06.2012

SAP AG. 2012b: Best Practices Discrete Manufacturing, SAP AG Walldorf, http://help.sap.com/saap/sap_bp/BBLibrary/Documentation/130_ERP606_Process_Overview_DE_XX.ppt Abruf am 02.05.2012

Sontow, K. 2011: ERP Praxis im Mittelstand, Trovarit AG Aachen, S. 4

Signorino, E. 2011: 2011 US Enterprise Mobility: IT Decision-Maker Survey, Yankee Group

AUTORENBIOGRAFIEN

Prof. Dr. **FRANK MORELLI** wirkt als Professor an der Hochschule Pforzheim im Bereich Betriebswirtschaft/Wirtschaftsinformatik – Management & IT und als Studiendekan des Masterstudiengangs Information Systems (MIS).

MATHIAS SCHRÖDER ist Absolvent des Masterstudiengangs MIS an der Hochschule Pforzheim und Technology Consultant Master Data Services der SAP Deutschland AG & Co. KG.

MAINPROJECT – ITIL-WISSENSTRANSFER IM RAHMEN DES ESF-PROGRAMMS

Meike Schumacher, Michael Tax, Georg Rainer Hofmann, Wolfgang Alm
Information Management Institut
Hochschule Aschaffenburg
Information Management Institut
Würzburger Str. 45
63743 Aschaffenburg

KEYWORDS
Akzeptanz, ITIL, IT-Management, IT-Service Management, Lebenslanges Lernen, Mittelstand, Prozessmanagement, Wissenstransfer

ABSTRACT

Im Oktober 2011 startete mit einer Laufzeit von drei Jahren ein Projekt des Europäischen Sozialfonds (ESF) mit der Bezeichnung „mainproject“. Das Projekt ist „nah an der Praxis“ am externen Hochschulstandort Zentrum für Wissenschaftliche Services im Industrie Center Obernburg lokalisiert.

Gegenstand von mainproject ist eine Netzwerktätigkeit zwischen dem Information Management Institut der Hochschule Aschaffenburg und den regionalen Unternehmen am bayerischen Untermain. Die dort beschäftigten Personen werden zur besseren Ausrichtung auf das sich wandelnde ökonomische Umfeld weiter entwickelt – speziell im Bereich innovativer, neuerer Formen der Prozessoptimierung und des Dienstleistungsmanagements.

Das Projekt mainproject ist bereits das zweite ESF-Projekt des Information Management Instituts. Die Erkenntnisse des ersten ESF-Projektes „KontAkS“ (Kontext und Akzeptanz von Systemen) fließen maßgeblich in die Arbeit von mainproject mit ein: Eine Prozessverbesserung im Unternehmen ist zwingend auf die Akzeptanz der beteiligten Akteure angewiesen. Akzeptanzhemmnisse, die es auf jeder Unternehmensebene oder auf Kundenseite geben kann, gilt es frühzeitig zu identifizieren und im Verbesserungsprozess zu berücksichtigen. Hierzu müssen geeignete akzeptanzfördernde Maßnahmen entwickelt und eingesetzt werden.

WISSENSTRANSFER IM RAHMEN VON MAINPROJECT

Das an der Hochschule Aschaffenburg (HAB) durchgeführte Projekt mainproject ist eine vom Bayerischen Staatsministerium geförderte und vom ESF sowie der Mainsite Services GmbH & Co. KG kofinanzierte Maßnahme zur Nutzung des Innovationspotenzials und des damit verbundenen Wissenstransfers zwischen der Hochschule Aschaffenburg (HAB) und den Unternehmen am Bayerischen Untermain. Verantwortlich für die Projektdurchführung ist das Anfang 2011 gegründete Information Management Institut (IMI) der HAB. Das Projekt läuft von Oktober 2011 bis September 2014 und umfasst einen Projektetat von 815.500 € (Fördersumme 407.750 €). Die Qualitätssicherung wird vom Fraunhofer-Institut für Offene Kommunikationssysteme in Berlin durchgeführt.

Entsprechend seiner Vorgaben ist der Projektstandort im Industrie Center Obernburg (ICO), innerhalb des von der HAB gegründeten Zentrums für Wissenschaftliche Services (ZeWiS), praxisnah aufgestellt. Das ICO ist ein Industriepark mit rund dreißig kleinen und mittleren Unternehmen (KMU) und dient, neben einigen weiteren KMU außerhalb des Standorts, als Ausgangslage für die Tätigkeit von mainproject. Standortbetreiber ist die Mainsite Services GmbH & Co. KG, die umfassende Serviceleistungen für die Unternehmen am Standort ICO, inklusive des Betriebs eines zentralen Rechenzentrums und IT-Dienstleistungen, für die auf dem Gelände lokalisierten Unternehmen erbringt.

Ziel von mainproject ist es, die Attraktivität des Bayerischen Untermains als Ansiedlungsregion – und damit die der dort ansässigen Unternehmen – durch gut geschultes und innovationsorientiertes Personal zu steigern. Um dieses Ziel zu erreichen soll Methodenwissen aus den Bereichen IT-Management, Dienstleistungsmanagement und Lean Management an die Unternehmen vermittelt und eingebracht werden. Die Mitarbeiter werden so durch praxisrelevante Kompetenzen und Fähigkeiten besser für das sich im permanenten Wandel befindende ökonomische Umfeld qualifiziert. Unterstützt wird dies zusätzlich durch den Netzwerkcharakter von mainproject. Das Projekt bietet im Rahmen der Hochschule eine neutrale Plattform für den Wissens- und Erfahrungsaustausch und fördert nicht nur den akademischen Diskurs zwischen der HAB und den Unternehmen, sondern auch den Austausch von Unternehmen untereinander. In der Praxis wird dies u.a. durch das Angebot von Fachgesprächen und Themennetzwerken realisiert. Ergänzend werden außerdem überregionale Kooperationspartner in Form von Universitäten, Instituten und Unternehmen eingebunden, um das Innovationspotenzial weiterer Standorte zu

nutzen. Das mainproject-Referenzmodell gibt einen Überblick über die Aktionsfelder des Projekts und ist aufgeteilt in die Hauptsäulen, Kompetenzschwerpunkte und Querschnittsthemen.

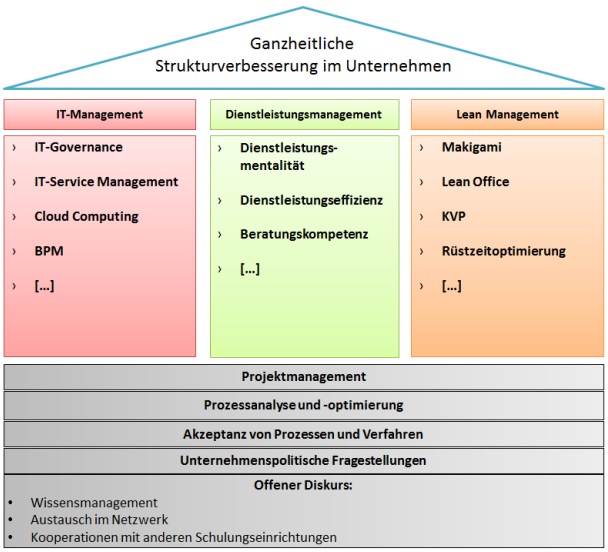


Abbildung 1: Das Referenzmodell setzt die Handlungsfelder von mainproject mit den Kompetenzschwerpunkten und Querschnittsthemen in Verbindung. Für die folgenden Ausarbeitungen liegt der Fokus auf dem IT-Service Management.

AKZEPTANZ VON IT-SERVICE MANAGEMENT IN BETRIEBEN AM BAYERISCHEN UNTERMAIN

Ausgangslage und Problemstellung

Herausforderungen in der IT – Die Bedeutung des IT-Managements und des IT-Service Managements für die betriebliche Organisation

Ausgehend vom Begriff Informationsmanagement kann IT-Management als Planung, Steuerung und Kontrolle von Informationssystemen und Informations- und Kommunikationstechnik als Teilaufgabe der Unternehmensführung verstanden werden (Krcmar 2005). IT-Management enthält dabei sowohl strategische Komponenten – als langfristige Sicht auf die Nutzung vorhandener und die Entwicklung zukünftiger Erfolgspotenziale – als auch operative Komponenten für das kurz- und mittelfristige unternehmerische Handeln. Dies beinhaltet u.a. auch die Entwicklung von IT-Lösungen und das Sicherstellen des IT-Betriebs (Tiemeyer 2009a). Die IT nimmt, als Summe der technischen und organisatorischen Mittel zur Unterstützung der Geschäfts- und Informationsprozesse (Tiemeyer 2009a), eine immer größere Bedeutung bei der Geschäftstätigkeit eines Unternehmens ein. Das Beherrschen von IT-Themen ist eine Voraussetzung für die effiziente Abwicklung von Geschäftsprozessen mit positiven Auswirkungen auf den geschäftlichen Erfolg eines Unternehmens. Der Einsatz von IT ist zudem meist so tief in der unternehmerischen Struktur verankert, dass ein fortlaufender Geschäftsbetrieb ohne diese nicht mehr möglich wäre und somit unabdingbar wird (Tiemeyer 2009a). Vielmehr kann die IT, wie in (Tiemeyer 2009a) und (Fröhlich et. al. 2007) beschrieben, durch effiziente Steuerung als Werttreiber eingesetzt werden und damit als Wettbewerbsvorteil dienen. (Fröhlich et. al. 2007) argumentieren, dass die Informationstechnologie als Kernaufgabe der Unternehmensführung, zu den entscheidenden Schlüsselfaktoren für den Unternehmenserfolg (i. S. v. kritischer Erfolgsfaktor) gehört. Die Verantwortlichen der IT-Organisation stehen dabei u.a. den in Tabelle 1 dargestellten Phänomenen und Herausforderungen der IT-Welt gegenüber.

Tabelle 1: Die Tabelle zeigt einige Phänomene und daraus resultierende Herausforderungen für IT-Verantwortliche (Tiemeyer 2009a). Da die IT ein sich schnell wandelndes und innovationsgetriebenes Feld ist, kann davon ausgegangen werden, dass zukünftig deutlich mehr strategische und operative Problemfelder entstehen werden. Um diesen begegnen zu können, können Änderungen in der Unternehmenskultur und ein Mentalitätswandel der beteiligten Personen notwendig werden. Daher muss als Basis im Unternehmen ein strukturiertes und zuverlässig durchgeführtes IT-Management vorhanden sein.

Phänomene der IT-Welt	Herausforderungen
Hohe Anforderungen an die IT-Abteilung durch Fachabteilungen und Unternehmensführung	IT-Strategie optimieren und Kundenorientierung der IT forcieren
Historisch gewachsene IT-Landschaften; steigende Komplexität der Technologien	Zielorientiertes Planen und Managen von IT-Architektur (u.a. IT-Infrastrukturen, IT-Applikationen, IT-Prozesse)
Steigende Nutzerzahlen, die IT-Support benötigen	Unterstützung für Endbenutzer verbessern (z.B. automatisierter Support, optimierte Benutzerverwaltung) und umfassendes Management von IT-Services
Modularisierung von Software und Standards, umfangreiches Angebot an Standardsoftware (SSW)	Koordination der Einführung von Software-Applikationen, Notwendigkeit der Integration von Standard-Lösungen forcieren
Sinkende oder gleichbleibende IT-Budgets	IT-Budgetierung und interne Kosten- und Leistungsverrechnung einführen; Einführung von Kennzahlen und Benchmarking
Zunehmende Anzahl kritischer IT-Anwendungen	Umfassende IT-Serviceleistungen anbieten und IT-Security-Lösungen entwickeln
Hohe Arbeitskräftefluktuation	Personalmanagement in der IT ausbauen
Zahlreiche Einflussfaktoren und Vorgaben von Rahmenbedingungen (z.B. Gesetze, Verordnungen)	Risikomanagement in der IT und IT-Compliance sicherstellen

Dabei befindet sich die IT-Organisation eines Unternehmens häufig in einem Spannungsfeld zwischen unternehmensinternen Forderungen und dem Marktdruck von außen (z.B. durch externe IT-Dienstleister). Verantwortlich für diese Spannungen sind laut (Schott 2006) vor allem die folgenden Faktoren:

- Die schwierige Wettbewerbssituation der Unternehmen, welche einen hohen Kostendruck erzeugt.
- Die hohe Innovationsgeschwindigkeit der Informations- und Kommunikationstechnologie (IKT), die durch einen hohen Kapitalbedarf geprägt ist und fehlende Expertise auf Seiten der Anwender zur Folge hat.
- Die negative Einstellung gegenüber der IT innerhalb des Unternehmens aufgrund von Qualitätsmängeln, unverhältnismäßigen Kostensteigerungen und insbesondere die fehlende Servicementalität der IT-Abteilungen.
- Mangelndes Verantwortungsbewusstsein für interne IT-Dienstleister seitens des Chief Information Officers (CIO).
- Steigende Komplexität im Rahmen unterschiedlicher Organisationsformen, beispielsweise durch Ausgliederung, Joint Ventures und Outsourcing.

Diese Faktoren erzeugen einen zunehmenden Rollenkonflikt der IT zwischen strategischen Aufgaben innerhalb eines Unternehmens und der Rolle als Dienstleister (Schott 2006). Mit Hinblick auf letzteres und der häufig negativen Einstellung der Fachabteilungen gegenüber den IT-Abteilungen, wird deutlich, dass in der IT eine zunehmende Kundenorientierung erforderlich ist. Somit wird für das Managen einer modernen IT-Organisation ein hohes Maß an Prozess- und Service-Orientierung benötigt (s. (Tiemeyer 2009b) und (Schott 2006)).

Dieser Wandel führt zum Kernthema der Akzeptanzanalyse, dem IT-Service Management (ITSM) der Unternehmen am Bayerischen Untermain. ITSM wird definiert als […] jene Prinzipien und Verfahren, die der Erstellung und Erbringung von zuverlässigen, kundengerechten IT-Dienstleistungen dienen. Neben der Verbesserung der Kundenbeziehungen zielt das [ITSM] auch auf eine Qualitätsverbesserung und Kostensenkung ab (Tiemeyer 2009a). Die Information Technology Infrastructure Library (ITIL) definiert ITSM wie folgt: [IT-]Service Management ist eine Reihe von spezialisierten, organisationalen Fähigkeiten zur Stiftung von Wert für Kunden in Form von Services (itSMF 2008). ITSM legt also den Schwerpunkt auf die Kundenorientierung der IT, in der die IT die Form einer Dienstleistung – als sogenannte IT-Services – annimmt. IT-Services sind gemäß ITIL-Definition […] eine Möglichkeit, Mehrwert für Kunden zu erbringen, indem das Erreichen der vom Kunden angestrebten Ergebnisse erleichtert oder gefördert wird. Dabei müssen die Kunden selbst keine Verantwortung für bestimmte Kosten und Risiken tragen (itSMF 2008). Zusammengefasst soll das ITSM vielen der weiter oben genannten Problemfeldern und Herausforderungen der IT-Abteilungen entgegen wirken. Werden die Begriffe „IT-Service“ und „Management“ getrennt, kann ITSM somit als eine Dienstleistung in der IT und – gemäß der (IT-) Management Definition – als deren Planung, Steuerung und Kontrolle verstanden werden.

Die grundlegenden Aktivitäten im ITSM erfordern, neben den typischen Managementaufgaben und der fachlichen Kompetenz, eine ausgeprägte soziale Kompetenz von Seiten der IT. IT-Services müssen abgestimmt auf die Geschäftsprozesse die Unternehmensziele unterstützen. Hierzu ist eine intensivierte Beratung und Betreuung der Fachbereiche durch die IT-Organisation notwendig (Olbrich 2008).

Zahlreiche Rahmenwerke (Frameworks) können eine IT-Organisation bei der Ausführung der Aktivitäten innerhalb des ITSM unterstützen (Marrone und Kolbe 2011). Bei mainproject wird insbesondere der ITSM-Ansatz gemäß des de-facto Standards ITIL (Ebel 2008) vertreten. ITIL ist ein vom Office of Government Commerce (OGC) entwickeltes Rahmenwerk für die Umsetzung von IT-Service Management im Unternehmen (Fröhlich et. al. 2007). Grundlegend setzt das Rahmenwerk dabei auf dokumentierte, herstellerunabhängige Best bzw. Good Practices, die eine Standardisierung von IT-Prozessen mit Ausrichtung auf den Geschäftsnutzen vorsehen. Das ITIL-Modell folgt dabei einem Service-Lebenszyklus, der in die fünf Module Service Strategy, Service Design, Service Transition, Service Operation und Continual Service Improvement aufgeteilt ist, und innerhalb der entsprechenden Phasen für das ITSM geeignete Prozesse bereithält (itSMF 2008). ITIL befindet sich aktuell in der dritten Version, die erstmals im Jahr 2007 veröffentlich wurde. Um die Optimierungszeiten des Rahmenwerks geringer zu halten, ist man dazu übergegangen regelmäßige Updates der Versionen, erstmals mit der Edition 2011, zu entwickeln. Die Edition 2011 ist also nicht als neue Version, sondern als Aktualisierung der dritten Version zu verstehen (APMG 2011).

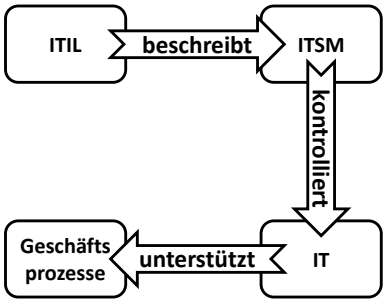


Abbildung 2: ITIL beschreibt nach Best Practice-Ansätzen welche Prozesse im Rahmen des IT-Service Managements eines Unternehmens durchgeführt werden müssen. Das IT-Service Management kann die IT im Unternehmen somit effizient kontrollieren und damit in

letzter Konsequenz die Geschäftsprozesse des Unternehmens unterstützen (Kopperger und Kunsmann 2009).

Wissenstransfer und Akzeptanz des IT-Service Managements

Es stellt sich die Frage, auf welche Akzeptanz die Durchführung von ITSM und die Einführung eines Rahmenwerks wie ITIL, bei den Unternehmen treffen. In (Hochstein et. al. 2004) wird die Akzeptanz der Mitarbeiter und der Geschäftsführung bei der Einführung von ITIL als wesentlicher Erfolgsfaktor bezeichnet. Die anfängliche Skepsis wurde hierbei durch die schnelle Umsetzung der ITSM-Prozesse gemindert. Akzeptanzfördernd war, dass so frühzeitig Erfolge aufgezeigt werden konnten, während die Optimierung der Prozesse und das Erstellen von Prozesshandbüchern später erfolgten. Die Akzeptanz und das Verständnis wurden somit nicht durch ausdetaillierte Dokumentationen, sondern durch begleitende interne Schulungen erzeugt. Auch in (Olbrich 2008) wird darauf hingewiesen, dass eine der Eingangsvoraussetzungen für die erfolgreiche Implementierung von neuen Prozessen die Akzeptanz ist – sowohl beim einführenden Unternehmen (Dienstleister) als auch beim Leistungsempfänger (Kunden). Eine Begründung könnte gemäß (Buhl 2008) unter anderem im umfangreichen Veränderungsprozess für die betroffenen Mitarbeiter, Kunden und Anwender und dem damit verbundenen Kulturwandel hin zur serviceorientierten Organisation liegen. Dieser muss von der Managementebene intensiv begleitet werden. Nach diesen Ansätzen steht für mainproject insbesondere die Begleitung des mentalen Veränderungsprozesses und die damit verbundenen intensivierten Methodenschulungen und Trainings der Mitarbeiter im Fokus, die im Zusammenhang mit der Einführung und Durchführung eines IT-Service Managements notwendig werden.

Mit dem Thema Akzeptanz von ITSM haben sich bereits eine Reihe weiterer Studien beschäftigt, wobei ITIL das am häufigsten eingesetzte ITSM-Rahmenwerk – den Status als de-facto Standard bestätigend – und mit der höchsten Akzeptanzrate eingeschätzte ist. Insgesamt seien die Akzeptanzraten von ITSM-Frameworks am steigen (Marrone und Kolbe 2011). Eine von der Unternehmensberatung exagon durchgeführte Studie, bestätigt diese Aussage. Hervorgehoben wird, dass in den meisten der befragten Unternehmen Klarheit darüber herrscht, dass IT-Prozesse verstärkt auf die Geschäftsprozesse ausgerichtet werden müssen. Positiv wird hierbei die Unterstützung bei der Neuorientierung durch ITIL, auch in Verbindung mit dem in ITIL Version 3 eingeführten Service-Lifecyle-Modells, eingeschätzt (Exagon 2009). Auch die Unternehmensberatung Materna führte im Jahr 2009 eine Studie (Siepe 2010) zu diesem Thema durch. Aus dieser geht hervor, dass ITIL auf eine größere Akzeptanz stößt als in den Vorjahren, der Einsatz sich allerdings tendenziell auf die operativen Prozesse, insbesondere den Service Desk in Verbindung mit Change und Incident Management konzentriert. Strategische Themen befinden sich weniger im Fokus. Speziell die Annäherung zwischen IT- und Geschäftsstrategie und die ITIL-Phase Continual Service Improvement – die kontinuierliche Verbesserung der IT-Services über alle Phasen ist eine der wichtigen Neuerungen der ITIL Version 3 – finden häufig keine Umsetzung oder sind den Unternehmen unbekannt. Eine Differenzierung nach Unternehmensgröße geht jedoch nicht hervor.

Auf Akzeptanzprobleme stößt ITIL insbesondere dann, wenn der Anwender keinen Nutzwert erkennen kann. Dies geschieht unter anderem dann, wenn ITIL nicht als Leitfaden wahrgenommen wird, sondern als starres Konstrukt, welches zu aufwendig in der Implementierung ist und dementsprechend Kostensteigerungen erwartet werden müssen. Das Rahmenwerk muss jedoch an das Unternehmen angepasst werden, um die Aufwände bzw. den Umsetzungsgrad selbst zu bestimmen. In einer Reihe von Untersuchungen verschiedener Frameworks wurde bei ITIL der geringste Prozentsatz bei den Kostensteigerungen ermittelt. Als akzeptanzhemmend eingestuft wird auch, dass ITIL zwar beschreibt was im ITSM getan werden muss (welche Prozesse mit welchem Ziel), es gibt jedoch wenig Hinweise darauf wie eine Umsetzung aussehen muss und die Unterstützung auf der Prozessebene endet. Das Erstellen von z.B. Implementierungsanleitungen, Verfahrensanweisungen und Kennzahlen bleibt in der Verantwortung der Unternehmen. Zusätzlich zu der prozessualen Beschreibung des ITSM, wird bei der Umsetzung im Unternehmen daher weiterhin ein großes Maß an Know-How bei der Begleitung der organisatorischen Veränderungen sowie im Bereich des Prozessmanagements benötigt. Häufig macht dies externe Beratungsleistungen erforderlich (Buhl 2008).

Für mainproject sind insbesondere die Akzeptanz von ITSM und zugehörige Rahmenwerke bei KMU von Interesse. (Buhl 2008) beschreibt, dass kleinere Unternehmen sich das Ziel setzen sollten nur wenige Teile von Rahmenwerken wie ITIL in ein bereits etabliertes Prozessmodell im Unternehmen mit einzubringen. Dabei ist zu beachten, wirkungsvoll ergänzende Maßnahmen und Erfahrungen aus Rahmenwerken mit möglichst geringem Aufwand einzusetzen, damit die notwendige Flexibilität nicht eingeschränkt wird. Der Mittelstand hingegen habe den Untersuchungen zufolge noch nicht das Potenzial der Frameworks realisiert. Es wird darauf hingewiesen, dass diese Unternehmen, ebenfalls aus Flexibilitätsgründen, kein vollständiges Prozessmodell einführen müssen. Sie sind jedoch groß genug um steigende Aufwände bei der Steuerung der IT-Organisation in Kauf nehmen zu müssen.

Eine Studie die sich explizit mit der Einführung von ITSM bei KMU in Österreich beschäftigte, noch unter Bestehen der ITIL Version 2, und daraus einen Ansatz

zur Stärkung der Akzeptanz von IT-Service Management in dieser Zielgruppe entwickelt hat, findet sich unter der Referenz Open-ITIL (Brandstätter und Peruzzi 2006). Trotz der gestiegenen Compliance - Anforderungen bezüglich der Geschäftstransparenz, inklusive der operativen Umsetzung der IT-Organisation, ist den Ausführungen zufolge bei den KMU in Österreich nur eine geringe Akzeptanz gegenüber ITSM-Frameworks festzustellen. Ausnahmen bilden hierbei große KMU, die ähnlich wie Konzernbetriebe, überwiegend bereits ITSM-Projekte durchgeführt haben. Abgesehen von diesen Ausnahmen, wird die Bedeutung von IT-Prozessen und deren Dokumentation bei den meisten KMU, im Vergleich zu den Kernprozessen der Unternehmen, als gering eingestuft. Als Grund hierfür wird ein mangelndes Verständnis für strategische Überlegungen abseits des Kerngeschäfts genannt und häufig kein Nutzwert erkannt. Es wird dennoch davon ausgegangen, dass auch in den KMU die Bedeutung des ITSM vor dem Hintergrund eines verstärkten Einsatzes von IT-Controlling und einer dadurch steigenden Kosten-effizienz wachsen wird. Als weitere Akzeptanz-hemmnisse werden die hohen Kosten einer Implementierung des ITSM, rudimentär beschriebene Prozesse in den Frameworks und die damit verbundene Notwendigkeit der externen Beratung sowie die Bindung von Ressourcen in Form von Personal genannt. Als Lösungsansatz wird die Entwicklung und Etablierung eines Open-Source-Rahmenwerks (im Sinne von Open-Source-Prozessen), angelehnt an ITIL, angestrebt um dem Bedürfnis der KMU nach transparenten Prozessen und Implementierungs-beschreibungen nachzukommen.

Das Projekt wurde bereits Ende 2007 mit der Entwicklung eines Evaluationsbogens für das Incident und Change Management beendet (OpenITIL o.J.).

Dass ITSM und ITIL im Mittelstand bisher nicht in voller Breite angekommen ist bestätigt eine weitere Studie aus dem Jahr 2011. Die 495 befragten mittelständischen deutschen Unternehmen, schätzten die Bedeutung der IT im Unternehmen mehrheitlich als groß ein. ITIL kommt jedoch nur in gut einem Viertel der Unternehmen zum Einsatz. Sich deckend mit der Umfrage von Materna, werden auch hier hauptsächlich operative Prozesse angewandt, während die strategischen Prozesse und Qualitätsverbessernde Maßnahmen wie Continual Service Improvement das Schlusslicht bilden. Bei 11 Prozent der Unternehmen konnte, trotz der nötigen kostenintensiven externen Beratungen und Schulungen, messbar eine Kostenreduzierung in der IT nachgewiesen werden (Groß 2011).

Den Ansatz über Wissenstransfer und Schulungsangeboten im Bereich des ITSM das Innovationspotenzial von KMU zu fördern wird auch vom Projekt INNOTRAIN IT in Baden-Württemberg vertreten. Im Gegensatz zu mainproject wird jedoch auf transnationaler Ebene in Mitteleuropa mit zahlreichen ausländischen Kooperationspartnern agiert, mit ausschließlichem Fokus auf ITSM. INNOTRAIN IT sieht den Grund für die fehlende Umsetzung von Technologie- und Prozessinnovation bei KMU vor allem in mangelnden Ressourcen und die damit einhergehende Konzentration auf IT-Basisfunktionen. IT-Verantwortliche sind somit nicht in der Lage sich neues Wissen anzueignen und im Betrieb umzusetzen. Um dem entgegenwirken zu können wurde eine Onlineplattform für Wissenstransfer, eigene Schulungskonzepte und ein Netzwerk zum Themenbereich ITSM entwickelt (WMBW 2010).

Auch wenn davon ausgegangen werden kann, dass die Ergebnisse dieser Studien auf die Region Bayerischer Untermain übertragen werden können, werden die ITSM-Strukturen und Akzeptanzhemmnisse im Zielgebiet, am vom Mittelstand geprägten Bayerischen Untermain (BayU o.J.), anhand von einigen Interviews überprüft. Es gilt herauszufinden, wieweit der Wandel zur Serviceorganisation und die Verbreitung von Rahmenwerken in den regionalen Unternehmen bereits vorangeschritten ist, wie der Wissenstransfer zu diesem Thema gestaltet werden muss, und dieser überhaupt erwünscht ist.
Da sich möglicherweise sich in der Praxis der Unternehmen andere Standards als ITIL im Ein-satz befinden, werden auch weitere Ansätze wie z.B. das Microsoft Operations Framework (MOF) und die enhanced Telecom Operations Map (eTOM) in der Erhebung berücksichtigt, bzw. entsprechende Antwortmöglichkeiten gegeben.

Zielsetzung
Sollen im Unternehmen nachhaltig Prozesse verbessert und die Qualität – ob in der Produktion, im Dienstleistungsbereich oder in der IT – erhöht werden, so muss ein signifikanter Nutzwert vorliegen. Um das Angebot von mainproject im Kompetenzschwerpunkt ITSM besser am Markt platzieren zu können, muss dieser zunächst erkannt und eingeschätzt werden, damit Akzeptanzhemmnisse frühzeitig identifiziert und berücksichtigt werden können. Gegenstand der Befragung ist daher eine Akzeptanz der fachlichen Inhalte des IT-Service Managements bei Unternehmen am Bayerischen Untermain. Um Synergien zu nutzen, werden Erfahrungen und Ergebnisse aus dem Vorgängerprojekt ESF-KontAkS eingebracht, dessen Fokus auf Kontext- und Akzeptanzanalysen im Bereich Automotive und Informationstechnik lag.

Als Nebeneffekt kann mit der Umfrage ein Bewusstsein für das Thema IT-Service Management geschaffen werden. Hatten Unternehmen bisher keine Berührungspunkte zu dieser Thematik, müssen sich die Adressaten bei der Beantwortung des Fragebogens zumindest kurzzeitig damit beschäftigen. Möglicherweise wird so ein erstes Interesse geweckt und

Entwicklungspotenziale erkannt bzw. aufgezeigt, die bisher noch nicht im Fokus der Unternehmen lagen.

Auf Basis der Ergebnisse sollen akzeptanzfördernde Maßnahmen und bedarfsgerechte Konzepte für den Wissenstransfer, speziell für die regionalen Betriebe, entwickelt werden.

Abgrenzung
Die Akzeptanzanalyse legt den Fokus, entsprechend der Rahmenvorgaben des ESF-Programms, auf KMU am Bayerischen Untermain. Eine Übertragbarkeit der Ergebnisse auf Unternehmen differenzierter Größenordnung und weitere Regionen Deutschlands bzw. auf internationaler Ebene ist denkbar, ein Anspruch auf Repräsentativität wird jedoch nicht erhoben. Unternehmen die aus dem genannten Raster fallen werden über entsprechende Fragestellungen identifiziert. Um eine erweiterte Übersicht über die Marktsituation zu erhalten werden Unternehmen ohne direkten Bezug zum Bayerischen Untermain, jedoch zur Metropolregion Rhein-Main, mit Hinblick auf die angedachte spätere Selbstständigkeit des Wissenstransferzentrums, in die Befragung mit einbezogen.

Aus Kapazitätsgründen werden die Aufgabenstellungen im ITSM und das Rahmenwerk ITIL im Beitrag nicht weiter vertieft. Auf die Erläuterung weiterer Rahmenwerke wie eTOM und MOF muss hier ebenfalls verzichtet werden.

Methodischer Ansatz

Durchführung einer standardisierten Befragung von Experten
Als Erhebungsmethode wurde eine Mischform aus standardisierter Befragung und Experteninterview gewählt. Die Fragen sowie die möglichen Antworten waren für alle Befragten gleich. Somit war es möglich, die gegebenen Antworten unmittelbar miteinander zu vergleichen. Durch die Frage nach ergänzenden Aspekten in Freitext-Form und der damit verbundenen Möglichkeit der offenen Antwort gelang auch eine Anpassung an individuelle Situationen.

Im Gegensatz zu rein quantitativ orientierten Methoden ging der Fragebogen ausschließlich Personen zu, bei denen eine sogenannte „Expertenvermutung“ besteht, was demzufolge zu einer geringeren Anzahl an ausgewerteten Fragebögen führt. Ob es sich bei den befragten Personen tatsächlich um Experten handelt kann nur aufgrund ihrer Position im Unternehmen vermutet werden.

Auswahl der befragten Unternehmen
Die Befragung der Unternehmen richtete sich an IT-Entscheider aus dem mainproject-Verteiler. Zusätzlich wurde die Befragung durch die IHK Aschaffenburg und deren IT-Netz Bayerischer Untermain unterstützt, die den Fragebogen an IT-Leiter in den regionalen Unternehmen verschickte.

Kernaussagen der Befragungen
Die Ergebnisse der regionalen Befragung decken sich sehr gut mit den Ergebnissen der vorher beschriebenen Studien. In den befragten Unternehmen sind in erster Linie die operativen Pro-zesse, wie das Störungs-, Problembehebungs- und Änderungsmanagement implementiert oder in Planung. Dagegen sind strategische Prozesse weit weniger im Fokus. Vor allem bei größeren KMU werden die größten Herausforderungen zur Erreichung der ITSM-Ziele in der Dienstleistungsmentalität der IT-Mitarbeiter bzw. der Serviceorientierung der IT-Organisation gesehen. Damit einhergehend besteht bei der Abstimmung zwischen IT, Fachabteilungen und Unternehmensführung Verbesserungspotenzial.

Die vorgestellten Studien zeigten auf, dass das „Continual Service Improvement“ aus ITIL in den dort betrachteten Unternehmen noch nicht ausreichend implementiert wurde oder gänzlich unbekannt war. Die Frage nach dem Stadium des kontinuierlichen Verbesserungsmanagements in den Unternehmen am Bayerischen Untermain zeigte ein geteiltes Bild. Während einige Unternehmen angaben, kontinuierliche Verbesserungsprozesse in der IT bereits zu nutzen, sahen andere überhaupt keinen Bedarf. Bei der Frage nach dem Bekanntheitsgrad von gängigen ITSM-Frameworks zeigte sich, dass diese in der Region zwar als bekannt angegeben werden, sich jedoch nicht in der Nutzung befinden. Die Gründe hierfür wurden zwar im Fragebogen mit abgefragt, wurden von den Teilnehmern jedoch meist nicht genannt. Hier könnte in einem nächsten Schritt noch einmal in persönlichen Interviews nachgehakt werden.

Ein für mainproject wichtiger Punkt war die Frage nach der Art des gewünschten Wissenstransfers. Hier sprachen sich die Unternehmen in erster Linie für den direkten Austausch mit anderen Unternehmen und Fachvorträge zum Thema IT-Service Management aus.

WEITERE VORGEHENSWEISE

Entsprechend der Bedarfe der Unternehmen der Region Bayerischer Untermain werden nun im Rahmen von mainproject Seminar- und Ausbildungsangebote entwickelt. Hierzu wird auch der Einsatz von Schulungssoftware, Simulationen und Planspiele (z.B. Fort Fantastic, Büro und Prozesssimulationen) in Erwägung gezogen. Da sich in der Region Defizite in bestimmten Bereichen zeigen, wie beispielsweise die „strategische“ Umsetzung von ITSM auf der Ebene der Unternehmensführung, werden speziell fokussierte Seminare zu entwickeln sein. Ziel ist es, Transparenz bei Methoden des IT-Managements und insbesondere des IT-Service Managements zu schaffen und zu diesem Zweck die Akzeptanzhemmnisse abzubauen.

Da sich die Ergebnisse im Bereich Continual Service Improvement zumindest zum Teil mit den bereits in Kapitel 2.1 angesprochenen Studien decken, können hier mit der mainproject-Hauptsäule Lean Management Synergien entwickelt werden. Die Integration von qualitätsverbessernden Maßnahmen aus diesem Bereich, in das IT-Management, könnte beispielsweise im Bereich Kontinuierlicher Verbesserungsprozess (KVP) und Prozessanalysemethoden liegen. Möglicherweise kann in diesem Umfeld ein Methoden-„Werkzeugkasten", bestehend aus Ansätzen des ITSM und des Lean Managements, speziell für KMU entwickelt werden.

Es ist von großer Bedeutung, ein „Bewusstsein" für die Bedeutung des ITSM zu erzeugen und dieses langfristig aufrecht zu erhalten. Ein erfolgversprechendes Instrument ist eine entsprechende Netzwerktätigkeit von Hochschulen und KMU im Rahmen des Wissenstransfers. Zu diesem Zweck wird die Einrichtung eines regionalen ITSM-Netzwerks angestrebt, was nach den Ergebnissen der Befragung auch von Unternehmensseite gewünscht ist. Fachgespräche zu wichtigen Themen des IT-Managements werden das Angebot abrunden.

Langfristig können zudem weitere Führungsthemen und Organisationsentwicklung im Sinne von Management of Change (z.B. Kulturwandel) sowie Führungskompetenz von Mitarbeitern in das Angebot von mainproject integriert werden. Als Handlungsfeld wurde hier auch im Bereich Weiterbildung – im Sinne eines „Lebenslangen Lernens" – die Führungskompetenz der Arbeitskräfte der mittleren Führungsebene in der gewerblichen Wirtschaft, speziell in KMUs identifiziert. Die „mittleren Führungskräfte" der gewerblichen Wirtschaft sind im Innovationsprozess – maßgeblich verursacht durch den technischen und gesellschaftlichen Wandel – besonders gefordert. Die Umsetzung organisatorischer Maßnahmen, wie Lean Management, ITSM, etc., oder die Etablierung technischer Innovationen, ist nicht-trivialer Natur. Hinzu treten Aufgaben im Bereich der Personalführung. Die mittlere Führungsebene erscheint hier zwar als ein zentraler Leistungsträger, ist aber für die anstehenden Führungsaufgaben in unternehmensführungs-theoretischer und wirtschafts-psychologischer Hinsicht nicht immer hinreichend gerüstet: Fachlich-technische Qualifikationen herrschen vor. Trotz besten Willens und hoher Motivation der Betroffenen treten daher Leistungsdefizite, gerade in den KMU der gewerblichen Wirtschaft, auf. Diesen kann durch entsprechende Weiterbildung im Bereich der „situativen" Organisationsformen (Projektarbeit, Teambuilding, etc.) in den KMU wirkungsvoll begegnet werden.

LITERATUR

APMG. Ohne Verfasser. 2011. ITIL® UPDATE FAQs - Summer 2011. http://www.best-management-practice.com/gempdf/ITIL_UPdate_FAQs_Summer_2011_June11.pdf. Abruf am 22.05.2012

BayU. Ohne Verfasser. Ohne Jahr. Bayerischer Untermain und High Tech. http://www.bayerischer-untermain.de/die-region-und-high-tech_3.html. Abruf am 22.05.2012

Brandstätter, M.; Peruzzi, T. 2006. Open-ITIL - ein Ansatz zur Akzeptanz-Verstärkung für den Einsatz von IT-Service Management nach ITIL in Klein- und Mittelunternehmen. LINUX SOLUTIONS GROUP e.V. http://www.osb-alliance.com/images/stories/PDF_Files/open-itil%20-%20ein%20ansatz%20zur%20akzeptanz.pdf. Abruf am 23.05.2012

Buhl, U. 2008 ITIL Praxisbuch – Beispiele und Tipps für die erfolgreiche Prozessoptimierung. mitp, REDLINE GMBH, Heidelberg.

Ebel, N. 2008. ITIL V3 Basis-Zertifizierung – Grundlagenwissen und Zertifizierungsvorbereitung für die ITIL Foundation-Prüfung. Addison-Wesley Verlag, München.

Exagon. Ohne Verfasser. 2009. ITIL 3 gewinnt deutlich an Akzeptanz - exagon-Studie: Immer mehr ITIL-Anwender erwarten eine bessere Verzahnung von IT-Prozessen und Business. http://www.exagon.de/Pressemeldungen-Detailansicht.690.0.html?&tx_ttnews[tt_news]=215&cHash=b12afcb190f1ec89b48f739455f2ec1b. Abruf am 24.05.2012

Fröhlich, M.; et. al. 2007. IT-Governance – Leitfaden für eine praxisgerechte Implementierung. Fröhlich, M; Glasner, K. (Hrsg.). Gabler Verlag, Wiesbaden.

Gabler Wirtschaftslexikon: Stichwort kritische Erfolgsfaktoren. Gabler Verlag (Hrsg.). oJ, http://wirtschaftslexikon.gabler.de/Archiv/10338/kritische-erfolgsfaktoren-v5.html. Abruf am 23.05.2012

Groß, M. 2011. ITSM – Im Mittelstand tummeln sich viele Itil-Muffel. In: Computerwoche Online. http://www.computerwoche.de/management/it-strategie/2491559/. Abruf am 23.05.2012

Hochstein, A.; Zarnekow, R.; Brenner, W. 2004. ITIL als Common-Practice-Referenzmodell für das IT-Service-Management – Formale Beurteilung und Implikationen für die Praxis. In: Wirtschaftsinformatik 46 (2004) 5, S. 382-389.

itSMF. Ohne Verfasser. 2008. Foundations in IT Service Management basierend auf ITIL V3. itSMF International – The IT Service Management Forum (Hrsg.). Van Haren Publishing, Zaltbommel.

Kopperger, D.; Kunsmann, J. 2009. Weisbecker, A.: IT-Servicemanagement. In: Tiemeyer, E. (Hrsg.): Handbuch IT-Management. Carl Hanser Verlag, München, 2009, S. 126 - 259.

Krcmar, H. 2005. Informationsmanagement. Springer Verlag, Berlin Heidelberg.

Marrone, M.; Kolbe, L. 2011. Einfluss von IT-Service-Management-Frameworks auf die IT-Organisation. In: Wirtschaftsinformatik 1 (2011), S. 5-19.

Olbrich, A. 2008. ITIL kompakt und verständlich. Vieweg + Teubner Verlag, GWV Fachverlage, Wiesbaden.

OpenITIL. Ohne Verfasser. Ohne Jahr. Open Source Business Alliance, http://www.osb-alliance.com/index.php/de/oss-erfolgsgeschichten/archiv/184-openitil. Abruf am 22.05.2012

Schott, E. 2006. IT-Organisation im Wandel: Neue Anforderungen, neue Aufgaben, neue Chancen. INTARGIA

Managementberatung, http://www.intargia.com/pdf/vortrag_it_organisation.pdf. Abruf am 23.05.2012

Siepe, C. 2010. Aktuelle MATERNA-Befragung: ITIL® kommt in Fahrt – aber nur teilweise – MATERNA IT-Service-Management Umfrage 2009. 2010, MATERNA, http://www.materna.de/DE/Pages/Presse/Pressemitteilungen/2010/BUI/Aktuelle%20MATERNA-Befragung%20ITIL%20kommt%20in%20Fahrt%20aber%20nur%20teilweise.html. Abruf am 22.05.2012

Tiemeyer, E. 2009a. IT-Management – Herausforderungen und Rollenverständnis heute. In: Tiemeyer, E. (Hrsg.): Handbuch IT-Management. Carl Hanser Verlag, München, S. 1 - 38.

Tiemeyer, E. 2009b. Organisation und Führung im IT-Bereich. In: Tiemeyer, E. (Hrsg.): Handbuch IT-Management. Carl Hanser Verlag, München, S. 360 - 398.

WMBW. 2010. Innovationsmotor IT. In: Wissenschaftsministerium Baden-Württemberg (Hrsg.): Innovation durch INTERREG – Beispiele europäischer transnationaler Zusammenarbeit. Wissenschaftsministerium Baden Württemberg, Pressestelle, Stuttgart, S. 24 - 25. http://www.interreg-bw.de/kcms/lib/download.php?id=1269595966681191&forcedownload=yes. Abruf am 24.05.2012

KONTAKT

Hochschule Aschaffenburg
Information Management Institut
Labor für Informations- und
Wissensbewertungssysteme
Würzburger Str. 45, 63743 Aschaffenburg
T +49 6021 4206-700

Dipl. Betriebswirtin (FH) Meike Schumacher,
meike.schumacher@h-ab.de

Michael Tax, B.A.,
michael.tax@h-ab.de

Prof. Dr. Georg Rainer Hofmann,
georg-rainer.hofmann@h-ab.de

Prof. Dr. Wolfgang Alm,
wolfgang.alm@h-ab.de

www.h-ab.de
www.mainproject.eu

DER WEG ZUR ENTERPRISE-CLOUD

Prof. Dr. Andreas Heberle, Prof. Dr. Rainer Neumann
Fakultät für Informatik und Wirtschaftsinformatik
Hochschule Karlsruhe – Technik und Wirtschaft
Moltkestr. 30, 76133 Karlsruhe, Deutschland
Email: Andreas.Heberle@hs-karlsruhe.de, Rainer.Neumann@hs-karlsruhe.de

STICHWORTE

Cloud Services, Web-Services, Identity Management, Prozessmanagement, Service-Orientierte Architektur, Enterprise Integration.

KURZFASSUNG

Ein großer Teil der heute entstehenden innovativen Software erscheint als Online-Dienst im Web – sei es als hochinteraktive Web-Anwendung, oder als Backend-Dienst für kleine Anwendungen wie mobile Apps oder übliche Client-Anwendungen. Unternehmen können sich durch die effektive Nutzung dieser Dienste Vorteile verschaffen, die sich entweder in reduzierten Kosten (TCO) oder in effizienteren Prozessen zeigen.

Voraussetzung hierfür ist ein klares Verständnis der notwendigen Aufgaben und der mit der Nutzung verbundenen Probleme. Diese lassen sich in drei Gruppen einteilen: Zugang zu Cloud-Diensten, Schutz der Daten in der Cloud und Integration verschiedener Cloud-Dienste zu sinnvollen und effektiven Prozessen.

Dieser Beitrag beschreibt die Aufgaben und Fragestellungen und gibt Hinweise, wie die Vielzahl verschiedener Dienste in einem Unternehmen zu einer virtuellen Enterprise-Cloud zusammengestellt werden kann: Wie können Zugänge zu Cloud-Diensten effektiv verwaltet werden? Welche Aspekte sind bei der Bereitstellung von Daten in der Cloud zu beachten? Wie sind Abläufe über mehrere Dienstumgebungen sinnvoll möglich?

EINLEITUNG

Das Thema Cloud Computing ist in aller Munde. Technische Plattformen von unterschiedlichen Anbietern (u.a. von Amazon, Google, Microsoft) sind entstanden und haben ihre Kinderkrankheiten überwunden. Im Moment entsteht ein neuer Markt für Software-as-a-Service (SaaS). Dienste werden über das Internet bereitgestellt und Kunden haben schon bzw. werden zukünftig die Auswahl haben, wessen Dienst sie zu der Lösung einer fachlichen oder organisatorischen Aufgabe verwenden wollen. Damit werden Dienste und Dienstanbieter austauschbar.

Auf der anderen Seite, haben Unternehmen existierende Prozesse und besitzen Software und Infrastruktur, die diese Prozesse automatisiert oder unterstützt. Zusätzlich haben die Unternehmen natürlich auch bestimmte Anforderungen sowohl an ihre Software, als auch an den Betrieb der Software. Hier erfordert die Nutzung von Cloud Computing doch einige Anpassungen. Während früher die Prozesse „innerhalb der Burg“ hinter Firewall und unter voller Kontrolle des Unternehmens abliefen, sollen nun externe Dienste eingebunden werden.

Die spannende Frage ist, wie passen die beiden Welten zusammen und wie kann dieser Markt an Diensten von Unternehmen so genutzt werden, dass sie auf der einen Seite profitieren, alle Anforderungen an Sicherheit und spezifische Eigenschaften ihres Business erfüllt sind und die Integration mit der existierenden Anwendungslandschaft sichergestellt ist, um getätigte Investitionen zu sichern.

Das Thema Sicherheit wird in Bezug auf die Verwendung von Cloud-Diensten immer als erstes Hindernis genannt. Das ist sicher berechtigt, aber man muss als Unternehmen schon genau analysieren, wo man tatsächlich ein Sicherheitsproblem hat und in welchen Punkten die Cloud vielleicht sogar „sicherer“ ist. Offensichtlich ist der Schutz von z.B. Kundendaten problematisch, aber welches kleinere oder mittelständische Unternehmen kann schon mit Sicherheit sagen, dass es seine Dienste sicherer betreibt als ein großer Anbieter, der das für viele Kunden macht. Weitere wichtige Fragen entstehen bezüglich Identity and Access Management sowie der Integration von Cloud-Diensten zur Automatisierung von Geschäftsprozessen.

In dieser Arbeit beleuchten wir die Nutzung von Cloud-Diensten in Unternehmen. Wir definieren unsere Sicht auf zukünftige Enterprise Clouds, diskutieren Herausforderungen und gehen auf Lösungsansätze ein.

GRUNDLAGEN

Hinter dem Begriff Cloud Computing verbirgt sich das Bereitstellen von IT-Infrastrukturen und Diensten über das Internet. Dabei stellen Anbieter den Nutzern dynamisch skalierbare verteilte Infrastrukturen (Hardware und Software) auf Abruf zur Verfügung, die entsprechend der Nutzung abgerechnet werden.

Es lassen sich vier Arten von Clouds unterscheiden. In einer *Public Cloud* stellt ein Anbieter seine Dienste mehreren Nutzern öffentlich zur Verfügung. Anbieter sind hier z.B. Amazon, Google oder Microsoft. *Private Clouds* befinden sich innerhalb eines Unternehmens, das damit auch volle Kontrolle über Daten und Zugriff auf Dienste hat. Man spricht über eine *Hybrid Cloud*, wenn ein Unternehmen eine Private Cloud besitzt und eine Public Cloud benutzt, um z.B. Lastspitzen auszugleichen oder sicherheitsunkritische Funktionalitäten von extern zu beziehen. In einer *Community Cloud* schließen sich Unternehmen derselben Branche zusammen und machen ihre Private Clouds nur den Mitgliedern der Community zugänglich.

Für Clouds gibt es unterschiedliche Servicemodelle, die auf einander aufbauen. *Infrastructure as a Service (IaaS)* stellt Speicherplatz, Rechenkapazität, Server, Switches usw. dem Kunden zur Verfügung. Bei *Platform as a Service (PaaS)* stellt ein Anbieter neben Infrastruktur auch Software inklusive Lizenzen, Wartung und Support bereit. Eigene Anwendungen können damit komplett in der Cloud entwickelt werden. Bei *Software as a Service (SaaS)* wird Software angeboten, z.B. Office-Lösungen, aber auch komplette CRM-Systeme, die über das Internet benutzt werden kann.

Die Vorteile für Unternehmen bei der Cloud-Nutzung sind vielfältig. Eine Cloud erlaubt die bedarfsgesteuerte Bereitstellung von Rechen- und Speicherkapazitäten, ohne selbst die Infrastruktur für Lastspitzen zu betreiben. Bezahlt wird nach Nutzung der Dienste. Außerdem muss sich ein Unternehmen nicht um die Wartung installierter Software sowie den Schutz vor z.B. Viren kümmern. Damit realisieren Unternehmen vor allem Kostenvorteile und können die eigene IT vereinfachen.

SaaS-Anbieter decken heute schon die meisten Anwendungsbereiche von Unternehmen ab. Das Angebot an Diensten kann in drei Kategorien unterteilt werden (siehe [KKLS12]):

- klassische Anwendungsgebiete wie z.B. Dokumentenmanagement, E-Procurement oder Marketing,
- Teilgebiete von Anwendungsbereichen wie z.B. Reisekostenabrechnung oder Web-Conferencing
- Branchenlösungen z.B. für Logistikunternehmen oder Steuerberater.

Die Anbieter sind vielfältig. Einer der Markführer ist Salesforce.com, das mittlerweile über 100000 Kunden hat[1]. Auch der Markt in Deutschland wächst. Zum Beispiel listet der SaaS-Lösungskatalog des SaaS-Forums 237 SaaS-Anbieter ([SaaS11]).

Technisch betrachtet werden diese Dienste auf unterschiedliche Arten angeboten: In der einfachsten Form sind sie nur über eine web-basierte Benutzeroberfläche zugänglich. Typischerweise stellen die Anbieter die Dienste zusätzlich als Web-Services entweder auf Basis von SOAP[2] und WSDL[3] (siehe [Papa07]), oder nach dem etwas einfacheren REST-Architekturstil (siehe [Fiel00]) zur Verfügung. Mobile Mini-Anwendungen (Apps), wie sie heute für die erfolgreichen Cloud-Anwendungen fast unumgänglich sind, benötigen genau diese Schnittstellen.

Das Vorhandensein solcher programmatisch nutzbarer Schnittstellen ermöglicht die Abbildung von Geschäftsprozessen auf Basis der Cloud-Dienste und lässt damit die Vision der Service-Orientierten Entwicklung greifbar werden – Organisationen könnten effizient Funktionalitäten aus der Cloud nutzen und zu sinnvollen Abläufen (Workflows) zusammenschalten.

DER WEG ZUR ENTERPRISE CLOUD

Der Markt für Dienste aus der Cloud entwickelt sich stark. Inzwischen gibt es vielfältige Dienste und Lösungen aus der Cloud, vom einfachen E-Mail-Dienst über Kommunikationsinfrastruktur bis hin zur Komplettlösung. Unternehmen haben damit die Möglichkeit ihre Fertigungstiefe bezüglich Software zu verringern, Best-of-Breed oder Standardsoftware aus der Cloud zu konsumieren und sich bei der Entwicklung eigener Software auf geschäftskritische Funktionalitäten und Kernprozesse zu konzentrieren.

Für die Nutzung sind unterschiedliche Szenarien möglich. Entweder kauft ein Unternehmen Komplettlösungen bei Anbietern, wie z.B. SAP mit BusinessByDesign oder die CRM-Suite von Salesforce. Oder es kauft einzelne Dienste, um Lücken im existierenden Software-Portfolio zu schließen bzw. um kostenintensive, selbst betriebene Software abzulösen.

Ein Problem mit Cloud-Diensten ist, dass es wenig Standardisierung gibt und die Dienste in die existierende Landschaft eingebunden werden müssen. Dafür benötigt ein Unternehmen eine geeignete technische Architektur und Infrastruktur, die die Integration einfach möglich macht. Weitere Optionen ergeben sich, wenn ein Unternehmen eine Private Cloud betreibt, um Sicherheitsprobleme zu umgehen, und zusätzlich Dienste aus Public Clouds nutzt.

---

[1] http://www.salesforce.com/de/customers/
[2] http://www.w3.org/TR/soap/
[3] http://www.w3.org/TR/wsdl

Abbildung 1: Schritte auf dem Weg zur Enterprise Cloud

Ein Unternehmen auf dem Weg in die Enterprise Cloud muss folgende Fragen klären bzw. folgende Schritte (siehe Abbildung 1) ausführen:

1. **Identifikation und Auswahl potenzieller Dienste**

   Hierbei geht es um die Frage, welche Dienste aus der Cloud funktionale Lücken der bestehenden Softwarelandschaft schließen. Dieser Schritt sollte also mit einer Schwachstellenanalyse im Haus beginnen.

   Bei der Auswahl der Dienste muss sich ein Unternehmen überlegen, wie stark es sich an den Anbieter bindet – ist dieser in einer wirtschaftlich ausreichend stabilen Situation und passen die gesetzlichen Rahmenbedingungen zur Nutzung? Gerade der letzte Punkt ist in Hinblick auf vertragliche Regelungen und Datensicherheit bzw. Datenschutz von großer Bedeutung.

2. **Wirtschaftlichkeitsanalyse**

   Die Abrechnungsmodelle in der Cloud variieren sehr stark – Benutzerbezogene Modelle werden oftmals mit Datentransfervolumina und Speicherkapazitäten gemischt – ein objektiver Vergleich verschiedener Anbieter fällt hier schwer, sollte aber gerade deshalb sorgfältig durchgeführt werden. Insbesondere für die Faktoren Verfügbarkeit, Leistung und Skalierbarkeit müssen vorab geeignete Erwartungswerte definiert werden.

3. **Technische Erschließung der Dienste**

   Auf technischer Seite muss geklärt werden, wie sich die Cloud-Services in die eigene Infrastruktur integrieren lassen. Im einfachsten Fall ist dies die Nutzung von Web-Seiten des Anbieters, etwas aufwändiger ist die Integration in automatisierte Abläufe. In jedem Fall muss jedoch der Zugang zu den Diensten und das damit verbundene Identity und Access Management erstellt werden.

4. **Kontrollierte Cloud-Nutzung**

   Die Nutzung von Cloud-Diensten muss aus Unternehmenssicht dahingehend überwacht werden, dass eine Bewertung der tatsächlichen Nutzungsanforderungen erfolgen kann: Sind die vertraglichen Rahmenbedingungen eingehalten? Passen die angefallenen Kosten zu den in Anspruch genommenen Leistungen?

Ein Unternehmen begegnet bei diesen Schritten schiedlichen Herausforderungen, auf die wir im den eingehen werden.

HERAUSFORDERUNGEN FÜR UNTERNEHMEN

Neben dem Thema Sicherheit, das Verantwortlichen als erstes in den Sinn kommt, geht es bei der Nutzung von Cloud-Diensten auch um die Frage, wie man den Zugriff auf Cloud-Dienste kosteneffizient und sicher gestalten kann. Außerdem müssen die externen Dienste so integriert werden, dass die Prozesse geeignet unterstützt werden.

Sicherheit

Bei der Diskussion von Sicherheitsfragen in der Cloud muss man unterscheiden zwischen Problemen, die man allgemein in Netzwerken und mit der eigenen IT-Infrastruktur hat, und zwischen Cloud-spezifischen Bedrohungen.

Zu den gemeinsamen Bedrohungen gehören u.a. sichere Übertragung von Informationen, Distributed-Denial-of-Service Attacken, bedrohliche Insider, Account und Service Hijacking ([ClSA10]) und natürlich auch technische Pannen, die zu Systemausfällen führen können. Diese Probleme hat man sowohl mit internen Systemen (sofern sie nicht vollkommen abgeschottet sind) als auch in Kombination mit Cloud-Diensten. Allerdings kann man davon ausgehen, dass Cloud-Anbieter erkannte Schwachstellen schneller erkennen und schließen werden.

Die Nutzung von Cloud-Diensten führt dazu, dass Software und Daten, die bisher durch Firewall, DMZ und andere Sicherheitsmechanismen geschützt waren, nun außerhalb liegen. Damit stehen Nutzer und potentielle Angreifer auf einer Stufe.

Datensicherheit

Datensicherheit hat mehrere Aspekte: sicherer Zugriff auf die Daten, sichere Übertragung sowie sichere Verarbeitung und Lagerung der Daten. Die Datenübertragung in und aus der Cloud wird über sichere Protokolle und Kanäle durchgeführt. Die Kontrolle des Zugriffs auf Daten hängt an der Umsetzung von Rollen und Berechtigungskonzepten.

Bei der Lagerung von Daten kann man unter Sicherheitsgesichtspunkten erwarten, dass die Daten verschlüsselt abgelegt werden. Die Verarbeitung von Daten ist kritisch, da die meisten Ansätze unverschlüsselte Daten für die Verarbeitung erwarten. Den Problemen wird unterschiedliche begegnet:

- Unternehmen lagern nur unkritische Daten in die Cloud aus, geschäftskritische und wertvolle Daten werden intern verwaltet und bearbeitet.
- Sensible Daten werden verschlüsselt und verteilt abgelegt. Hier gibt es unterschiedliche Ansätze. Zum Beispiel wird bei MimoSecco – Middleware for Mobile and Secure Cloud Computing ([Mimo12]) Sicherheit unter Verwendung von Hardware-Tokens verbessert. OmniCloud ([Frau12a]) ermöglicht per Software die sichere Verwendung von Cloud-Storage Diensten und bietet auch einen Umzugsservice, damit man nicht von einem Anbieter abhängig ist.
- Mittels Homomorphic Encryption ([LaNV11]) können Berechnungen direkt auf den verschlüsselten Daten durchgeführt werden. Nur der Besitzer der Daten kennt den Schlüssel. Der Cloud-Anbieter, der mit den Daten rechnet, kennt die entschlüsselten Daten dabei nicht.

Eine aktuelle Studie des Fraunhofer SIT besagt, dass die Cloud-Anbieter die Frage nach Sicherheit sehr ernst nehmen, aber Probleme mit der durchgängigen Umsetzung haben [Frau12b]. Hier besteht also noch Verbesserungsbedarf.

Vertrauenswürdigkeit der Cloud-Anbieter

Die Verwendung von Cloud-Diensten setzt voraus, dass der Anbieter vertrauenswürdig ist. Der erste Schritt ist, dass Anbieter und Nutzer eine Vertragsbeziehung eingehen und Service Levels vereinbaren.

Zusätzlich gibt es Standards, die für Cloud-Anbieter relevant sind, z.B. ISO/IEC 27001 für Netzwerksicherheit. Außerdem sind Zertifizierungsprogramme entwickelt worden. Z.B. hat der Verband der deutschen Cloud Computing-Industrie das EuroCloud Star Audit Certificate für SaaS entwickelt ([EuDe11]). Allerdings müssen sich die Zertifikate erst noch bewähren.

Operationale Sicherheit

Für den Kunden ist die Dienstqualität, Verfügbarkeit, Performance etc., die ein Cloud-Anbieter zusichert wichtig, da unter Umständen Geschäftsprozesse nicht ablaufen können, wenn ein Dienst nicht verfügbar ist. Die Abmachung und vertragliche Zusicherung von Service Level Agreements ist daher essentiell.

Wichtig ist außerdem die Zuverlässigkeit und wirtschaftliche Situation des Anbieters. Hier stellen sich die Fragen was würde z.B. mit den Daten passieren, wenn der Anbieter den Betrieb einstellt oder eine Katastrophe ein Rechenzentrum des Anbieters lahmlegt. Zusätzlich muss geklärt sein, ob und wie Daten bei einem Anbieterwechsel umgezogen werden können.

Für den Kunden ist Transparenz zu Verbrauch und Kosten inklusive einem entsprechenden Reporting wünschenswert. Die einzelnen Anbieter stellen zwar Reportingfunktionalität zur Verfügung, aber diese ist über die Anbieter hinweg nicht standardisiert, so dass in einem Multi-Cloud-Szenario zusätzliche Integrationsaufwände anfallen.

Rechtssicherheit

Grundsätzlich gehen Anbieter und Abnehmer eine Vertragsbeziehung ein. Das Vertrauen ergibt sich aus dem Vertrag. Allerdings gibt es in den unterschiedlichen Ländern rechtliche Unterschiede, so dass der Gerichtsstand bei Streitigkeiten relevant ist. Außerdem unterscheiden sich die Auflagen bzgl. Vorratsdatenspeicherung und Aufbewahrungsfristen.

Zum Beispiel müssen in Deutschland Rechnungen für 30 Jahre aufbewahrt werden. Der Service-Anbieter muss das dann auch garantieren. Kritisch ist auch das Thema Datenschutz. Deutschland hat z.B. ein sehr viel restriktiveres Datenschutzgesetz als die USA. Vor allem der USA Patriots Act [USCo01] ist für deutsche Firmen kritisch.

Auch wenn die Daten eines amerikanischen Service-Anbieters außerhalb der USA lagern, dann können US-Behörden Zugriff auf diese Daten erlangen [Sawa11]. Im Moment sind bzgl. Datenschutz unterschiedliche Reformbemühungen und Gesetzesanpassungen im Gange, z.B. [Euro11].

Identity & Access Management

Ein Unternehmen hat üblicherweise eine Benutzerverwaltung inklusive existierender Rollen und Berechtigungen im Einsatz. Dort werden neue Mitarbeiter mit der zur Job-Beschreibung passenden Rollen eingetragen oder bei Austritt aus der Firma gelöscht. Hier kommen in Firmen Werkzeuge wie ein LDAP Directory oder z.B.

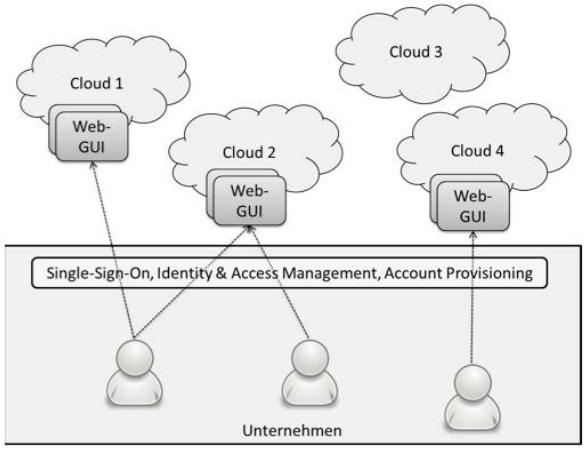


Abbildung 2: Identity & Access Management

Active Directory von Microsoft zum Einsatz. Werden externe Dienste eingesetzt, dann müssen Benutzer und Rollen des Dienstes mit existierenden Benutzerstrukturen verbunden werden. Abbildung 2 veranschaulicht die Aufgaben des Identity & Access Managements.

Single-Sign-On

Benutzt man Dienste mit Geschäftsbezug, dann erfordert das üblicherweise ein Login des Anwenders. Allerdings soll ein Anwender sich genau einmal am System anmelden müssen, auch wenn im Hintergrund unterschiedliche Dienste mit eigenen Logins zum Einsatz kommen. Hierfür gibt es unterschiedliche Single-Sign-On Lösungen. Im Falle von Web-Anwendungen wird oftmals wird die einfachste Variante des automatischen Ausfüllens von Formulardaten durch den Browser genutzt. Innerhalb der Microsoft Systemlandschaft sind Lösungen basierend auf Active-Directory und den dort genutzten Protokollen (z.B. SPNEGO, Kerberos) weit verbreitet.

Integration der eigenen Benutzerverwaltung

Die Integration der Benutzer und Rollen eines externen Dienstes ist Voraussetzung für die richtige Nutzung des Dienstes. Teilweise bringen Cloud-Dienste schon die Integration mit einem Unternehmens-LDAP mit. Außerdem gibt es schon Standards wie z.B. OpenID, mit denen man Identitäten zwischen Anbietern verifizieren kann. Setzt man allerdings Cloud-Dienste unterschiedlicher Anbieter ein, dann muss die Integration üblicherweise von der internen IT durchgeführt werden.

Provisioning von Cloud Services

Entscheidet sich ein Unternehmen für die Verwendung eines Cloud-Service, dann ist die Benutzung üblicherweise an eine Rolle gebunden. HR-Services sollten z.B. nur von HR-Mitarbeitern verwendet werden können. Das bedeutet aber, dass man bei Neunutzung eines Dienstes die entsprechenden Mitarbeiter freischalten muss, neue Mitarbeiter müssen nachgetragen werden, ausscheidende Mitarbeiter müssen entfernt werden. Werden diese Aufgaben manuell ausgeführt, dann bedeutet das relevante Kosten für ein Unternehmen. Automatisierung ist erwünscht, allerdings gibt es noch nicht viele Werkzeuge bzw. Anbieter für solche Lösungen.

Automatisierung von Geschäftsprozessen mit Cloud Services

Cloud-Dienste können entkoppelt und autonom verwendet werden. Das ist das heute noch übliche Geschäftsmodell von vielen Anbietern. Den größten Nutzen aus dem SaaS-Ansatz kann ein Unternehmen allerdings ziehen, wenn die Cloud Services für die Automatisierung bzw. Unterstützung von Geschäftsprozessen eingesetzt werden und mit der existierenden internen Software nahtlos integriert sind. Cloud-Dienste werden also als Teile einer Service-orientierten Architektur (SOA) betrachtet.

Integration interner und externer Dienste

Früher haben Firmen viel in die Integration von Anwendungen investiert (Enterprise Application Integration). Das war notwendig, weil Anwendungen, die aus Geschäftssicht zusammenspielen sollten, mit unterschiedlichen Technologien, auf unterschiedlichen Plattformen, aber auch mit unterschiedlichen Datenmodellen entwickelt wurden und deshalb nicht richtig zusammengepasst haben. Die Integration findet dabei auf unterschiedlichen Ebenen statt: auf der Datenebene, auf der funktionalen Ebene und auf der Präsentationsebene.

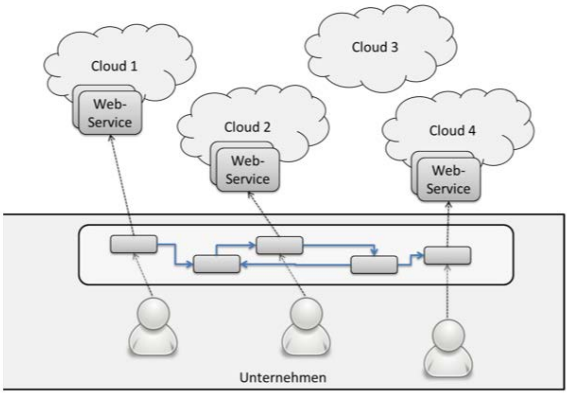


Abbildung 3: Prozessorientierte Verschaltung von Diensten

Ähnliche Integrationsaufgaben hat man nun auch der, wenn man Internet-Dienste unterschiedlicher teller einbinden will. Ein Anbieter definiert sein eigenes Datenmodell (hat z.B. sein eigenes Kundenobjekt), hat seine Technologie (z.B. SOAP Web Services) und bestimmt, wie die Interaktion mit Menschen über User Interfaces (z.B. ein HTML 5 mit vorgegebenem Layout) funktioniert. Bindet man mehrere Dienste unterschiedlicher Anbieter ein, dann vergrößert sich die Integrationsaufgabe.

Eine Service-orientierte Architektur ist dann schon fast Voraussetzung, da Dienste als Bausteine bereits vorgesehen sind, die Infrastruktur z.B. in Form eines Enterprise Service Bus Integrationsunterstützung bietet und damit Dienste einfacher eingebunden werden können.

Ein wichtiger Aspekt bei der Integration externer Dienste ist Sicherheit. Technisch muss eine sichere Übertragung, Authentifizierung und möglicherweise die End-to-End-Verschlüsselung sensibler Daten sichergestellt werden. Hier bieten SOAP Web Services mehr Möglichkeiten als RESTful Web Services.

Prozessautomatisierung

Geschäftsprozesse werden von Fachexperten definiert, sind an der Strategie orientiert und ändern sich, wenn sich z.B. der Markt oder das Angebot verändert oder wenn es neue gesetzliche Regelungen gibt. Geschäftsprozesse eines Unternehmens können in unterschiedli-

chen Varianten ausgeprägt sein, z.B. um länderspezifische Eigenheiten in internationalen Tochterfirmen abzubilden. Daher ist es wichtig, Geschäftsprozesse möglichst flexibel und einfach anpassbar zu implementieren.

Die Dienste einer Service-orientierten Architektur entsprechen dabei einzelnen Prozessaktivitäten, Teilprozessen oder sogar kompletten Prozessen. Um einen Geschäftsprozess abzubilden, werden existierende Dienste passend verschaltet und die Logik zur Ansteuerung der Dienste wird durch eine Process Engine ausgeführt. Die Process Engine startet Prozesse (z.B. durch Eingang eines Urlaubsantrags), verwaltet unterschiedliche Prozessinstanzen (z.B. Urlaubsanträge der Mitarbeiter Müller und Maier) und initiiert die nächsten Schritte einer Prozessinstanz (z.B. Manager Schmidt muss den Antrag von Herrn Maier genehmigen).

Der Einsatz einer Business Process Management Suite (BPMS) in Kombination mit einer Business Rules Engine ermöglicht die schnelle Umsetzung und einfache Anpassung von Prozessen. Änderungen werden dabei vor allem an den Prozessmodellen (in Business Process Model and Notation [ObMG11] beschrieben) und an den Geschäftsregeln vorgenommen. Durch den Austausch kompletter Dienste kann neue Geschäftslogik eingebunden werden.

Die BPMS bietet auch noch Funktionalität für das Monitoring der Prozessausführung und ist damit eine Informationsquelle für die Prozessoptimierung.

Cross-Cloud-Workflows

Cloud-Services können oftmals bereits mit anderen Cloud-Services interagieren – die Authentifizierung mit Mechanismen wie Open-ID ist ein sehr rudimentäres Beispiel, bei dem ein Service-Anbieter Dienste eines anderen nutzt. Weitere Beispiele findet man z.B. bei der Integration von Mail-Services oder Archivlösungen.

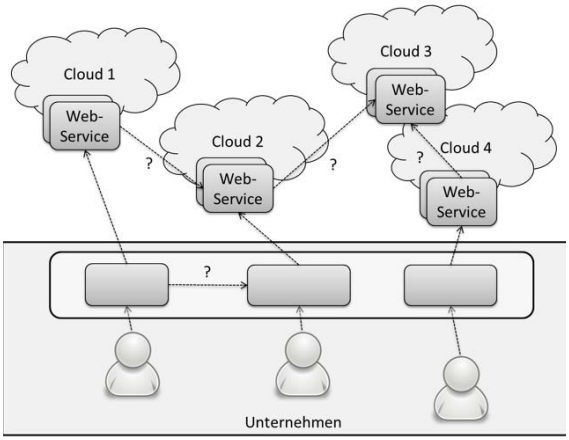


Abbildung 4: Cross-Cloud Workflows

Im Gegensatz zu den elementaren Diensten finden sich in der Cloud also bereits Teilabläufe, die – geschickt kombiniert – zu größeren und effizienten Workflows kombiniert werden können. Dazu müssen die genutzten Cloud-Services geeignet konfiguriert werden, wofür es in der Regel jedoch keine geeignete Programmierschnittstelle gibt, da diese Art der Kombination von der aktuellen Anbietern oft nicht vorgesehen ist.

Unter anderem stellt sich hier das Problem der Identity Propagation – wie werden Abläufe aus einer Cloud von der ausführenden Person in einer anderen Cloud angestoßen und unter welchem Namen erfolgt das? Abbildung 4 veranschaulicht die Situation.

ZUSAMMENFASSUNG UND AUSBLICK

Wir haben in diesem Beitrag vorgestellt, wie Unternehmen zukünftig unterschiedlichste Dienste von unterschiedlichen Anbietern aus ihrer Enterprise Cloud in ihre Anwendungslandschaft integrieren können. Ein Benutzer arbeitet zukünftig mit einem Prozessportal oder stellt sich sein User Interface nach eigenen Vorlieben zusammen (z.B. als Mashup) und sollte gar nicht merken, dass er Dienste aus unterschiedlichen Quellen des Internets konsumiert. Der zukünftig zu erwartende Markt für Dienste ermöglicht dann sogar den Austausch funktional äquivalenter Services.

Wichtig für den Erfolg der Enterprise Cloud ist, dass bestimmte Herausforderungen gelöst werden. Dazu gehören neben Sicherheitsproblemen auch Betriebsfragen, z.B, wie man das Service-Provisioning und die Abrechnung sicher und weitestgehend automatisiert vornehmen kann. Eine weitere Herausforderung liegt in der nahtlosen und sicheren Integration der (Web) Services und die weitestgehend werkzeugunterstützte Automatisierung von Geschäftsprozessen unter Verwendung dieser Dienste.

In dieser Arbeit haben wir für einen Teil der Herausforderungen Antworten bzw. Lösungen vorgestellt. Für andere Probleme, z.B. zur sicheren Verarbeitung sensitiver Daten, gibt es zwar schon Lösungsansätze, diese müssen sich in der Praxis allerdings erst noch bewähren. Speziell beim Thema Cross-Cloud Workflows müssen geeignete Lösungen erst noch entwickelt werden.

Wir sind jedoch davon überzeugt, dass zukünftig kleine, mittlere und große Unternehmen die Enterprise Cloud nutzenbringend einsetzen werden.

LITERATUR

[ClSA10] *Cloud Security Alliance*: „Top Threats to Cloud Computing“. cloudsecurityalliance.org. 2010, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. Abruf am 2012-05-12

[Euro11] *Europa Press Release*: „EU-Justizkommissarin Viviane Reding und Bundesverbraucherministerin Ilse Aigner setzen sich gemeinsam für einen stärkeren Datenschutz auf EU-Ebene ein“. In: Europa Press Releases Rapid. 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/762&format=HTML&aged=0&language=DE&guiLanguage=en. Abruf am 2012-05-12

[EuDe11] *EuroCloud Deutschland_eco e.V*: „SaaS Gütesiegel 1.0 - Kurzinformation“. 2011, http://www.saas-audit.de/files/2011/03/quick-reference_de.pdf. Abruf am 2012-05-12

[Fiel00] *Fielding, Roy Thomas*: „Architectural Styles and the Design of Network-based Software Architectures.“. UNIVERSITY OF CALIFORNIA, IRVINE, Dissertation, 2000.

[Frau12a] *Fraunhofer-Institut für Sichere Informationstechnologie*: „OmniCloud - Sicheres Datenbackup in beliebigen Storage-Clouds“. 2012, http://www.sit.fraunhofer.de/de/kompetenzfelder/projekte/omnicloud.html. Abruf am 2012-05-12

[Frau12b] *Fraunhofer-Institut für Sichere Informationstechnologie*: „On the Security of Cloud Storage Services.“ 2012, http://www.sit.fraunhofer.de/content/dam/sit/en/studies/Cloud-Storage-Security_a4.pdf. Abruf am 2012-05-12

[Henk11] *Henkel, Markus*: “OmniCloud: verschlüsselte Daten außerhalb der Cloud”. In: Enterprise Efficiency - The Efficient Information Technology Community. 2011,

http://de.enterpriseefficiency.com/author.asp?section_id=1292&doc_id=234344. Abruf am 2012-05-12.

[KKLS12] *Kleemann, Sascha; Leiker, Viktor; Künle, Tobias und Schwald Daniel*: „Services und servicebasierte Anwendungen aus der Cloud“. Seminararbeit, Hochschule Karlsruhe – Technik und Wirtschaft, Fachbereich Wirtschaftsinformatik. 2012.

[LaNV11] *Lauter, Kristin; Naehrig, Michael und Vaikuntanathan, Vinod* : „Can Homomorphic Encryption be Practical?”. In CCSW ´11Proceedings of the 3rd ACM workshop on Cloud computing security workshop.

[Mimo12] *Projektkonsortium MimoSecco*: MimoSecco – Middleware for Mobile and Secure Cloud Computing. 2012, http://www.mimosecco.de/. Abruf am 2012-05-12

[ObMG11] *Object Management Group*: Business Process Model and Notation (BPMN) – Version 2.0. 2011, http://www.omg.org/spec/BPMN/2.0/. Abruf am 2012-05-12.

[Papa07]*Papazoglu, Michael*: „Web Services: Principles and Technology”. Prentice Hall. 1st edition, 2007.

[SaaS11] *SaaS-Forum*: „SaaS-Forum Lösungskatalog“, 2011

[Sawa11] *Sawall, Achim*: „USA Patriot Act: Europäische Cloud-Daten nicht vor US-Zugriff sicher“. In: golem.de IT-News für Profis. 2011, http://www.golem.de/1106/84620.html. Abruf am 2012-05-12

[USCo01] *US Congress*: „H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT)“. In: The Library of Congress. 2001, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:. Abruf am 2012-05-12