HZD
Hessische Zentrale für Datenverarbeitung

HESSEN

Trendbericht 2010

Herausgeber:
Hessische Zentrale für Datenverarbeitung | Mainzer Straße 29 | 65185 Wiesbaden
Telefon: (06 11) 3 40-0 | E-Mail: info@hzd.hessen.de

Verantwortlich:
Dr. Markus Beckmann
Telefon: (06 11) 3 40 12 80 | E-Mail: Markus.Beckmann@hzd.hessen.de

Druck:
Hessisches Landesamt für Bodenmanagement und Geoinformation | Schaperstraße 16 | 65195 Wiesbaden

Erscheinungstermin:
Januar 2010

Inhalt

Vorwort

In den vierzig Jahren ihres Bestehens hat die HZD die Entwicklung der IT aufmerksam verfolgt und aktiv daran teilgenommen. Interaktive Anwendungen und schnelle Netze haben längst Lochkarten und Batchbetrieb abgelöst und ermöglichen moderne Verwaltungs-IT an verteilten Standorten – so auch seit zwanzig Jahren in Hünfeld. Obwohl inzwischen zur anerkannten Infrastruktur avanciert, musste die IT aber in diesen Jahren immer wieder stürmische Zeiten erleben.

Als im Jahr 2000 die sogenannte Dotcom-Blase platzte, verschwanden nicht nur viele Unternehmen von der Bildfläche, die ihre Geschäftsmodelle auf den potenziellen Möglichkeiten des Internets aufgebaut hatten. Im Nachgang waren auch immer weniger Informationen über neue Entwicklungen in der IT zu finden – nicht nur bei der Webtechnik. Die Frage, wie denn mit der vorhandenen IT die bestehenden Geschäftsmodelle und auch das Verwaltungshandeln unterstützt werden könnten, trat in den Vordergrund. „Konsolidierung“ war das Schlagwort der Stunde.

Seit 2007 und verstärkt im Jahr 2008 hat eine neue Krise die Weltwirtschaft erfasst, die sich – ausgehend von den Finanzsystemen – auf alle Wirtschaftszweige auswirken kann. Man könnte vermuten, dass diese sich nun auch wieder auf die IT auswirkt – und einige Anzeichen dafür gibt es inzwischen tatsächlich. Nicht unmittelbar für das Geschäft erforderliche Investitionen in Anwendungen und Infrastruktur werden zurückgestellt, und viele Projektaktivitäten werden auf das absolut notwendige Maß reduziert. An den Informationen über Entwicklungen in der Informations- und Kommunikationstechnik ist dieser Trend aber noch nicht abzulesen.

Es gibt noch immer zahlreiche Veröffentlichungen über neue Ideen, Techniken und Konzepte. Einige von ihnen detaillieren die Entwicklungen der letzten Jahre. So wird beispielsweise viel über die praktische Umsetzung von Cloud Computing veröffentlicht – insbesondere unter Sicherheitsaspekten. Andere setzen bei den Grundlagen im Umgang mit Computern und Anwendungen an und liefern damit Hinweise auf möglicherweise bevorstehende grundlegende Veränderungen in unserem Umgang mit IT. Hier werden z. B. neue Interaktionsmöglichkeiten mit dem Rechner über den Bildschirm oder künftige Formen vernetzter Zusammenarbeit skizziert. Dass auch die Durchdringung des täglichen Lebens mit Informationstechnik weiter heftig voranschreitet, ist an den zahlreichen Diskussionen um das Thema Sicherheit und Datenschutz zu erkennen.

Woran mag es aber liegen, dass die Informationstechnik sich – noch – kaum gebremst zu entwickeln scheint? Hierfür kann es mehrere Gründe geben. Die Erwartung, dass es sich um eine befristete Krise handelt, mag dabei genauso eine Rolle spielen wie die Hoffnung, dass IT als „Geschäftsbeschleuniger“ ihre Auswirkungen nur abgeschwächt zu spüren bekommt. Hinzu kommt, dass Innovation zurzeit ein spannendes Thema ist, das selbst einen Trend – auch außerhalb der IT – darstellt. Das Europäische Jahr der Kreativität und Innovation unterstreicht dies. Schließlich stehen vergleichsweise viele Ressourcen – zumindest Personal und Zeit – zur Verfügung, um sich neuen Entwicklungen widmen zu können. Es bleibt zu hoffen, dass die Erwartungen an ein baldiges Ende der Krise sich erfüllen und das Potenzial der neuen Ideen auch tatsächlich ausgeschöpft werden kann – zum Wohl der Wirtschaft, der Verwaltung und aller Menschen dahinter. Wie es weitergeht, werden wir in den folgenden Trendberichten sehen. Zunächst aber wünschen wir eine spannende Lektüre zu den aktuellen Entwicklungen.

Zu diesem Text

Mit dem Trendbericht ermöglichen wir unseren Leserinnen und Lesern einen Ausblick auf die aktuellen Trends in der Informationstechnologie. Dabei wollen wir uns jedoch nicht auf eine rein fachliche Information über die technischen Hintergründe und die weitere Entwicklung beschränken.

Als IT-Gesamtdienstleister für die hessische Landesverwaltung steht für uns die strategische Bedeutung der erfassten Trends für die Verwaltung im Mittelpunkt. Daher haben wir jedes einzelne Thema im Hinblick auf seine Auswirkungen auf die Verwaltung bewertet. Der Fokus liegt dabei auf der hessischen Landesverwaltung. Neben einem kurzen Bewertungstext werden jeweils drei Kennzahlen angegeben, die die Einordnung der Themen in IT-strategische Überlegungen erlauben:

Verwaltungsrelevanz

Die Verwaltungsrelevanz gibt an, in welchem Maß sich ein Trend auf die Verwaltung auswirken kann. Dies kann auf zweierlei Arten erfolgen: Zum einen können Trends zu technischen Änderungen in der IT-Landschaft führen bzw. solche Änderungen ermöglichen. Diese Trends sind daher in dem Maß verwaltungsrelevant, wie sie sich auf einige oder alle IT-Arbeitsplätze im Land auswirken – entweder direkt am Arbeitsplatz oder durch die Gesamtinfrastruktur. Zum anderen können IT-Trends dazu führen, dass sich Verwaltungsabläufe ändern oder ganz neue Abläufe etabliert werden (können). In diesen Fällen haben die IT-Trends also Auswirkungen auf die Kernprozesse der Verwaltung.

Die Verwaltungsrelevanz wird auf einer fünfteiligen Skala angegeben, die die Auswirkung des Trends auf die Verwaltung bewertet:

Auswirkung:

 keine
 geringe
 mittlere
 deutliche
 starke

Marktreife/Produktverfügbarkeit

Der Wert für Marktreife bzw. Produktverfügbarkeit gibt an, wie lange es dauern wird, bis Produkte am Markt verfügbar sind, die auf der im Trend beschriebenen Entwicklung basieren. Die fünfteilige Skala gibt die Marktreife bzw. Produktverfügbarkeit mit folgenden Werten an:

 sofort
 1–2 Jahre
 2–4 Jahre
 mind. 4 Jahre
 noch nicht absehbar

Umsetzungsgeschwindigkeit

Die Umsetzungsgeschwindigkeit gibt an, wie schnell ein Trend in der Verwaltung umgesetzt werden kann. Sie kann als ein Maß für die Komplexität der entsprechenden Trendergebnisse gesehen werden. Je komplizierter ein Resultat oder Produkt ist, desto länger dauert es, es in Verwaltung und Unternehmen nutzbar zu machen. Die fünfteilige Skala gibt die Einführungsgeschwindigkeit mit folgenden Werten an:

 sofort
 1–2 Jahre
 2–4 Jahre
 mind. 4 Jahre
 noch nicht absehbar

Seminare bei der HZD

Die HZD bietet zahlreiche Seminare zu aktuellen Themen an. Trendthemen aus diesem Bericht, die im Schulungsangebot der HZD aufgegriffen werden, sind entsprechend gekennzeichnet.

siehe Seite 44/45

Methoden, Grundlagen, Standards

„Form follows function" – Architekturen und Reengineering

Umstrukturierung ist nicht nur für Organisationen ein wichtiges Thema, sondern auch für IT-Systeme. In beiden Fällen ist die Erwartung, dass ein neuer Zuschnitt der funktionalen Einheiten noch besser als der bestehende dazu geeignet ist, Unternehmensziele zu erreichen. In Bezug auf IT-Systeme – insbesondere auch Softwaresysteme – gab es in den letzten Jahren immer wieder Anlass zu prüfen, ob ihre Architektur noch den Erfordernissen einer modernen Softwarelandschaft entspricht, die insbesondere dazu geeignet ist, die Gesamtgeschäftsstrategie der betreibenden Organisation zu unterstützen. Die Neuausrichtung einer Softwarearchitektur kann an zwei Stellen ansetzen: zum einen bei der Entwicklung neuer Systeme und zum anderen bei der Analyse bestehender Systeme. Letzteres kann sowohl im Hinblick auf ihre Pflege und Weiterentwicklung geschehen als auch zu dem Zweck, bereits realisierte Komponenten zu identifizieren, die eventuell in anderen Systemen verwendet werden können. Das Thema Reengineering und Restrukturierung von Architekturen hat daher in der Softwareentwicklung an Bedeutung gewonnen.

Die weite Verbreitung von Webtechnologien – nicht nur im Internet, sondern auch in geschlossenen Netzen – hat ein neues Licht auf Client-Server-Architekturen geworfen. Auch dadurch, dass immer bessere Infrastrukturen zur Verfügung stehen, werden klassische „Vor-Ort-Anwendungen" in Frage gestellt, und der Zugriff über Webschnittstellen auf zentrale Anwendungen weitet sich aus (⇨ „Ware als Dienstleistung – SaaS"). Dies gipfelt gegebenenfalls in dem Bestreben, unternehmensweit eine sogenannte serviceorientierte Architektur, SOA, aufzubauen. Aber auch dann, wenn etablierte Anwendungen auf andere neue Technologien umgestellt werden sollen oder müssen, stellt sich die Frage nach ihrer Architektur. Dabei versteht man unter einer Softwarearchitektur ein Modell von ihren Komponenten und von deren Zusammenhängen – untereinander wie auch mit der Umgebung. Ergänzend kann man noch die zugrundeliegenden Entwurfsprinzipien dazurechnen.

Jedes Softwaresystem hat eine Architektur – zumindest implizit. Wenn man an einem System arbeiten will und es dabei vollständig betrachten muss, ist es ab einer gewissen Größe erforderlich, seine Architektur explizit zu beschreiben. Die Strukturierung einer Software in einem Architekturmodell ist ein guter Weg, seine Komplexität zu reduzieren – genauer gesagt: die Komplexität seiner Darstellung zu reduzieren. Dies gilt sowohl bei der Konstruktion neuer Systeme als auch bei der Analyse bestehender Systeme.

Ein Architekturmodell kann anhand verschiedener Kriterien strukturiert werden. Solche Kriterien können sich z. B. aus verwendeten Technologien wie einem zugrundeliegenden Entwicklungsframework ergeben. Ein anderer Ansatz orientiert sich am Zweck von Systembestandteilen. Die verschiedenen Kriterien, anhand derer die Architektur beschrieben wird, schließen sich nicht gegenseitig aus. Sie können vielmehr dazu verwendet werden, verschiedene spezifische Sichten auf dieselbe Software zu beschreiben. Unabhängig davon, welche Sichtweise man einnimmt, und unabhängig davon, ob das Darstellen der Architektur der Konstruktion oder der Analyse dient, sollte eine Architektur stets unter drei Gesichtspunkten geprüft werden, nämlich im Hinblick auf Syntax, Semantik und Strategie. Bei der syntaktischen Prüfung geht es um die Verständlichkeit und die Konsistenz der formalen Darstellung. Wenn diese nicht durchgängig gewährleistet werden, können später eventuell nur Teile der Architektur bearbeitet werden – insbesondere beim Einsatz von Entwicklungswerkzeugen, die das Modell automatisch verarbeiten sollen. Bei der semantischen Prüfung wird untersucht, ob – unter Berücksichtigung des Strukturierungskriteriums – den Komponenten des Modells auch Teile des realen Systems entsprechen. Eine weitere Frage in diesem Zusammenhang lautet, ob das zugrundeliegende Strukturierungskriterium des einzelnen Modells der Geschäftsstrategie genügt. Schließlich sollten mehrere Architekturen auch immer im strategischen Zusammenhang betrachtet werden. Wie oben erwähnt, kann man zu einem System verschiedene Architektursichten beschreiben. Diese Architekturen einzelner Systeme ergeben zusammen eine Gesamtarchitektur, bei der die verschiedenen Systeme – als

Komponenten betrachtet – mehr oder weniger lose gekoppelt sind. Um beurteilen zu können, ob auch diese Gesamtarchitektur der Geschäftsstrategie dient, ist es notwendig, die gegebenenfalls verschiedenen Architektursichten zu vereinheitlichen. Dabei ist es in „gewachsenen“ Systemlandschaften gar nicht so einfach, eine solche einheitliche Sicht zu gewinnen. Versucht man, Systeme mit ungeeigneten Methoden zu strukturieren, führt dies eventuell zu Problemen, die dann gerne der Methode angelastet werden. So wurde jüngst die Modellsicht serviceorientierter Architekturen generell in Frage gestellt, weil viele einschlägige Projekte scheiterten, bei denen bestehende Systeme in eine serviceorientierte Architektur überführt werden sollten. Die Autoren der Berichte kamen zu dem Ergebnis, dass bei den betrachteten Projekten die Probleme aber eher daran lagen, dass dabei versucht wurde, technische SOA-Konzepte auf Gesamtsysteme anzuwenden, die im Hinblick auf die zugrundeliegende Geschäftsstrategie anders strukturiert worden waren. Anstatt die Architekturen zielgerichtet umzubauen, wurde offenbar versucht, die alten Komponenten in Services zu verpacken. Beim Reengineering und bei der Restrukturierung von Architekturen sollte also immer vorab geprüft werden, wie die geschäftsstrategische Ausrichtung der bestehenden Architektur auf diejenige der Zielarchitektur überführt werden kann.

Bewertung

Der Zusammenhang zwischen Strategien, Geschäftsabläufen und Architekturen ist auch in Verwaltungen von Bedeutung. Die Notwendigkeit, effizientes Verwaltungshandeln durch ebenso effiziente Softwaresysteme zu unterstützen, legt es nahe, neben einzelnen Systemarchitekturen auch Gesamtarchitekturen zu betrachten. Dazu müssen zum einen bestehende Systeme analysiert und ihre Modelle im Rahmen einer langfristigen Planung auf eine Zielarchitektur abgebildet werden. Zum anderen muss sich die Architektur neu zu entwickelnder Systeme an dieser Gesamtzielarchitektur orientieren. Im Hinblick auf die langfristige Entwicklung ihrer IT-Landschaften ist es für Verwaltungen also wichtig, ihre Geschäftsstrategie und ihre Zielarchitektur vorausschauend aufeinander abstimmen zu können.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Kollaboration heute und morgen

Viele Köche verderben zwar den Brei, aber manchmal ist es unerlässlich, dass mehrere Beteiligte an einem gemeinsamen Objekt arbeiten. Und das gilt heute auch im Bereich der elektronischen Kommunikation und der elektronischen Dokumente. Dabei wurden bisher diese beiden Facetten der Zusammenarbeit jeweils für sich betrachtet und durch spezifische Werkzeuge unterstützt. Das klassische Instrument der elektronischen Kommunikation, die E-Mail, gehört zu den ältesten Anwendungen vernetzter Computer und hat sich seit seinen Anfangstagen nicht wesentlich weiterentwickelt. Auch andere Kommunikationswerkzeuge ähneln dieser Technik sehr – nur dass sie schneller ablaufen bis hin zum synchronen Austausch einzelner Zeichen im Chat. Die Notwendigkeit, elektronische Post auch länger aufzubewahren, zu kategorisieren und recherchierbar zu machen, hat dazu geführt, dass viele Mailanwendungen heute als das wesentliche Arbeitsmittel im Büro herhalten müssen. Beschränkt sich die Zusammenarbeit in Gruppen nicht allein auf den Austausch von Gedanken und die Verteilung von Dokumenten – als Mailanhang leicht möglich –, sondern will man tatsächlich auch gemeinsam an Dokumenten arbeiten, stößt der Austausch per Mail an seine Grenzen. Schnell werden eine gemeinsame Dateiablage und eine Versionsverwaltung benötigt, die durch Methoden zum ein- und auschecken von Objekten verhindern, dass mehrere Personen gleichzeitig an einem Dokument arbeiten. Ein Klassiker von Anwendungen, die diese Form der Kollaboration ermöglichen, sogenannte Groupware, wird in der Wikipedia als „ein dokumentenorientiertes, verteiltes Datenbanksystem mit sehr enger E-Mail-Anbindung“ bezeichnet. Andere Produkte wie CIRCA oder BSCW sind in Verwaltungen ebenfalls vielfach anzutreffen.

SEMINARE
siehe Seite 44
• MOSS Hands On Seminar
• Kleine und mittlere Projekte in MOSS verwalten

Oft wird aber gerade die Möglichkeit echter paralleler Arbeit benötigt, wenn zeitkritische Aufgaben anstehen und das sequenzielle Arbeiten bzw. das Zusammenführen von verschiedenen Änderungen ihre Erledigung behindern. Allerdings waren bisher die öffentlichen Netze in der Regel nicht leistungsfähig genug, um diese Art der Zusammenarbeit sinnvoll zu ermöglichen. Schon allein die Änderungen, die ein Teammitglied machte, zeitnah – um nicht zu sagen zeitgleich – auf mehreren Rechnern an verschiedenen Orten mitverfolgen zu können, scheiterte mangels ausreichender Bandbreite. Heutzutage erfüllen viele Netze die notwendigen Voraussetzungen, sodass es zahlreiche Anwendungen für die gleichzeitige Bearbeitung von Dokumenten gibt.

Inzwischen geht der Trend bei den Werkzeugen für die elektronische Zusammenarbeit in Richtung einer stärkeren Integration von Kommunikations- und Kollaborationsfunktionen – ergänzt um Koordinationswerkzeuge wie gemeinsame Kalender, Aufgabenlisten und ähnliche. Auch die verschiedenen Kommunikationsformen, die sich unter dem Stichwort „Web 2.0“ entwickelt haben, halten dort Einzug. So kann man z. B. ein Weblog als Projekttagebuch nutzen, das Projektglossar als Wiki anlegen oder Statusmeldungen per Mikroblogging übermitteln. Aus Arbeitsteams, die sich in einfachen Kollaborationsplattformen oft nur in Berechtigungsgruppen widerspiegeln, werden so kleine soziale Netze. Möglich werden solche Arbeitsstrukturen z. B. durch die Integration von Office-Anwendungen mit Kollaborationsdiensten in einem Portal, wie es ein Microsoft Office SharePoint Server, kurz MOSS, zur Verfügung stellt.

Einen Vorgeschmack auf die Zukunft elektronischer Zusammenarbeit gibt Google Wave. Auch wenn sich diese Plattform noch in der Entwicklung befindet und selbst wenn einige der auf der „I/O-Entwicklerkonferenz“ gezeigten Features vielleicht noch vorgegaukelt wären, so scheinen doch schon allein die Ideen hinter Wave dazu geeignet, unsere Vorstellungen von Kollaborationswerkzeugen nachhaltig zu verändern. Das Neue an diesem Konzept ist auf den ersten Blick gar nicht so spektakulär: Die bisher normalerweise vorhandene Trennung zwischen Kommunikations- und Kollaborationsfunktionen wird nahezu aufgehoben. Garniert mit einigen interessanten Zusatzfunktionen wie etwa dem synchronen Übersetzen in andere Sprachen oder einem Playback, mit dem man mehrstufige Änderungen nachvollziehen kann, entsteht ein ganz neuer Eindruck von verteilter Online-Arbeit. Schon bei der Auswahl der Kommunikationsform zeigen sich Unterschiede: Entscheidet man sich normalerweise zwischen E-Mail und Chat, kann nun der Übergang zwischen asynchroner und synchroner Kommunikation fließend sein, und die Nachrichten werden plötzlich zeichenweise sofort übermittelt und nicht erst nach dem expliziten Absenden. Im Stil einer Diskussion in einem Forum können dann die Beteiligten – der Kreis ist durch Einladung dynamisch erweiterbar – an der ursprünglichen Nachricht arbeiten, wobei Änderungen in einer Versionsverwaltung dokumentiert werden. So kann sich jemand, der erst später zu einer Diskussion hinzustößt, die Änderungen in animierter Form vorführen lassen. Auch das dynamische Bereitstellen von Medien – wie es sonst oft über Bilder- oder Videoportale geschieht – ist in das Kollaborationswerkzeug integriert.

Bisher besteht das System aus drei Teilen: einer Webanwendung, einem Protokoll und einer Plattform, die über sogenannte APIs erweiterbar sein soll. So sollen eigene Komponenten in die Kommunikationsstränge integrierbar sein. Als Beispiel wurde ein interaktives Schachspiel in ein Dokument eingebettet. Alle drei Teile von Wave sollen mittelfristig als Open Source zur Verfügung stehen, was nicht nur derartige Entwicklungen befördern kann, sondern auch ermöglicht, dass Firmen und Organisationen ihr eigenes System betreiben können. So können z. B. Dokumente mithilfe von Firewalls geschützt werden, während die übrige Kommunikation mit anderen Installationen grundsätzlich zugelassen wird.

Noch haftet der Präsentation von Wave bei Googles I/O-Entwicklerkonferenz ein wenig das Magische einer Zaubershow an. Man hat auf der einen Seite das Gefühl, alles zu verstehen, und fragt sich zugleich, was wirklich dahintersteckt. Da das Produkt zurzeit auch noch nicht öffentlich verfügbar ist, wird eine Beurteilung der tatsächlichen Fähigkeiten

und der potenziellen Einflüsse auf den Büroalltag noch etwas auf sich warten lassen. Einige Autoren wagen die Prognose, dass es noch fünf bis zehn Jahre dauern wird, bis Wave eine echte Konkurrenz zu etablierten Plattformen wie Lotus Notes oder MOSS darstellen wird.

Bewertung

Wo viele Informationen ausgetauscht werden und tatsächlich gemeinsam an Dokumenten gearbeitet wird, werden zunehmend Kollaborationsdienste Einzug halten – sei es in Form von dezidierten Anwendungen oder von integrierten Arbeitsumgebungen. Neben der dafür notwendigen technisch-organisatorischen Entwicklung, die damit verbunden ist, ist aber – insbesondere für Verwaltungen – die spannendere Frage die nach den arbeitsorganisatorischen Abläufen bzw. Veränderungen. Kollaborationswerkzeuge verleiten dazu, Organisationsgrenzen zu ignorieren. Jeder, der schon Kopien von E-Mails an seine Vorgesetzten verteilt hat, indem er sie „auf Cc: gesetzt" hat, kennt das. In stark hierarchisch strukturierten Organisationen mit scharf abgegrenzten Zuständigkeiten ist diese Art von Kommunikation nur bedingt notwendig oder nicht erwünscht. Große Änderungen in den Arbeitsabläufen von Verwaltungen, wie sie z. B. durch die EU-Dienstleistungsrichtlinie angestoßen werden, und der sich ständig verändernde Umgang mit Informationstechnik über die Generationen werden aber langfristig Einfluss auch auf die Arbeitsweise von Verwaltungen haben. Es steht dem öffentlichen Bereich daher gut zu Gesicht, wenn er sich frühzeitig mit den bereits existierenden und künftigen Möglichkeiten der elektronischen Zusammenarbeit auseinandersetzt, um derartige Werkzeuge sicher, angemessen und zielführend nutzen zu können.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

PRINCE2:2009 – Die Methode früher bekannt als PRINCE

Der Name, den sich ein Künstler gibt, kann Einfluss darauf haben, wie sehr er bei Publikum und Presse im Gespräch bleibt. Im Folgenden soll es aber nicht um den Musiker gehen, der neben dem Namen „Prince" schon viele andere Pseudonyme* benutzt hat. Es geht vielmehr um eine strukturierte Projektmanagementmethode, die 1989 unter dem Namen PRINCE zunächst als britischer Regierungsstandard für IT-Projekte eingeführt wurde. Dabei steht „PRINCE" für „Projects in Controlled Environments". Da sich die Elemente der Methode aber auch auf andere Projekte anwenden lassen, wurde 1996 mit PRINCE2 eine neue Fassung veröffentlicht, die für alle Arten von Projekten geeignet ist. Zuletzt war eine Version aus dem Jahr 2005 gültig, die daher auch mit PRINCE2:2005 bezeichnet wird. Eigentümer des Standards ist das britische Office of Government Commerce, OGC. Inzwischen ist PRINCE2 aber weit über Großbritannien hinaus bekannt und im Einsatz. In Deutschland erfuhr diese Methode in den letzten Jahren immer mehr Interesse. So wurden 2008 fast doppelt so viele PRINCE2-Anwender zertifiziert (s. u.) wie noch ein Jahr zuvor. Zudem ist Mitte des Jahres 2009 nun unter dem Namen „PRINCE2:2009" eine aktualisierte Version von PRINCE2 erschienen. Mit diesem Namen soll zum Ausdruck kommen, dass es sich nicht um eine vollständig neue Version handelt, die grundlegend anderen Prinzipien folgt oder die gegenüber ihrem Vorgänger völlig anders strukturiert ist, wie es beispielsweise der Standard für das IT-Servicemanagement ITIL 3 gegenüber ITIL 2 ist. Ein Ziel der Arbeiten war es vielmehr, PRINCE2 klarer zu strukturieren und praktisch handhabbarer zu machen. Einer der wesentlichen redaktionellen Aspekte bei der Überarbeitung war es, den Inhalt dadurch zu straffen, dass bisher wiederholt beschriebene Dinge nun einmalig an zentraler Stelle dargestellt werden.

* *Eins der Pseudonyme des Musikers lautete „TAFKAP" – ein Akronym für „The Artist Formerly Known As Prince".*

PRINCE2 ist – wie eingangs erwähnt – eine strukturierte Methode für das Projektmanagement. Sie ist prozessbasiert und konzentriert sich auf die Managementbereiche wie Planung, Steuerung, Qualität und Risiken und trennt diese von der fachlichen Aufgabe der Erstellung der im Projekt angestrebten Ergebnisse. PRINCE2 basiert auf den praktischen Erfahrungen aus zahlreichen Projekten, hat aber den Anspruch, mehr zu sein als eine Sammlung guter Beispiele. So wurden als „Leitfaden" für das Projektmanagement sieben Prinzipien definiert, denen ein mit PRINCE2 gemanagtes Projekt während der gesamten Laufzeit folgen soll. Eines dieser Prinzipien ist die Phasenorientierung der Planung und Steuerung eines Projektes – von der Vorbereitung über die Initiierung und mehrere Umsetzungsphasen hin bis zum kontrollierten Abschluss. Die Prozesse von PRINCE2 beschreiben die konkreten Schritte, mit denen in den einzelnen Phasen die Erstellung von Ergebnissen gesteuert wird. Dabei stehen die zu entwickelnden Produkte im Vordergrund und nicht die Dokumente, die im Laufe des Projektes anfallen. Dies war eins der Probleme, mit denen PRINCE2:2005 in der Praxis zu kämpfen hatte: Zahlreiche Projektunterlagen wurden erstellt, weil die Methode es vorschrieb. Die Ideen dahinter wurden nicht richtig deutlich, weil die grundlegenden Prinzipien zwar über den Text verstreut immer wieder einmal erwähnt, aber nicht zusammenhängend vermittelt wurden. Folgerichtig werden in der neuen Fassung die Prinzipien nun direkt nach der Einleitung vorgestellt:

Ausrichtung des Projektes auf geschäftliche Erfordernisse

Bei der Anwendung von PRINCE2 liegt jedem Projekt ein spezifischer Geschäftsplan, englisch „Business Case", zugrunde, der es jederzeit erlaubt zu entscheiden, ob das Projekt noch wünschenswert und realisierbar, sein Ziel erreichbar und das Unterfangen somit wert ist, dass weiter darin investiert wird. Die Fortschreibung dieses Business Case ist daher eins der sieben Themen, die in jeder Phase des Projektes immer wieder bearbeitet werden müssen.

Lernen aus Erfahrungen

Obwohl jedes Projekt einzigartig ist, gibt es immer wieder Erfahrungen, von denen andere Projekte profitieren können. Die Methode verlangt von Projektteams nicht nur, bereits gemachte Erfahrungen zu nutzen, sondern auch ihrerseits Erfahrungen zu dokumentieren und nutzbar zu machen.

Definierte Rollen und Zuständigkeiten

Definierte Rollen und abgestimmte Zuständigkeiten gibt es in nahezu allen Modellen für organisierte und strukturierte Arbeit. PRINCE2 betont die Notwendigkeit, dass in Projektmanagementteams die Interessen des Unternehmens, der Benutzer und der Lieferanten vertreten werden.

Steuerung über Phasen

Die Unterteilung des Projektes in Phasen dient nicht nur seiner zeitlichen und logischen Strukturierung. Durch die Phasen – genauer durch ihre Übergänge – werden Punkte im Ablaufplan definiert, an denen das Projekt geprüft und vom Lenkungsausschuss über seine Fortsetzung entschieden wird. Hierzu wird insbesondere der Business Case herangezogen.

Management nach dem Ausnahmenprinzip

Für Termine, Kosten, Dauer, Qualität, Umfang der geplanten Produkte, Risiken und Nutzen des Projektes werden Toleranzgrenzen definiert. Wenn sich abzeichnet, dass diese Grenzen überschritten werden, muss das nächsthöhere Management eingeschaltet werden, das über das weitere Vorgehen entscheidet.

Fokussierung auf Produkte

„Wichtig ist, was am Ende herauskommt." Daher konzentriert sich PRINCE2 darauf, dass die Produkte und ihre Qualitätsmerkmale beschrieben werden, und darauf, das Projekt so zu steuern, dass die gewünschten Ergebnisse entstehen. Die fachlichen Methoden zur Erstellung der vereinbarten Ergebnisse durch Spezialisten sind nicht Gegenstand von PRINCE2. Hierbei dienen die Entscheidungspunkte

der Phasenübergänge auch dazu festzustellen, ob alle Interessengruppen mit den bisher erzielten Ergebnissen einverstanden sind.

Anpassung an die Projektrahmenbedingungen

Universelle Projektmanagementmethoden müssen in vielen unterschiedlichen Umgebungen und für verschiedene Projekte anwendbar sein, wenn sie ein De-facto-Standard sein wollen. Daher müssen sie mehr beschreiben, als in vielen einzelnen Projekten jeweils von Bedeutung ist. Die konkrete Anpassung der Methode an die Rahmenbedingungen eines spezifischen Projektes – in Anlehnung an das englische „Tayloring", also das maßgenaue Zurechtschneiden der Methode – ist daher ein wichtiger Bestandteil von PRINCE2. Ohne eine derart angemessene Anpassung wird der Aufwand, den die Methode erzeugt, schnell zu groß, und es werden der Form halber Dokumente generiert, anstatt sich – wie gefordert – auf die Ergebnisse zu konzentrieren.

Hat man sich mit den Grundprinzipien von PRINCE2 vertraut gemacht, werden noch sieben Themen präsentiert. Diese ziehen sich durch alle Phasen eines Projektes hindurch und müssen immer wieder bearbeitet werden. Dies dient insbesondere der Einhaltung der Grundprinzipien. Neben dem oben genannten Business Case, der die Frage nach dem Wozu beantworten soll, sind das die Themen Organisation (Wer?), Qualität (Was?), Planung (Wie? Wie viel? Wann?), Risiken (Was, wenn ...?), Änderungen (Wie wirkt sich das aus?) und Fortschritt (Wo sind wir? Wohin geht es? Geht es weiter?).

Nach der Darstellung der Themen folgt dann die Beschreibung der Prozesse. Schon ihre Namen machen deutlich, dass es hier um universelle Managementprozesse geht, die unabhängig von den fachlichen Inhalten und den zu erstellenden Produkten beschrieben sind.

Projekt vorbereiten

Durch die Aktivitäten dieses Prozesses soll sichergestellt werden, dass, schon bevor in das Projekt investiert wird, die oben genannten Grundprinzipien eingehalten werden. Das bedeutet insbesondere, dass das Projekt unter unternehmerischen Gesichtspunkten eine Daseinsberechtigung hat. Dazu muss definiert sein, was das Ziel ist und wer an einer Initialisierung beteiligt sein muss. Die Initialisierungsphase muss geplant werden.

Projekt lenken

Dieser Prozess dient einem Lenkungsausschuss im höheren Management dazu, das Projekt zu starten und zu beenden, es mit übergreifenden Programmen abzustimmen, die notwendigen Phasenentscheidungen zu treffen und sicherzustellen, dass das Projekt weiterhin umsetzbar bleibt. In Abgrenzung zu diesen grundlegenden Aufgaben werden die Aktivitäten der operativen Projektsteuerung – wie etwa die Planung der Aktivitäten – dem Projektmanager überlassen.

Projekt initiieren

In diesem ersten Prozess des operativen Projektmanagements liegt das Augenmerk auf der Vermittlung der konkreten Projektziele und Rahmenbedingungen an alle Beteiligten – und in deren Übereinkunft darüber. Dazu gehören die geschäftliche Grundlage, Nutzen und Risiken sowie der fachliche Inhalt und die Beteiligten des Projektes. Außerdem verständigt man sich darauf, wie Produkte erstellt und Qualitätsziele erreicht, wie Baselines eingerichtet und überwacht oder wie Risiken, Änderungen und der Projektfortschritt verfolgt werden.

Phase steuern

Dies ist der Prozess, in dem die eigentliche Steuerungsarbeit stattfindet. Hier werden die Arbeitspakete für die Produkterstellung beauftragt, ihr Bearbeitungsstatus überwacht und die Ergebnisse entgegengenommen. Auf dieser Basis wird der Gesamtstatus des Projektes analysiert, und Abweichungen von der Planung werden korrigiert. Auch die Berichterstattung an den Lenkungsausschuss ist Bestandteil dieses Prozesses.

Produktlieferung managen

Beim Arbeitsprozess für die Produkterstellung liegt der Fokus auf den Managementaktivitäten. Konkrete Methoden und Techniken der Produkterstellung werden dabei nicht betrachtet. Dementsprechend werden zugewiesene Arbeitspakete angenommen, abgearbeitet, überwacht und schließlich abgeliefert. Auch in diesem Prozess, der die prozessuale Schnittstelle zu Lieferanten darstellt, werden die Dokumente zu den relevanten Themen wie z. B. Risiken, Qualität und Planung fortgeschrieben.

Phasengrenzen managen

Den Phasengrenzen kommt bei PRINCE2 besondere Bedeutung zu, da sie die geplanten Punkte sind, an denen der Lenkungsausschuss über den Status des Projektes und über dessen Fortführung entscheidet. Diese Beurteilung begründet sich aus der weiteren Tragfähigkeit des Geschäftsplans, aus dem aktualisierten Projektplan und aus der Akzeptanz der Risiken. Falls die für das Projekt definierten Toleranzen für die genannten Parameter Kosten, Dauer usw. überschritten werden, veranlasst der Lenkungsausschuss eine Ausnahmeplanung.

Projekt abschließen

PRINCE2 legt Wert auf einen sauberen und definierten Abschluss von Projekten. Dies gilt sowohl für ein geplantes wie auch für ein vorzeitiges Ende. Bei einem geplanten Ende ist es besonders wichtig zu dokumentieren, dass der Projektauftrag erfüllt wurde und dass die vereinbarten Produkte geliefert und akzeptiert wurden. Wird das Projekt vorzeitig beendet, sollen die verwertbaren (Teil-)Ergebnisse gesichert und die Abweichungen von den ursprünglichen Zielen dokumentiert werden. In beiden Fällen werden die vom Projekt belegten Ressourcen wieder freigegeben, und die verwertbaren Ergebnisse werden an den Betrieb bzw. das operative Geschäft übergeben. Im Hinblick auf das Prinzip „Lernen aus Erfahrungen“ ist eine abschließende Evaluierung des Projektes sinnvoll und notwendig. Schließlich wird die Projektdokumentation gesichert, die betroffenen Organisationseinheiten werden über den anstehenden Projektabschluss informiert und dem Lenkungsausschuss wird der Abschluss des Projektes empfohlen. Die hier kurz dargestellten Prinzipien, Themen und Prozesse werden im Handbuch für den Projektmanager detailliert beschrieben, das entsprechend „Managing Successful Projects with PRINCE2“ heißt. Ein weiterer Bestandteil von PRINCE2:2009 ist der Leitfaden für das höhere Management, das in Projekte involviert ist – z. B. im Lenkungsausschuss oder über ein Programmmanagement. Dieser hat den Titel „Directing Successful Projects with PRINCE2“. PRINCE2 bietet Personen, die mit dem Projektmanagement befasst sind, nicht nur Anleitung für die praktische Arbeit, sondern auch die Möglichkeit, sich zertifizieren zu lassen. Dazu gibt es zum einen das Grundlagenexamen, englisch „Foundation Exam“, das „lebenslang“ gilt. Das Expertenexamen für Praktiker, englisch „Practitioner Exam“, muss dagegen alle fünf Jahre aufgefrischt werden. Da auf Basis der bestandenen Prüfungen ausschließlich personenspezifische Zertifikate vergeben werden, können sich Organisationen nicht insgesamt für PRINCE2 zertifizieren lassen. Nichtsdestoweniger ist es für Organisationen wichtig, eine derartige Methode ganzheitlich einzuführen und verbindlich für alle Projekte anzuwenden, um Reibungsverluste zwischen verschiedenen Projekten zu vermeiden, die sonst eventuell verschiedenen Prinzipien folgen oder unterschiedliche Prozesse anwenden.

Bewertung

PRINCE2 ist zunächst einer unter vielen Standards für das Projektmanagement. Er unterscheidet sich von anderen Ansätzen z. B. dadurch, dass er eine vollständige Methode definiert und nicht nur eine Sammlung guter Beispiele darstellt. Ein weiteres Merkmal ist, dass PRINCE2 sich auf die Managementaspekte von Projekten konzentriert und die eigentlichen Produktionstechniken außer Acht lässt. Dadurch ist PRINCE2 zum einen in vielen Branchen einsetzbar, zum anderen eignet sich dieser Standard besonders für E-Government-Projekte in Verwaltungen, da diese nur selten tatsächlich an der Realisierung von Systemen beteiligt sind. Wo das der Fall ist – z. B. bei Anwendungen für sehr spezifische Fachverfahren –, kann der Projektmanagementteil durch eine Metho-

de für die Systementwicklung ergänzt werden. Ein weiterer Vorteil der aufgefrischten Methode wird darin gesehen, dass Integration mit dem inzwischen auch in Verwaltungen weit verbreiteten IT-Servicemanagement nach ITIL, das ebenfalls vom OGC stammt, möglich ist.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

ODF – Open-Document-Format in Verwaltungen

Es gibt zahlreiche Programme, die die Bearbeitung von Texten, Tabellen und Bildern auf dem Computer ermöglichen. Manche davon sind kleine Spezialanwendungen für bestimmte Aufgaben, z. B. das Drucken von Etiketten, andere haben den Anspruch, allgemeine Büroaufgaben zu unterstützen. Solche Büroanwendungen – oder „Office-Programme“ – werden gerne in sogenannten Office-Paketen gebündelt und eventuell auch funktional gekoppelt. Das erlaubt es auf mehr oder weniger einfache Weise, Teildokumente zwischen den Anwendungen auszutauschen und z. B. eine Tabelle in einen Brief einzubinden. Doch nicht immer sind in allen Anwendungen eines solchen Office-Paketes die gleichen Merkmale und Funktionen enthalten, und so kann es schwierig sein, manche Elemente auszutauschen. Dieses Problem verschärft sich in der Regel, wenn man Elemente oder gar ganze Dokumente zwischen den Anwendungen verschiedener Hersteller austauschen will. Die Ursache liegt einerseits darin, dass verschiedene Programme unterschiedliche Fähigkeiten aufweisen, die sich nicht ohne Weiteres portieren lassen. Doch auch wenn man ausschließlich vermeintlich gleiche Funktionen nutzt, erlebt man mitunter böse Überraschungen bei dem Versuch, Dokumente mit einer anderen Anwendung zu öffnen. Andererseits ist die Art und Weise, wie Informationen über die verwendeten Funktionen in den Dokumenten gespeichert werden, verschieden.

Als ein Beispiel dafür, wie unterschiedlich die Art der Beschreibung von Dokumenten ist, kann man einen einfachen Text mit einer Hervorhebung verwenden. In der Sprache für Webseiten, HTML, wird die Information, dass ein Wort fett gedruckt werden soll, explizit in das Dokument geschrieben. Ein entsprechendes Beispiel könnte so aussehen: **Hier wird ein Wort fett gedruckt.** Mit ein wenig Rahmentext, den ein HTML-Dokument benötigt, wird daraus eine kleine Datei von rund 80 Zeichen, die mit einem einfachen Editor lesbar ist. Speichert man dieses Stückchen Text mit einem gängigen Textverarbeitungsprogramm in dessen spezifischem Format ab, werden daraus schnell 20 Kilobyte an Daten, die in einem einfachen Texteditor viele wirre Zeichenfolgen enthalten.

Bedenkt man, welche Möglichkeiten der Formatierung und Gestaltung moderne Textverarbeitungssysteme bieten, wird klar, dass Textdokumente in der Regel sehr viel an spezifischen Steuerungsinformationen enthalten. Und diese werden von anderen Programmen normalerweise nicht verstanden. Abhilfe können Adapter schaffen, die es einer Anwendung erlauben, die spezifischen Steuerungsinformationen anderer Programme auf die eigenen Merkmale abzubilden und so das Dokument entsprechend darzustellen. Bisher war das Interesse der Softwarehersteller aber immer darauf gerichtet, die Konvertierung in das eigene Format zu ermöglichen, die Verwendung der eigenen Dokumente in fremden Anwendungen aber nur bedingt zu unterstützen. Diese Art der „Kundenbindung“ macht die Zusammenarbeit in gemischten Teams manchmal etwas schwierig, wenn nicht alle Teilnehmer zufällig das gleiche Programm verwenden. Um eine tragfähige Lösung für dieses Problem zu finden, wurde im Jahr 2002 eine Organisation gegründet, die ein frei verfügbares Format für Office-Anwendungen definieren sollte. Grundlage der Entwicklung, die in der Sprache XML umgesetzt wurde, war das Format des frei verfügbaren Office-Pakets OpenOffice.org. Seit der Veröffentlichung des Open-Document-Formats, ODF, im Jahr 2005 wur-

de das Format in der Version 1.0 als internationaler Standard mit der Nummer ISO/IEC DIS 26300 freigegeben. Die aktuell gültige Version hat die Nummer 1.1, und es wird an Version 1.2 gearbeitet.

Leider wird anhand dieses Standards deutlich, dass die Festlegung der Formate allein nicht genügt, um Interoperabilität zwischen Anwendungen zu gewährleisten. So gibt es zurzeit einen Streit zwischen der Gemeinschaft, die ODF entwickelt, und einem namhaften Hersteller von Büroanwendungen, da dieser zwar in seinen aktuellen Programmen ODF unterstützt, einige Merkmale aber eigenwillig behandelt. So werden Passwörter von geschützten Dateien nicht abgefragt, sodass der Zugriff auf diese nicht möglich ist. Die Zusammenarbeit mehrerer Autoren an Dokumenten wird erschwert, da Änderungsmarkierungen ignoriert werden. Und die Handhabung von Formeln in einer Anwendung für Tabellenkalkulation entspricht auch nicht den Erwartungen, da an deren Stelle zum Teil nur die letzten berechneten Werte übernommen werden. Auch die Tatsache, dass der Hersteller ein eigenes Format im Eilverfahren hat standardisieren lassen, macht deutlich, dass der durch offene Formate angestrebte Wettbewerb unter den Softwareherstellern von diesen nicht immer gerne gesehen wird. Aber schließlich ist auch gerade dieser Wettbewerb für viele öffentliche Verwaltungen der Antrieb, offene Standards – und insbesondere ein offenes Dokumentenformat – zu fordern und zu fördern. Neben der resultierenden Interoperabilität verspricht man sich davon auch Innovation bei den Anwendungen und eine Verbesserung ihrer Sicherheit. Folglich haben sich seit 2006 auch zahlreiche Regierungen, regionale und kommunale Verwaltungen entschlossen, mehr oder weniger verbindlich das offene Dokumentenformat einzuführen. Neben entsprechenden Empfehlungen bzw. Verordnungen in Belgien, Dänemark, Frankreich, den Niederlanden, Skandinavien und vielen anderen Ländern hat auch der IT-Rat der Bundesregierung beschlossen, ODF schrittweise in der Bundesverwaltung einzusetzen. Bis 2010 sollen Bundesbehörden in der Lage sein, entsprechend formatierte Dokumente zu verarbeiten. Diese Fähigkeit einer Verwaltung ist nicht nur im Hinblick auf die interne Arbeit einzelner Ressorts zu sehen. Auch bei der Zusammenarbeit mit anderen Verwaltungen oder auch mit der Wirtschaft, mit Organisationen sowie mit Bürgerinnen und Bürgern bietet ein offenes Format mehr Flexibilität, wenn an Dokumenten gearbeitet werden können soll.

Für die Hersteller von Office-Anwendungen besteht eine Herausforderung beim Umgang mit ODF darin, für die spezifischen Fähigkeiten der eigenen Programme und die – gewünschten – Innovationen Mittel und Wege zu finden, wie diese in Dokumenten codiert werden können, ohne eigene „Dialekte“ des Standards zu kreieren oder diesen ganz zu zerstören.

Bewertung

Für Verwaltungen bieten offene Dokumentformate mehr Flexibilität beim Austausch von Informationen mit anderen, als vermeintliche Produktstandards dies tun. Ob die Verwendung von ODF anstelle anwendungsspezifischer Formate zu einer Einschränkung der Funktionalitäten in den Programmen führt, hängt davon ab, in welchem Umfang nicht standardkonforme Merkmale tatsächlich genutzt werden. Auch muss im Einzelfall geprüft werden, ob bei der Einführung eines anderen Dokumentformats auch tatsächlich erforderlich ist, ein anderes Office-Paket zu verwenden. In diesem Fall müssen gegebenenfalls Migrationsaufwände auf Seiten des Betriebs und der Benutzer berücksichtigt werden. Dabei wird von Letztgenannten die Umstellung der Arbeitsweise auch häufig dann verlangt, wenn neue Generationen von Anwendungen desselben Herstellers eingeführt werden.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Internet und Web 2.0

Das Netz der Dinge

Während sich der Hype um RFID, Radio Frequency Identification, gelegt hat und die Berichterstattung zu dieser Einzeltechnik nicht nur in Deutschland, sondern auch weltweit zurückgeht, gewinnt ein Thema an Bedeutung, bei dem diese mehr oder weniger kleinen Funketiketten eine wichtige Rolle spielen. Im Netz der Dinge, das in den nächsten 15 bis 20 Jahren entstehen soll, werden nicht nur Computer, Smart-Phones und der heimische Fernseher miteinander vernetzt sein. In den von Forschung und Industrie skizzierten Szenarien kommunizieren auch Autos mit Ampeln oder die Waren im Supermarkt mit uns. So soll beispielsweise das digitale Produktgedächtnis dazu dienen, Informationen über die Entwicklung einer Ware – z. B. die sachgerechte Lagerung – abrufen zu können. Da aber eine Weinflasche normalerweise nicht über einen Netzanschluss verfügt, müssen derartige Informationen auf RFID-Tags untergebracht werden. Der Warenfluss in Produktion und Handel stellt bisher in Fallstudien das Hauptanwendungsgebiet der entsprechenden Techniken dar, da hierbei verschiedene Aspekte der Vernetzung von Dingen verdeutlicht werden können: vom Identifizieren der Objekte über die logistische Lenkung und das Wiederauffinden bis zum Austausch einfacher oder komplexer Informationen mit der Umwelt.

Bevor das Netz der Dinge aber die Labore verlässt und im täglichen Leben Einzug hält, ist noch eine Reihe von Voraussetzungen zu schaffen – ein Prozess, der noch einige Jahre benötigen wird. Wenn zahllose Alltagsgegenstände zu Trägern oder Empfängern digitaler Informationen werden, wird das Datenaufkommen weiter steigen. Verglichen mit der Übertragung von Fernsehfilmen in Datennetzen werden dabei nur kleine Datenpakete ausgetauscht. Die Masse der Objekte – man denke allein an einen gut gefüllten Supermarkt – ist aber nicht zu vernachlässigen. Entsprechend wird im Ausbau von Hochgeschwindigkeitsverbindungen eine wesentliche Voraussetzung für das Funktionieren des Netzes gesehen. Dabei rückt zunehmend der flächendeckende Einsatz von Glasfaserkabeln in den Blick. Allerdings werden für die Umsetzung zehn bis 15 Jahre veranschlagt. So setzt man in den nächsten drei bis vier Jahren auf den verstärkten Ausbau konventioneller Netztechnik mit Kupferkabeln.

Eine weitere Herausforderung bei der Vernetzung besteht auch in der Steuerung der Verbindungen. Dabei müssen nicht nur sehr viele Objekte eindeutig identifiziert werden – dies geschieht anhand des sogenannten „Electronic Product Code“, EPC, – sondern es müssen vor allem zahllose Ad-hoc-Verbindungen hergestellt und verwaltet werden. Von der selbstorganisierenden Kommunikation mit „intelligenten“ Objekten – Smart Items – bis hin zu autonomen Netzen, die sich im Wesentlichen selbst warten, werden aber wohl noch etwa fünf Jahre vergehen. Und schließlich besteht ein weiterer Aspekt der Vernetzung auch in der Interaktion zwischen Objekt und Mensch. Beim Gebrauch von Alltagsgegenständen wird sich der Nutzer in der Regel nicht hinsetzen und bewusst Informationen verarbeiten wollen – schon gar nicht mit Tastatur oder Maus. Der Einsatz von entsprechenden Sensoren und multimodalen Schnittstellen, die verschiedene Kommunikationsformen zulassen, wird also Pflicht in derartigen Szenarien.

Weitere Voraussetzungen ergeben sich aus der benötigten Energieversorgung. Da viele Alltagsdinge nicht über eigene Stromquellen verfügen, muss sichergestellt werden, dass der Energiebedarf für die Vernetzung möglichst gering ist und aus der Umwelt bezogen werden kann.

Darüber hinaus gewinnen wirtschaftlich tragfähige Anwendungen für das „Netz der Dinge“ an Bedeutung. Seit 2004 für reale Praxisstudien die ersten Supermärkte ohne klassischen Kassiervorgang entstanden, wurden Technik und Abläufe weiterentwickelt. Nun muss sich zeigen, dass sich diese auch in – komplexeren – Geschäftsprozessen nutzen lassen. Das Bundesministerium für Bildung und Forschung, BMBF, fördert ein entsprechendes Vorhaben mit über 17 Millionen Euro.

Das Netz der Dinge birgt also zahlreiche Chancen – aber auch Risiken. So reicht es nicht aus, einfache Kommunikationskanäle zu schaffen, um den Missbrauch der Techniken zu vermeiden. Das Netz der Dinge muss vielmehr eine angemessene Sicher-

heitsinfrastruktur bereitstellen. Und so etwas muss von Anfang an in den Entwürfen für eine entsprechende Architektur untergebracht werden, da sich Sicherheit und Datenschutz nur schwerlich im Nachhinein in etablierten Systemen und Abläufen verankern lassen. Dies betont auch der 14 Punkte umfassende Aktionsplan der EU-Kommission, der bei der Entwicklung des Internets der Dinge eine führende Rolle spielen will. Folgerichtig wird dort auch die Frage nach der Governance – also der organisatorisch-operativen Regelung und Steuerung – des Netzes der Dinge gestellt. Die kommenden Jahre müssen zeigen, ob es gelingt, angemessene Maßnahmen für Sicherheit und Datenschutz mit den technischen Möglichkeiten des Netzes der Dinge so zu kombinieren, dass inhaltlich sinnvolle, wirtschaftlich tragfähige und sichere Anwendungen möglich sind.

Bewertung

Die Szenarien aus Produktion und Handel lassen sich nur bedingt auf Verwaltungen übertragen. Nichtsdestoweniger müssen Verwaltungen zahlreiche Objekte steuern – seien es die eigenen Ressourcen für das operative Geschäft oder auch Komponenten von Liegenschaften oder Infrastrukturen, für deren Instand- bzw. Inbetriebhaltung sie zuständig sind. Insofern lassen sich auch im öffentlichen Bereich eigene Anwendungsfälle für das Netz der Dinge entwickeln. Bis man beurteilen kann, welche davon tatsächlich sinnvoll realisierbar sind, werden aber noch weitere Erfahrungen aus Echtanwendungen jenseits der Labore benötigt.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Anarchie im Unternehmen? Enterprise-Wikis

Wer das Wort „Wiki“ liest, denkt häufig zuerst an die Online-Enzyklopädie Wikipedia. Diese Assoziation führt dazu, dass man den Begriff lediglich auf die anhand von Stichwörtern strukturierten Websammlungen reduziert. Dabei bezeichnet ein Wiki ganz allgemein eine Hypertextsammlung, an der – und das ist das Besondere – alle Nutzer direkt mitschreiben können. Ein Wiki kann daher also auch Beiträge zu aktuellen Themen umfassen, kann eine Forumsfunktion für Diskussionen enthalten u. v. m.

Zieht man die allgemeinere Definition von Wiki in Betracht, erscheint es sinnvoller, von Enterprise-Wikis zu sprechen, als wenn man diesen Begriff allein für ein Unternehmens-Glossar verwendet. Als mögliche Anwendungsbereiche werden genannt: eine Wissensbasis z. B. für Best Practices oder zu bekannten Störungen für den Support, Projektdokumentation, Wissenstransfer oder die Begleitung strategischer Prozesse. So gibt es große Konzerne, die über 8.000 Wikis betreiben. Damit die genannten Beispiele und andere Anwendungen im Unternehmen funktionieren, müssen alle Mitarbeiter – oder zumindest viele – bereit sein, implizites Wissen, das in den Köpfen steckt, zu explizitem Teamwissen zu machen, das von allen und jederzeit abrufbar ist. In diesem Fall kann ein Unternehmens-Wiki – als Medium – den Einstieg in Kollaboration erleichtern. Darf man in einem Wiki nur die offiziellen Informationen des Hauses hinterlegen, reduziert sich die Funktion dieses Werkzeuges auf diejenige eines CMS. Zwischen diesen beiden Extremen – auf der einen Seite das allgemeine Wiki, in dem jeder alles darf, auf der anderen Seite das CMS mit streng definierten Workflows, Zuständigkeiten und Genehmigungen – bewegt sich das Unternehmens-Wiki. Ein wesentliches Merkmal besteht darin, dass es über mehr verschiedene Berechtigungen verfügt als ein vollständig offenes Wiki. Das ermöglicht es z. B., auf einer Plattform verschiedene Teil-Wikis zu betreiben, die nur für einzelne Benutzergruppen – etwa Abteilungen – verwendbar sind, innerhalb dieser Gruppen aber die volle Flexibilität eines Wikis bieten. Um das zu gewährleisten, müssen Unternehmens-Wikis gut

SEMINARE
siehe Seite 45
• Wikis - eine Einführung

skalierbar sein. Sie erlauben dann, Rücksicht auf die Unternehmens- und Kommunikationskultur zu nehmen, da nicht immer die vollständige Offenheit aller Informationen gewollt oder möglich ist. Neben der allgemeinen Skepsis gegenüber den auch von Laien frei bearbeitbaren Inhalten ist insbesondere die Angst vor Vandalismus – also dem mutwilligen Zerstören oder Verfälschen von Inhalten – ein häufig geäußertes Bedenken gegen den Einsatz von Wikis. Dem können die Verantwortlichen für Unternehmens-Wikis dadurch begegnen, dass sie ausschließlich die namentliche Änderung von Beiträgen zulassen. Damit vergibt man sich zwar die Chance, auch „Tabuthemen" öffentlich anzusprechen, von denen das Unternehmen sonst eventuell gar nicht erfährt, dass sie kritisch sind, stärkt aber auf der anderen Seite das Vertrauen in die Verlässlichkeit der bereitgestellten Informationen. Daneben ist eine detaillierte Versionsverwaltung, die Änderungen sichtbar machen kann, ein wichtiges Schutzinstrument.

Neben den Softwaresystemen für allgemeine Wikis gibt es inzwischen auch Anwendungspakete, die für den Unternehmenseinsatz bestimmt sind, darunter auch frei zugängliche Open-Source-Produkte. Neben den schon angesprochenen erweiterten Berechtigungskonzepten bieten sie in der Regel auch sogenannte WYSIWYG-Editoren für die Bearbeitung der Beiträge. Dadurch müssen die Mitarbeiter sich nicht mit der Syntax für die Formatierung von Texten befassen, sondern können entsprechend dem Prinzip „what you see is what you get" grafisch arbeiten. Dies ist für die Akzeptanz eines Wikis wichtig – insbesondere in nur wenig technisch geprägten Bereichen.

Bei der Einführung eines Unternehmens-Wikis spielt auch die Frage eine wichtige Rolle, inwieweit es in die bestehende Anwendungslandschaft integriert werden kann. Hier sind zum einen technische Schnittstellen zu bestehenden Anwendungen von Bedeutung, da Dokumente und Informationen übernommen werden sollen. Zum anderen muss man sich aber auch über die logische Anbindung an bzw. Abgrenzung gegen andere Angebote Gedanken machen, um nicht doppelte oder voneinander abweichende Informationen zu haben. Neben diesen grundsätzlichen Überlegungen, wie sich ein Wiki in die Unternehmenslandschaft integrieren lässt, gibt es eine ganze Reihe von praktischen Erfolgsfaktoren, die darüber entscheiden, ob dieser Informationsdienst – und damit verbunden die offene Zusammenarbeit – für das Unternehmen förderlich ist. Dies ist zunächst ein Sponsor im Management, der dafür sorgt, dass die Idee nicht nur geduldet, sondern auch gefördert wird. Desweiteren ist die „kritische Masse" an Koautoren ein wichtiger Faktor. Erst wenn tatsächlich viele Personen an dem Wiki mitarbeiten, kann es sowohl notwendige Breite als auch Tiefe der Informationen erlangen.

Um das zu erreichen, sollten bei der Veröffentlichung des Unternehmens-Wikis bereits eine Reihe von Beiträgen vorhanden sein. Die Änderungsworkflows müssen möglichst einfach sein – gegebenenfalls beschränkt man sich zunächst auf unkritische Themen. Die Werkzeuge für die Bearbeitung müssen möglichst einfach und am besten zusammen mit den Prozessen in einem Nutzerhandbuch beschrieben sein, und schließlich sind ausgewiesene Wiki-„Experten" hilfreich, die die Nutzer bei der Bearbeitung unterstützen und beraten können. Mit der zunehmenden Befüllung eines Wikis wird die Verlinkung der einzelnen Informationen untereinander ein kritischer Faktor. Auch innerhalb eines Wikis sollten Informationen möglichst nicht mehrfach aufgeführt werden, sondern jeweils nur an einer Stelle, und dann per Link erreichbar sein. Schließlich muss man jeweils bedenken, in welchem Maß ein Thema für diese vernetzte und offene Arbeitsweise geeignet ist, bevor man es in das Unternehmens-Wiki aufnimmt. Schon der Datenschutz verbietet es, dass z. B. die Personalabteilung alle ihre Unterlagen in einem offenen Wiki bereitstellt. Auch auf andere Daten sollten nur Gruppen von Personen zugreifen können. Hierfür sollte man dann prüfen, ob man ein separates Gruppen-Wiki aufsetzt oder das Berechtigungssystem des Unternehmens-Wikis entsprechend anwendet. Auch Themen, die viele strukturierte Daten aufweisen, wie etwa das Controlling, können nur bedingt sinnvoll in Wikis abgebildet werden, selbst dann, wenn es für ihre Software entsprechende Funktionsmodule oder Plug-ins gibt. Bei der Einführung von Unternehmens-Wikis ist also ein gewisses Au-

genmaß vonnöten, um auf der einen Seite diesen Ansatz zur Kollaboration nicht bereits im Keim zu ersticken, auf der anderen Seite aber auch nicht zum alles beherrschenden Spielzeug zu machen.

Bewertung

Verwaltungen sind in besonderem Maß hierarchisch organisiert und in Zuständigkeitsbereiche unterteilt; Aufgaben und ihre Erfüllung sind oft detailliert geregelt. Trotzdem sind viele Zuständigkeitsbereiche inhaltlich mit einander vernetzt, sodass Grundlagen- oder Spezialwissen zu einem Thema auch an anderen Stellen verwendet werden kann bzw. muss. Insofern kann es für Verwaltungen durchaus sinnvoll sein, gemeinsame Wissensbasen anzulegen und zu pflegen. Auch für zeitlich begrenzte Aufgaben mit Projektcharakter kann ein Verwaltungs-Wiki das richtige Maß an Flexibilität bieten, um benötigte Informationen bereitzustellen. Eventuell ist es jedoch wichtig, zwischen „amtlichen“ und frei bearbeitbaren Informationen zu unterscheiden, denn nicht immer korrigiert die Autorengemeinschaft fehlerhafte Artikel so schnell, dass man jederzeit blind auf Wikis vertrauen kann. Hier ist es sinnvoll, Technik und Arbeitsweise einfach zu erproben und dann zu prüfen, ob ein Verwaltungs-Wiki im eigenen Bereich eingesetzt werden kann.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Von Twitter, Weblogs und Journalisten

„Der Presse geht es schlecht, und schuld daran ist Web 2.0.“ So könnte das Fazit lauten, wenn man manche Diskussion um den Beitrag neuer Online-Medien zur Presselandschaft zusammenfassen würde. Die Misere fing an, als im Internet die online verfügbaren Publikationen wie Pilze aus dem Boden schossen. Die Werbeagenturen entdeckten diese als günstige Alternative zu den Druckmedien, bei denen ihre Botschaften mit immer geringer werdenden Auflagen an die Leser gebracht wurden. Der aus der Abwanderung von Werbekunden resultierende Kostenzwang bei den Printmedien führte dazu, dass viele traditionsreiche Zeitungen und Zeitschriften aus den Regalen verschwunden sind. Bevor es zu diesen letzten Schritten kommt, werden oft Redaktionen verkleinert und Journalisten durch Hobbyautoren ersetzt. Und von denen gibt es auch immer mehr. Im Stil von Kurzmeldungen, Glossen, Kommentaren oder auch in längeren Artikeln schreiben sie in ihren Weblogs über alles, was ihnen vor die Tastatur kommt – und sei es über einen Artikel in einem anderen Weblog, in einer Zeitung oder über einen Beitrag im Fernsehen. Viele Weblogs sind durchaus flott geschrieben und erfreuen sich daher einer mehr oder weniger großen Leserschaft. Dabei entzieht sich jedoch oft dem Leser, in welchem Maße das Material authentisch ist, inwieweit tatsächlich und selbstständig recherchiert wurde und somit, wie verlässlich ein Beitrag ist. Solange sich ein Autor dabei über „Omas Gartenhäuschen“ auslässt, mögen diese Fragen vernachlässigbar sein. Wenn es jedoch um wichtige öffentliche Ereignisse geht, stehen die Weblogs in Konkurrenz zu den journalistischen Beiträgen in Druckmedien – zumal sie viel zeitnaher und weiträumiger verbreitet werden können als Zeitung oder Zeitschrift. So klagen Journalisten über Weblogs, die ihnen – trotz schlechter Qualität – die Butter vom Brot stehlen und die sie doch gleichzeitig nicht ignorieren können, da Weblogs ja auch wieder Informationsquelle sein können.

Und nun bekommen die klassischen Weblogs ihrerseits Konkurrenz: das sogenannte Mikroblogging – allen voran über den Dienst Twitter. Derartige Dienste beschränken die Länge der einzelnen Bei-

träge auf die Länge einer SMS. Was als Informationsdienst im Privaten konzipiert wurde, um seinen Freunden kurz mitzuteilen, was man gerade tut, hat sich inzwischen zu einem eigenen Nachrichtenkanal entwickelt. Per Webanwendung oder auch über das Handy lassen sich in Sekundenschnelle kurze Nachrichten in alle Welt senden. So verbreiten sich Informationen von der politischen Bühne oder aus den Krisenzentren der Welt inzwischen über Mikroblogs nahezu in Echtzeit. Prominente Beispiele für derartige Berichte, die auch die Schwierigkeiten dieser Art von Berichterstattung deutlich machen, waren die Twitter-Mitteilungen aus der Bundesversammlung, die das Ergebnis der Bundespräsidentenwahl vorweg nahmen. Während man bei diesem Ereignis kurz danach im Fernsehen zur Bestätigung die Vermeldung des Ergebnisses und die Vereidigung des Präsidenten erleben konnte, muss man sich bei Mitteilungen von anderen Schauplätzen fragen, wie verlässlich die Informationen sind – insbesondere dann, wenn keine weiteren Medien von dort verfügbar sind. Aber Geschwindigkeit ist fast alles, und heute gilt mehr denn je: Nichts ist so alt wie die Zeitung bzw. die Meldung von gestern. Und so setzt das Mikroblogging dem traditionellen Journalismus zu – aber nicht ihm ausschließlich. Auch in der Szene der klassischen Blogger wird inzwischen beklagt, dass die Kurzmeldungen qualitativ hochwertige Weblogs von der Beliebtheitsskala verdrängen. Die schnelle Meldung wirft Informationsschnipsel auf den Monitor, und es bleibt dem Leser überlassen, sich aus diesen Schnipseln einen Eindruck zu verschaffen. Anstatt ein mehr oder weniger rundes Bild in Form eines mehr oder weniger gut recherchierten Langartikels von einem einzelnen Verfasser zu bekommen, müssen zunächst die für ein Thema relevanten Autoren gefunden und ihre Nachrichten vom Leser zu einem Gesamtbild kombiniert werden.

Aber auch im Wechselspiel von Mikro- und „Lang"-Blogging gibt es eine zweite Seite der Medaille. Mikroblogging-Dienste werden zunehmend – alternativ oder ergänzend zu RSS-Feeds – dazu verwendet, auf Weblog-Beiträge hinzuweisen – sozusagen ein Appetithappen in Minimalform. Und auch klassische Pressemedien nutzen diesen Weg, über ihre Beiträge zu informieren. Einmal mehr gilt: „Es kommt darauf an, was man daraus macht." Das trifft hier sowohl für Autoren wie auch für Leser zu. Für die einen gilt das im Hinblick auf den bewussten und verantwortlichen Umgang mit den Werkzeugen, für die anderen bezüglich des bewussten und verantwortlichen Umgangs mit den Inhalten.

Bewertung

Verwaltungen zählen zwar nicht zu den klassischen Nachrichtenschreibern. Trotzdem gibt es zahlreiche Informationen, die sie an Bürgerinnen und Bürger vermitteln müssen. Dies kann von der kurzen Mitteilung über geänderte Öffnungszeiten eines Amtes oder aktuelle Berichte zum Fortschritt längerer Vorhaben bis hin zu ausführlichen Hintergrundberichten zu den Auswirkungen von Gesetzesänderungen reichen. In dem Maße, in dem sich die Informationskanäle im Allgemeinen ändern und damit auch die Konsumgewohnheiten von Bürgerinnen und Bürgern, sollten auch Verwaltungen einen entsprechenden Methodenmix für ihre Öffentlichkeitsarbeit in Erwägung ziehen. Dabei ist aber zu berücksichtigen, dass von Veröffentlichungen von Verwaltungen in besonderem Maße Verlässlichkeit erwartet wird. Folglich sollten Verwaltungen derartige Werkzeuge im Rahmen geordneter Kommunikationsprozesse einsetzen.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

„Mail an alle, …" – Semantic E-Mail Addressing

E-Mail ist heute in weiten Kreisen eine der wichtigsten Kommunikationsformen. Dabei müssen sich die Absender und Empfänger von Nachrichten nicht einmal persönlich kennen. Oft ist auch der Grad, in dem ein Absender einer E-Mail ihren Empfänger kennt, von dem Grad verschieden, in dem dieser Empfänger den Absender kennt. So wissen in großen Organisationen in der Regel alle Mitglieder, wen sie ansprechen – bzw. anschreiben – müssen, wenn sie sich mit dem obersten Chef in Verbindung setzen möchten. Umgekehrt weiß dieser Chef nicht immer, wer da gerade versucht, mit ihm Kontakt aufzunehmen. Doch diese unsymmetrische Verteilung kann auch umgekehrt sein. Der Absender von E-Mail an eine Verteilerliste weiß nicht immer, an wen er denn gerade schreibt. Das kann z. B. daran liegen, dass er die einzelnen Adressaten nicht persönlich kennt, wenn diese sich selbst in die Adressenliste eintragen können oder die Liste nicht öffentlich ist. Umgekehrt können die Leser den Verfasser sehr wohl kennen. Die Kommunikation per E-Mail kann zusätzlich dadurch erschwert werden, dass einzelne E-Mail-Adressen, ganze Verteilerlisten oder auch Zuständigkeiten in einer Organisation sich im Lauf der Zeit ändern. Dadurch kann es passieren, dass eine Nachricht zwar die richtige Person, aber nicht die richtige „Funktion" erreicht. Sogenannte Funktionsadressen können zumindest das letztgenannte Problem etwas mildern.

Das Projekt Semantic E-Mail Addressing, SEAmail, der Stanford-Universität möchte einige der Adressierungsprobleme bei E-Mail grundsätzlich lösen. Das Ziel dabei ist es, den Verfasser von E-Mail davon zu entlasten, sich Gedanken über einzelne E-Mail-Adressen machen, oder seine eigenen Verteilerlisten permanent pflegen zu müssen. Dazu soll eine semantische Adressierung dienen, bei der nicht mehr die – vermeintlich – mit einer Person oder auch Funktion verknüpfte Zeichenfolge der entsprechenden E-Mail-Adresse angegeben werden muss. Vielmehr wird hier der Adressat anhand von anderen Merkmalen spezifiziert. Eine solche Spezifikation kann im einfachsten Fall anhand des Namens erfolgen. Das SEAmail-System übersetzt dann diese Beschreibung anhand seines Datenbestandes in eine herkömmliche E-Mail-Adresse. Ist der Datenbestand sehr groß, kann es nötig sein, weitere Merkmale hinzuzufügen, um die Auswahl einzugrenzen. Diese können z. B. ein Wohnort, eine Firma, eine Organisationseinheit oder eine Funktion sein. Umgekehrt kann man auch ganze Gruppen von Personen ansprechen, wenn man sich auf weniger spezifische Merkmale beschränkt. Adressiert man eine Organisationseinheit, verteilt SEAmail die entsprechende Nachricht an ihre Mitglieder. Je mehr Merkmale mit herkömmlichen E-Mail-Adressen verknüpft werden, desto flexibler wird die semantische Adressierung. Werden auch fachliche Zuständigkeiten und besondere Interessen erfasst, könnte z. B. eine Einladung zu einer Veranstaltung an „alle Softwareentwickler, die sich für Web 2.0 interessieren" geschickt werden.

Diese Beispiele machen deutlich, dass SEAmail über einen umfassenden, integrierten und aktuellen Datenbestand verfügen muss, um gleichzeitig möglichst flexibel und treffsicher mit semantisch adressierter E-Mail arbeiten zu können. Innerhalb geschlossener Organisationen können solche Informationen aus den dort vorhandenen Verzeichnissen und Datenbanken kommen, wobei Datenschutz- und Sicherheitsregelungen sowie Bestimmungen zum Schutz der Privatsphäre zu beachten sind. In weniger streng organisierten Umgebungen könnten die Informationen von den Nutzern selbst zur Verfügung gestellt und gepflegt werden. Einmal mehr drängen sich soziale Netze als Datenquellen auf, da dort häufig entsprechende Informationen hinterlegt werden. Auch hier stellt sich die zurzeit viel diskutierte Frage nach der Privatsphäre in solchen Netzen. Eng mit dieser Frage verbunden ist die Problematik von Spam, also unerwünschter Werbemail, die im besten Fall nur lästig ist. Die Verwendung semantischer Adressen eröffnet hier ganz neue Möglichkeiten des zielgenauen Bombardierens mit einschlägigen Produktinformationen.

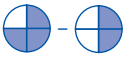
Auf der anderen Seite könnten sich mithilfe von SEAmail-Techniken auch ganz neuartige Filter bauen lassen, die erwünschte und unerwünschte E-Mail voneinander trennen und nicht allein mit E-Mail-

Adressen, Domänennamen und globalen Stichwörtern arbeiten. So ließe sich z. B. das Merkmal „um mehrere Ecken bekannt“ verwenden, um Nachrichten zu akzeptieren: Auch die Bekannten meiner Bekannten dürfen mir Nachrichten schicken. Dieses Prinzip – englisch „Friend of a Friend“, FOAF, – lässt sich über mehrere Stufen ausdehnen.

Das Kombinieren von Merkmalen – sei es zum Aufbauen von semantischen Adressen oder von Filtern – ist nicht unbedingt einfach. Eine vage Vorstellung von einer Zielgruppe gedanklich in eine scharf definierte korrekte Regel aus mehreren Inklusionen und Exklusionen zu übertragen und diese dann textuell zu beschreiben, bedarf etwas Übung. Daher wird vom SEAmail-Projekt vorgeschlagen, anstelle eines Textfeldes, in das die Regel eingetragen wird, ein dialogorientiertes Werkzeug zum Bilden von semantischen Adressen anzubieten. Neben einer solchen Benutzeroberfläche und dem weiter oben genannten Datenbestand benötigt eine SEAmail-Anwendung noch eine E-Mail-Komponente, die den eigentlichen Versand an die einzelnen E-Mail-Adressen übernimmt, und einen Anwendungscode, der den Prozess – von der semantischen Adressierung und der Übersetzung der Adressen bis zum E-Mail-Versand – steuert. Die grundlegenden technischen Voraussetzungen für semantisch adressierte E-Mail sind also nicht sehr umfangreich. Die Voraussetzungen für den praktischen Einsatz sind es dagegen schon: Den Nutzern muss SEAmail möglichst einfach zur Verfügung gestellt werden – am besten integriert in ihre übliche E-Mail-Umgebung. Des Weiteren müssen die notwendigen Daten beschafft und gepflegt werden. Und schließlich müssen die Nutzer im verantwortungsvollen Umgang mit semantischen Adressen geschult werden; gegebenenfalls sind Richtlinien für den Gebrauch einzuführen und technisch zu unterstützen.

Bewertung

Verwaltungen sind in hohem Maß strukturiert und die Zuständigkeiten von Organisationseinheiten und Personen in der Regel scharf definiert. Zudem gibt es in verwaltungsübergreifenden Bereichen oft Gremien und Arbeitsgruppen mit wechselnden Besetzungen. Hier bietet es sich an, elektronische Informationen auf der Basis semantischer E-Mail-Adressierung zu versenden. Die dynamische Generierung der semantischen Adressen hat dabei den großen Vorteil gegenüber statischen Funktionsadressen, dass sie jederzeit aktuell sind – sofern die Basisinformationen zeitnah gepflegt werden. Es ist jedoch nicht zu vernachlässigen, dass mit SEAmail massiv die Nutzungsgewohnheiten für ein Werkzeug verändert werden, das sich inzwischen auch in den nicht technisch ausgerichteten Bereichen der Verwaltung weitgehend etabliert hat. Bevor man daran geht, die technischen Voraussetzungen für den Einsatz zu schaffen, müssen die kritischen Punkte wie Werkzeugintegration, Datenbereitstellung und Nutzerführung bzw. -unterstützung geregelt sein. Zuvor muss SEAmail aber noch beweisen, dass es auch außerhalb des Labors funktioniert.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Technik

Von der Leine gelassen – kabellose Stromübertragung

Das kennt vermutlich jeder, der hin und wieder auf Dienstreisen abends in das Hotel kommt: Man sucht zunächst eine Steckdose, die vermutlich hinter dem Nachttisch oder unter dem obligatorischen Schreibtisch angebracht ist, stöpselt Radiowecker oder Minibar aus, kramt die Netzgeräte von Handy, PDA und Notebook hervor, schließt alles an und hofft, dass man am nächsten Morgen nicht das Gerät hinter dem Nachttisch vergisst. Da erscheint einem das folgende Szenario ein wenig wie Science-Fiction, in der man seine Geräte einfach auf eine markierte Fläche auf besagtem Schreibtisch legt und diese am nächsten Morgen aufgeladen wieder einsteckt. Dieses Szenario könnte in einigen Jahren Realität werden. Zumindest haben sich verschiedene Hersteller aus der Elektroindustrie zusammengetan, um im Wireless Power Consortium Standards für das kabellose Aufladen von Geräten zu entwickeln. Dabei stehen zunächst kleine mobile Geräte wie Handy oder Notebook mit einer Leistungsübertragung von bis zu fünf Watt im Vordergrund. Mittelfristig sollen aber z. B. auch Küchengeräte mit bis zu 100 Watt versorgt werden können. „Und wie soll das gehen?“, fragt man sich und vergisst dabei, dass manche elektrische Zahnbürste diese Technik schon seit Jahren beherrscht.

Das zugrundeliegende Prinzip ist die sogenannte magnetische Induktion. Dabei wird über eine elektrische Spule ein sich stetig änderndes Magnetfeld erzeugt. Bringt man eine weitere Spule als Empfänger in dieses Magnetfeld, wird in ihr ein Strom erzeugt, der dann genutzt werden kann. Jeder übliche Trafo funktioniert auf diese Art. Aber erst jetzt scheint die Technik so weit entwickelt, dass man die engen Grenzen des Trafogehäuses oder der Ladestation für die Zahnbürste verlassen und die Geräte – bis zu einem gewissen Grad – verschieden positionieren kann. Zudem zeigt das Beispiel der elektrischen Zahnbürsten, bei denen jedes Modell eine spezifische Ladestation hat, dass Gerätestandards notwendig sind, wenn man den Wust der Ladegeräte nicht durch eine Sammlung inkompatibler Ladestationen ersetzen möchte, die sich dann eventuell auch noch gegenseitig stören.

Im Labor hat man bereits Leistungen von bis zu 60 Watt über eine Entfernung von rund 80 Zentimetern übertragen können. Es wird jedoch erwartet, dass bis zu marktreifen Produkten noch vier bis fünf Jahre vergehen werden. Und bis die Technik dann auch tatsächlich in Hotels, Konferenzräumen, Büros oder Küchen Normalität ist, wird vermutlich noch einige Zeit vergehen. Doch die Firmen nutzen die Zeit nicht nur, um standardisierte Geräte zu entwickeln, sondern auch Intelligenz darin einzubauen. Auch wenn die technischen Rahmenbedingungen verschiedener Geräte gleich sein mögen, kann der aktuelle Ladezustand des Akkus oder dessen Alter unterschiedliche Ladevorgänge notwendig machen. Indem Ladestation und Gerät nicht nur Energie, sondern auch Informationen austauschen, soll es möglich sein, dass diese individuellen Bedürfnisse berücksichtigt werden.

Ob die kabellose Aufladung von Geräten den Dienstreisenden tatsächlich besser schlafen lässt, muss sich zeigen. Die Entwickler zumindest weisen darauf hin, dass die Magnetfelder in den bisher erzeugten Stärken „höchstwahrscheinlich“ ungefährlich sind. Angesichts intelligenter elektronischer Implantate, die zunehmend in der Medizin verwendet werden, sollte das Restrisiko der Technik vor ihrem massenhaften Einsatz noch minimiert werden.

Bewertung

Für die an einen festen Büroarbeitsplatz gebundene Verwaltungstätigkeit ist die kabellose Stromversorgung nahezu irrelevant. Sicher lässt sich hier mancher Arbeitsplatz etwas ansprechender gestalten, wenn man keinen Kabelsalat mehr hinter dem Schreibtisch hat. Ansonsten gibt es keinen Vorteil. Aber auch Verwaltungsarbeit wird flexibler – sei es räumlich durch ein Handy, das das Bürotelefon abgelöst hat, oder auch organisatorisch durch dynamische Arbeitsgruppen. Dabei wird man für jedes Gerät dankbar sein, das den Aktionsradius nicht auf die Länge des Stromkabels beschränkt oder den Transport von Netzgeräten erfordert.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Mehr Durchblick? Neue Merkmale von Bildschirmen

Der Bildschirm dürfte wohl die wichtigste Komponente am Computerarbeitsplatz sein, und auch in vielen anderen Bereichen – etwa der Unterhaltungselektronik – spielen gute Monitore eine wesentliche Rolle. Nachdem in den letzten Jahren hauptsächlich die Verbesserung der Bildqualität und der Energieeffizienz vorangetrieben wurde, stehen nun zusätzliche Merkmale im Fokus der Entwicklung, die die Rolle des Bildschirms als Maschine-Mensch-Schnittstelle hervorheben. Zum einen werden neue – dreidimensionale – Erlebniswelten erschlossen. Zum anderen wird der Bildschirm auch zunehmend als Eingabemedium verwendet. Und schließlich soll die Produktivität am Arbeitsplatz durch mehrere Bildschirme erhöht werden.

3-D-Bildschirme

Techniken, um auf zweidimensionalen Medien (vermeintlich) dreidimensionale Bilder zu übermitteln, sind bereits mehr als hundert Jahre alt. Die bekannteste davon dürfte darin bestehen, Bilder in Komplementärfarben zu überlagern, die aus etwas unterschiedlichen Winkeln aufgenommen wurden. Diese Anaglyphenbilder können durch die Verwendung von entsprechend eingefärbten Brillen – in der Regel rot und grün – wieder getrennt werden. Das Gehirn des Betrachters setzt sie dann zu einem dreidimensionalen Bild zusammen. Die Methode wurde bereits im Fernsehen und im Kino genutzt und ist auch bei Computeranwendungen zu finden. Da durch die farbigen Filter aber auch andere Farben beeinträchtigt werden, eignet sich dieser Ansatz nur für solche Fälle, in denen die 3-D-Information wichtiger ist als eine mehrfarbige Darstellung. Andere Techniken, die ebenfalls mit Spezialbrillen arbeiten, können auch mit normalen farbigen Bildern umgehen. Dies ist zum einen die Verwendung von Polarisationsfiltern, kurz Polfiltern, auf Bildschirm und Brille. Diese Filter schränken die Richtung ein, in der Licht – als elektromagnetische Welle – schwingt. Wenn man die beiden Teilbilder einer 3-D-Darstellung auf dem Bildschirm mit einem Winkel von 90 Grad zueinander polarisiert, kann man das überlagerte Gesamtbild durch eine Brille mit entsprechend ausgerichteten Polfiltern für das linke und rechte Auge wieder auftrennen. Polfilter sind in der Regel farbneutral und können somit auch für bunte Darstellungen verwendet werden.

Eine weitere Technik mit Spezialbrillen setzt auf die Trägheit des Auges bzw. des Gehirns. Normalerweise kann der Mensch bis zu 25 Bilder pro Sekunde „unterscheiden“ – er nimmt wahr, dass keine kontinuierliche Veränderung, sondern zwischen den einzelnen Bildern eine Unterbrechung stattfindet. Werden mehr Bilder pro Sekunde gezeigt, können vermeintlich fließende Bewegungen dargestellt werden. Kinder kennen diesen Effekt vom „Daumenkino“. Bei Bildschirmen wird diese Technik dadurch realisiert, dass die unterschiedlichen Bilder mit hoher Geschwindigkeit abwechselnd gezeigt werden. Neue Geräte tun dies mit einer Frequenz von 120 Hertz, sodass jedes Teilbild – entsprechend mit der halben Frequenz – immer noch 60-mal pro Sekunde gezeigt wird. Dies liegt weit über der oben genannten Grenze dessen, was der Mensch auflösen kann. Um nun die Bilder für die beiden Augen eines Betrachters wieder trennen zu können, muss dieser eine sogenannte Shutterbrille tragen. Der englische Begriff „Shutter“ bezeichnet einen Rollladen oder auch den Verschluss einer Kamera. Bei der Shutterbrille werden in schneller Folge abwechselnd das linke und das rechte Auge abgedeckt. Erfolgt dies synchron mit dem Wechsel der beiden Teilbilder auf dem Monitor, sieht das linke Auge immer nur das eine Teilbild, das rechte Auge jeweils das andere. Auch hier überlagert das Gehirn die separat empfangenen Bilder zu einem Gesamtbild. Die „Verschlüsse“ in der Brille bestehen aus Flüssigkristallanzeigen, die elektronisch zwischen

durchlässig und undurchlässig hin- und hergeschaltet werden. Auch diese Anzeigen sind farbneutral.

Die bisher genannten Verfahren haben den Nachteil, dass ihre Nutzer jeweils eine Spezialbrille tragen müssen – Rot-Grün-, Polfilter- oder Shutter-Modell. Sogenannte autostereoskopische Verfahren kommen ohne derartige Hilfsmittel aus. Bei ihnen werden die Bilder auf dem Bildschirm derart getrennt, dass die geringfügig unterschiedlichen Positionen des linken und rechten Auges ausreichen, um die Bilder zu trennen. Dazu werden auf dem Bildschirm Raster- oder Linsenfolien aufgebracht, die je nach Betrachtungswinkel eins von zwei – oder auch mehreren – Teilbildern zeigen. Linsenfolien – auch Lentikularfolien – sind ebenfalls von Kinderspielzeugen bekannt, nämlich von „Wackelbildern".

Zu all diesen Techniken wurden zuletzt Anwendungen und Bildschirme für den EDV-Bereich entwickelt und auf den Markt gebracht. Und auch im Kino halten 3-D-Filme zunehmend Einzug. Ein großes Einsatzgebiet für 3-D-Technik sind Unterhaltungsmedien wie Spiele und Filme. Aber auch im Bereich der technischen Konstruktion oder Modellierung finden sich inzwischen ernsthafte Anwendungen.

Doppelbildschirme

Wenn auch nicht durch eine zusätzliche Dimension wie beim 3-D-Bildschirm, lässt sich doch mit einem zusätzlichen Monitor der Blick weiten und die Informationsfülle im PC auf dem Schreibtisch ausbreiten. Mit dem Einsatz eines zweiten Bildschirms soll sich laut mehrerer Studien die Produktivität am normalen Büroarbeitsplatz erheblich steigern lassen. Dabei wurden zum einen Monitore mit Breitbilddarstellung angeführt, und zum anderen sollen vergleichbare Ergebnisse mit mehreren Bildschirmen zu erzielen sein. Dass eine der Untersuchungen von einer amerikanischen Universität zusammen mit einem Hersteller von Bildschirmen durchgeführt wurde, mag Einfluss auf die Ergebnisse gahabt haben. Auffällig ist aber, dass gerade im Notebook-Bereich Anstrengungen unternommen werden, auch unterwegs für mehr „Weitblick" zu sorgen. Während der klassische Zweitmonitor am stationären Arbeitsplatz nicht mehr so außergewöhnlich ist, seit die Preise für Bildschirme – insbesondere platzsparende LCD-Versionen – deutlich gesunken sind, müssen sich die Hersteller mobiler Technik schon einiges einfallen lassen, um das zusätzliche Display auf die Reise zu schicken. Dabei gibt es verschiedene Varianten, wie dies bewerkstelligt wird. Die erste Variante mutet zunächst eher wie ein Gimmick an – ein bedingt nützliches Spielzeug, das lediglich einen Kaufanreiz darstellt: In dem 10-Zoll-Notebook ist im Touchpanel, über das der Mauszeiger bedient werden kann, eine vier Zoll große Anzeige untergebracht. Dieser Minibildschirm hat dabei immerhin eine Auflösung von 854 x 480 Bildpunkten. Für die zusätzliche Büroarbeit ist der Winzling aber trotzdem nicht geeignet. So besteht eine Idee des Herstellers auch vielmehr darin, spezialisierte Eingabeinstrumente auf dem Display darzustellen, die über die berührungsempfindliche Oberfläche bedient werden können. Dies können Spezialtastaturen – etwa für einen Taschenrechner oder für Musikinstrumente – sein, eine „Shortcut"-Liste oder auch das Bedienelement für ein elektronisches Buch. Dass die Minianzeige an die Taschenausgabe von Spielekonsolen erinnert, legt nahe, dort auch entsprechende Spiele unterzubringen.

Die zweite Variante des Zusatzbildschirms besteht darin, ein etwas kleineres Display im 17-Zoll-Hauptbildschirm unterzubringen, das bei Bedarf herausgezogen werden kann. Dabei stellt die 10,6 Zoll große Anzeige sicher keinen vollwertigen Zweitbildschirm dar. Trotzdem lassen sich dort die Fenster von kleineren Anwendungen sinnvoll unterbringen.

Einen Schritt weiter geht ein Hersteller, der seinen Notebooks jeweils zwei gleiche Bildschirme mitgibt. Diese befinden sich in geschlossenem Zustand hintereinander und können dann so geschoben werden, dass ein Arbeitsplatz mit zwei nebeneinander liegenden Monitoren entsteht. Avisiert sind ein Notebook mit zwei 15,4-Zoll-Bildschirmen bzw. mit zweimal 13,3 Zoll. Am Markt verfügbar sind diese Rechner jedoch noch nicht.

Angesichts der verschiedenen Lösungen für mehr Bildschirme am Arbeitsplatz lohnt es sich, zunächst einen Blick auf mögliche Anwendungsszenarien zu

werfen, bevor man in zusätzliche Büroausstattung investiert: Ein wesentliches Kriterium bei der Entscheidungsfindung dürfte es sein, ob man Spezialanwendungen betreibt, die allein schon den Einsatz eines zweiten Bildschirms erfordern oder zumindest nahelegen. Dies können zum einen Anwendungen für die grafische Datenverarbeitung sein, die große, qualitativ hochwertige Bildschirme benötigen, oder Anwendungen für die Konstruktion. Zum anderen können dies Anwendungen mit vielen Einzelinformationen sein, die parallel oder im schnellen Wechsel darstellbar sein müssen. Beispiele dafür sind Überwachungssysteme, Anwendungen für das Finanzcontrolling oder Softwareentwicklungsumgebungen. Diese letztgenannten Beispiele geben auch Hinweise auf Szenarien, in denen zwei Bildschirme im „normalen" Büroalltag förderlich sein können.

Wenn häufig Informationen aus verschiedenen Quellen gleichzeitig verarbeitet werden müssen und der Wechsel zwischen verschiedenen Anwendungen oder verschiedenen Dokumenten zur Suche nach dem richtigen Fenster wird, bietet sich der erweiterte Monitor an. Am stationären Arbeitsplatz lassen sich entsprechende Lösungen oft mit der vorhandenen Technik realisieren, da viele Grafikkarten in der Lage sind, zwei Bildschirme anzusteuern. Spezielle Karten erlauben sogar den Betrieb von bis zu vier Monitoren. Welche Geräte man einsetzt, hängt dann auch noch davon ab, ob die verschiedenen darzustellenden Informationen aus unterschiedlichen Anwendungen kommen oder anderweitig unabhängig voneinander sind. In diesem Fall können Größe und Ausstattung der Bildschirme eventuell verschieden sein. Sollen die Bildschirme eine homogene Arbeitsoberfläche ergeben, empfiehlt es sich, baugleiche Geräte mit möglichst schmalen Rändern zu verwenden und diese direkt nebeneinander zu positionieren. Ob in allen Fällen die Produktivität tatsächlich gesteigert werden kann, scheint zweifelhaft. Die Verlockung, auf einem der Monitore immer sein E-Mail-Postfach zu verfolgen, scheint groß – auch wenn viele Arbeitspsychologen und Organisationsgurus empfehlen, das Mailprogramm auch einmal zu schließen, da der ständige Blick darauf nur für Ablenkung sorgt und somit die Produktivität negativ beeinflusst.

Umfrage

Folgende Frage wurde in einem Netzwerk gestellt: „Steigern zwei Bildschirme am normalen Büroarbeitsplatz tatsächlich die Produktivität? Wer hat Erfahrungen?"

Diese nicht repräsentative Umfrage lieferte 41 Antworten – 39 davon binnen eines halben Tages. Die überwiegende Zahl der Antworten (34) fiel positiv aus, wobei zum Teil Erfahrungen mit konkreten Anwendungen geliefert wurden. Insbesondere bei der manuellen Übertragung von Daten (z. B. aus Faxen) und beim Datenabgleich zwischen verschiedenen Dokumenten halten diese Personen den zweiten Bildschirm für sehr hilfreich. Ein weiteres Anwendungsgebiet betrifft die parallele Arbeit an Dokumenten und technischen Systemen bzw. Fachanwendungen.

Sechs Befragte konnten entweder keinen Zusammenhang mit der Produktivität erkennen oder schlugen lediglich als Alternative einen einzelnen, entsprechend großen Monitor vor.

Eine kritische Stimme merkte an, dass mehr Platz auch zu mehr Hast und verbunden damit zu einer negativen Entwicklung führe.

Bildschirme mit Berührungseingabe

Eine weitere Entwicklung am Markt stellen „Bildschirme mit Berührungseingabe" – englisch „Touch Screens" – dar. Die zugrundeliegenden Konzepte und auch Techniken liegen seit Jahren vor, drängen aber nun verstärkt auf den Markt. Der Bildschirm als bidirektionale Schnittstelle zwischen Mensch und Computer hat mit der Verbreitung entsprechender PDAs und Smart Phones sein Nischendasein für Spezialanwendungen – etwa die Maschinenüberwachung und -steuerung – schon vor einiger Zeit beendet und ist lautlos zum Massenphänomen geworden. Zusätzlichen Schwung erhält das Thema durch neue Möglichkeiten der Interaktion – die sogenannte Gestensteuerung. Diese ermöglicht es, auf dem Bild-

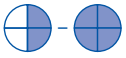
schirm nicht nur jeweils einen Punkt zu steuern, sondern gleichzeitig mehrere Koordinaten zu nutzen. So lassen sich z. B. Objekte auf dem Bildschirm durch eine Kreisbewegung mit zwei Fingern drehen oder durch das Zusammen- bzw. Auseinanderziehen der Finger verkleinern respektive vergrößern. Möglich wird das insbesondere durch sogenannte kapazitive Touchscreens. Diese besitzen eine beschichtete Oberfläche, auf denen ein gleichmäßiges elektrisches Feld erzeugt wird. Berührt man dieses mit den Fingern, können kleine Ströme gemessen werden, aus denen die berührten Koordinaten ermittelt werden. Da hier für die Eingabe keine Hilfsmittel wie Stifte verwendet werden können, gilt diese Technik als nicht barrierefrei. Klassische resistive Touchscreens dagegen reagieren lediglich auf Druck – z. B. auch mit einem Stift – und verbinden dann zwei dünne leitende Schichten miteinander. Die resultierenden Spannungsänderungen lassen allerdings nur die Ermittlung einer Koordinate zu.

Neben kleinformatigen Touchscreens für Smart Phones werden nun auch größere entwickelt – etwa für die Geräte zum Lesen elektronischer Bücher, sogenannte E-Books. Noch einige Nummern größer können Touchscreens auch für Präsentationswände oder in Tischform als Arbeitsunterlage genutzt werden. Die letzten Computermessen zeigten zahlreiche Varianten davon. Bei diesen Bildschirmen werden die „Eingaben“ von der Rückseite her mit Kameras erfasst. Dies erfordert zwar auf der einen Seite viel Platz, erlaubt aber auch, neben den reinen Koordinaten noch verschiedene Objekte auf der Oberfläche zu erkennen. So können z. B. Karten mit definierten Mustern auf der Rückseite so auf den Bildschirm gelegt oder daran geheftet werden, dass die Anwendung verschiedene Inhalte den einzelnen Positionen zuordnen kann.

Neben den genannten Spezialanwendungen in spezifischen Umfeldern wie einer Werkshalle und dem Masseneinsatz von Touchscreens bei mobilen Endgeräten, die neben Stifteingabe und Mikrotastatur kaum andere Bedienelemente zulassen, müssen die neuen Möglichkeiten, die berührungsempfindliche Bildschirme bieten, erst noch für den Computeralltag erschlossen werden. Im Büro drängt sich die Eingabe auf dem Bildschirm nicht direkt auf, und auch die Notwendigkeit der Gestensteuerung liegt nicht auf der Hand. Diese Sicht mag aber von lange geübten Arbeitsmustern geprägt sein. Großbildschirme, die gleichzeitig von mehreren Personen und Objekten „bedient“ werden können, haben vielleicht noch am ehesten das Potenzial, die etablierten Sichtweisen aufzubrechen. Ob sich daraus ernsthafte Anwendungen – insbesondere für den normalen Arbeitsplatz – entwickeln, bleibt abzuwarten.

Bewertung

Der Bildschirm als das wichtigste Element der Maschine-Mensch-Schnittstelle wird in den kommenden Jahren weiter an Bedeutung gewinnen, da er diejenige Stelle ist, an der die sich weiter verstärkende Informationsflut sichtbar – und gegebenenfalls auch bedienbar – wird. Dies legen aktuelle technische Entwicklungen nahe. Bisher sieht es so aus, als ob diese Entwicklungen auf Speziallösungen abzielen. Die klassische Verwaltung könnte am ehesten vom Einsatz von Doppelbildschirmen profitieren, der der zunehmenden Digitalisierung des Büroalltags – in Office- und Fachanwendungen – Rechnung tragen würde. Da es aber im gesamten öffentlichen Bereich eine Vielzahl von verschiedenen Arbeitsplätzen mit unterschiedlichen Anforderungen an eine optimierte Maschine-Mensch-Kommunikation gibt, muss im Einzelfall geprüft werden, ob die neuen Möglichkeiten, die moderne Bildschirmsysteme bieten, dazu beitragen können, die Produktivität zu verbessern.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Blättern oder Scrollen – Elektronische Bücher

Schon seit mehreren Jahren wird immer wieder das Ende des klassischen Buches vorhergesagt. Elektronische Bücher, sogenannte E-Books, sollen die Alternative zu gedruckten Ausgaben darstellen. Ihre weite Verbreitung könnte eventuell sogar den Buchhandel aus der Geschäftswelt verschwinden lassen, da der Vertrieb dann ebenfalls auf elektronischem Weg erfolgen würde. Die Anhänger echter Bücher halten dagegen, dass beim elektronischen Verschnitt nicht alle Sinne angesprochen werden; insbesondere das haptische Erleben – also das Fühlen von Größe, Struktur, Gewicht usw. – bliebe auf der Strecke. Auch ist immer wieder zu hören, dass das Lesen am Bildschirm als anstrengend empfunden wird. Diese beiden Punkte machen deutlich, dass der Qualität der Geräte, auf denen E-Books gelesen werden sollen, eine besondere Bedeutung zukommt. Neben PDAs und normalen Arbeitsplatzcomputern sind es vor allem spezifisch zum Lesen von E-Books entwickelte Geräte, E-Book-Reader, die dem elektronischen Medium zum endgültigen Durchbruch verhelfen sollen. In puncto Bedienung sind aber auch diesen Geräten klare Grenzen gesetzt – zumindest was das Nachahmen der haptisch wahrnehmbaren Eigenschaften von Büchern betrifft. Es gibt zwar Geräte, bei denen man per Gestensteuerung auf dem Bildschirm „umblättern“ kann, allerdings setzen die meisten Geräte auf herkömmliche Elemente einer Benutzerschnittstelle wie spezielle Tasten oder einfache Elemente auf dem Touchscreen. Ansonsten werben die Hersteller mit geringen Abmessungen und leichtem Gewicht, verbunden mit der Möglichkeit, bis zu 1.000 Bücher gleichzeitig mit sich herumzutragen. Damit wird das Lesegerät dann schnell zu einem echten Wertgegenstand, denn auch wenn es eine ganze Reihe von kostenlosen E-Books gibt, kommen außer den 250 bis 400 Euro für ein Lesegerät noch erhebliche Zusatzkosten auf den Nutzer zu, wenn er das Gerät mit aktuellen Titeln füllen möchte.

Der zweite der angesprochenen kritischen Punkte für E-Book-Reader ist die Qualität der Darstellung. Wer schon einmal mit einem Notebook in der Sonne gesessen oder im Sommer versucht hat, auf seinem Handy eine Telefonnummer zu lesen, weiß, dass allein schon Helligkeit und Kontrast der Anzeige zwei Größen sind, die bei mobilen Geräten nur bei geeigneter Beleuchtung befriedigende Werte erreichen. Auch die Schärfe der Darstellung ist oft für längeres entspanntes Lesen nicht ausreichend. Diesen Herausforderungen begegnen einige Hersteller mit der Verwendung sogenannter elektronischer Tinte bzw. elektronischen Papiers (⇨ HZD-Trendbericht 2003). Derart hergestellte Bildschirme erlauben eine sehr klare schwarz-weiße Darstellung mit sehr hohem Kontrast, die auch in heller Umgebung gut zu lesen ist. Allerdings benötigen sie auch ein Mindestmaß an Helligkeit, denn sie arbeiten ausschließlich mit indirekter Beleuchtung.

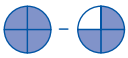
Angeboten oder vertrieben werden viele E-Book-Reader von Verlagen oder Buchhändlern, die zum Teil eigene Dokumentformate verwenden und ihre Bücher über digitales Rechtemanagement gegen unerlaubte Weitergabe schützen. So entsteht eine gewisse Abhängigkeit des Lesers von Verlag bzw. Händler, die es bei gedruckten Büchern in der Form nicht gibt. Deutlich wird diese Abhängigkeit an einer aktuellen juristischen Auseinandersetzung, die damit endete, dass ein Buchhändler seinen Kunden eine Entschädigung zahlte, weil er ungefragt E-Books von ihren Lesegeräten gelöscht hatte. Dabei waren jedoch nicht nur die Bücher, für die der Lieferant nicht die nötigen Rechte besessen hatte, gelöscht worden, sondern auch die elektronischen Notizen eines Lesers, die er auf dem Gerät zu dem Buch gemacht hatte.

Auch wenn zunehmend mehr und bessere Geräte zum Lesen von E-Books auf den Markt kommen und zu immer mehr Büchern auch elektronische Fassungen erscheinen, trifft man noch immer auf ein hohes Maß an Skepsis gegenüber dieser Technik. Ob künftig das elektronische Buch oder das gedruckte Buch zum Nischenprodukt – mit oder ohne Kultstatus – wird, zeigt sich erst in einigen Jahren.

Bewertung

Für Verwaltungen sind E-Books aus zweierlei Perspektiven interessant – zum einen aus der des Erzeugers von Informationen und zum anderen der des

Konsumenten. Für Verwaltungen ist es inzwischen schon in vielen Fällen üblich, schriftliche Informationen zusätzlich in ansprechender elektronischer Form herauszugeben. Ob dies in Zukunft auch für umfangreiche Informationen der ausschließliche Weg der Verteilung sein kann, hängt davon ab, in welchem Maß geeignete Lesegeräte bei den Adressaten vorausgesetzt werden können. Gegebenenfalls kann hier in Kombination mit „Buchdruck auf Anforderung“ ein kostengünstiger Vertriebsweg gefunden werden. Für Verwaltungen als Konsumenten von E-Books zeichnen sich kaum große spezifische Szenarien ab, die die massenhafte Anschaffung von speziellen E-Book-Readern sinnvoll machen. Sofern Bücher nicht für isolierte Zwecke wie Fortbildung genutzt werden, stehen die entsprechenden Informationen in der Regel im Zusammenhang mit der normalen Arbeit. Hierbei dürfte der parallele Zugriff auf das E-Book einerseits und auf weitere elektronische Informationen andererseits vom normalen Computerarbeitsplatz aus der bessere Weg sein. Nichtsdestoweniger müssen Verwaltungen beobachten, wie sich der Markt für E-Books und die für sie relevante Fachliteratur weiterentwickelt.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Für solide Arbeit: SSD statt Festplatte

Welche Bedeutung es für die tägliche Arbeit hat, wenn man die Früchte seines Tuns dauerhaft abspeichern kann, weiß man spätestens dann, wenn sie sich bei einem Stromausfall einmal aus dem „Gedächtnis“ des Computers verflüchtigt haben, ohne dass sie vorher gesichert waren. Grundlegende Techniken für eine dauerhafte Speicherung in der IT gibt es inzwischen viele. Sie reichen vom Magnetband über Magnet- und optische Platten bis zu Speicherchips und holographischen Speichern – Lochkarten u. Ä. spielen heute keine große Rolle mehr. Innerhalb dieser Technikgruppen gibt es wiederum jeweils verschiedene Spielarten. Man denke allein an den jüngsten Streit um die beste Technik für die „Blu-ray-Disc“. Jede dieser grundlegenden Techniken hat – oder hatte – in ihrer Zeit gewisse Vor- und Nachteile, die sie ihren Platz im Spannungsdreieck zwischen Größe, Geschwindigkeit und Kosten des Speichers finden lassen. Trotzdem verschwinden manche Technikvarianten, die vorübergehend als besonders pfiffig galten, wieder sang- und klanglos von der Bildfläche. So waren Wechselplatten für PCs mit Speicherkapazitäten um 100 Megabyte in den neunziger Jahren für kurze Zeit sehr populär, wurden dann aber sehr schnell durch beschreibbare CDs verdrängt.

Nun zeichnet sich seit einiger Zeit ein erneuter Wechsel bei den grundlegenden Techniken – zumindest für breite Einsatzgebiete – ab: Industrie und Marktbeobachter erwarten, dass die klassischen magnetischen Festplatten in absehbarer Zeit von sogenannten Solid State Disks, SSDs, abgelöst werden, bei denen die Daten auf Speicherchips abgelegt werden. Dabei führt der Name – und insbesondere auch die Variante „Solid State Drive“ – eigentlich auf eine falsche Spur, denn die Chips befinden sich nicht auf einer (rotierenden) Platte. SSDs kommen ohne bewegliche Teile aus, was sie gegenüber Festplatten deutlich robuster macht, deutlich kürzere Zugriffszeiten ermöglicht und schließlich den Energieverbrauch sowie die Geräuschentwicklung senkt. Der Name ist vielmehr in der Tatsache begründet, dass sich SSDs „wie Festplatten“ verwenden lassen. Das bedeutet, dass sie vom Computer entsprechend an-

gesteuert werden können. Dadurch sind sie bei der Datenübermittlung auch schneller als herkömmliche Speicherkarten oder USB-Sticks. Einen wesentlichen Beitrag zur Leistungsfähigkeit des Speichermediums kann der Controller leisten, der die Ansteuerung der Speicherchips regelt. So kann dieser z. B. selbst über einen Zwischenspeicher, den sogenannten Cache, verfügen, der zu schreibende oder zu lesende Daten in „flüchtigen" Chips ablegt, die ohne Stromversorgung die Informationen wieder verlieren. Die Chips für die nicht flüchtige – sprich dauerhafte – Speicherung sind heute in der Regel Flash-Speicher, die ihren Inhalt auch ohne Stromversorgung behalten können. Dabei geht man von Speicherfristen von bis zu zehn Jahren aus. Andere SSDs werden mit SDRAM bestückt, das über eine Batterie mit Strom versorgt werden muss, wenn der Computer ausgeschaltet ist. Da dies aber den Energiebedarf erhöht, erhalten die Flash-Speicher normalerweise den Vorzug, auch wenn SDRAM schneller ist. Schließlich sind mobile Geräte ein wichtiger Einsatzbereich für SSDs, die nicht nur kompakt und leicht, sondern eben auch möglichst lange unabhängig vom Stromnetz sein sollen. Mit Kapazitäten von bis zu zwei Terabyte und Lese- und Schreibgeschwindigkeiten von bis zu 250 MB/s werden SSDs aber auch schon im Serverbereich eingesetzt. Und ihre Verwendung in großen Speicherarrays wird ebenfalls vorangetrieben.

Neben den reinen SSDs werden auch Mischformen eingesetzt, bei denen Speicherchips und magnetische Platten kombiniert werden, sogenannte Hybridplatten. Während man dabei die Vorteile bei der Energieeffizienz, bei Gewicht und Geräuschentwicklung wieder verliert, kann man die Geschwindigkeitsvorteile fast vollständig nutzen und mit dem Preisvorteil von Festplatten kombinieren, die bisher noch ein deutlich günstigeres Verhältnis von Kosten pro Speicherkapazität haben als Chips. Der Trick besteht darin, häufig benötigte Daten in den Chips zu speichern, während selten verwendete Daten auf der Festplatte lagern. Dieses Prinzip macht zum einen deutlich, dass man bei der Auswahl einer konkreten Technik die tatsächliche Nutzung seiner Daten im Auge haben muss. Zum anderen zeigt es, dass Aussagen über maximale Datenraten nur bedingt etwas über die Leistungsfähigkeit eines Speichers sagen und man die durchschnittlichen Zugriffszeiten beachten sollte.

Bewertung

Es ist noch gar nicht so lange her, dass wir dachten, eine Festplatte mit einem Gigabyte Kapazität würde ein Leben lang halten. Doch immer wieder schaffen wir es auch, die größten Datenträger vollständig zu belegen, und warten darauf, dass die nächste Größenordnung zum erschwinglichen Standard wird. Auch in den Verwaltungen fallen immer mehr elektronische Daten an, und mit der gespeicherten Datenmenge wächst auch die Notwendigkeit, auf diese schnell zugreifen zu können. In den meisten Fällen wird man allerdings warten können, bis Solid State Disks Standardkomponenten in Rechnern und Speicherarrays geworden sind. Ob man in Einzelfällen gezielt auf diese Technik umstellt, muss man jeweils im spezifischen Kontext untersuchen – z. B. wenn beim mobilen Arbeiten große Datenmengen verarbeitet werden müssen oder die Laufzeit des Akkus ein kritischer Faktor ist. In diesem Fall muss man dann aber auch prüfen, welche konkrete Ausprägung der Technik die speziellen Anforderungen tatsächlich erfüllt.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Programmierung und Software

Ware als Dienstleistung – SaaS

Software ist eigentlich etwas Immaterielles. Wenn sie verwendet wird, ist sie nur in Form von Elektronen, die sich durch Rechner und Leitungen bewegen, und von Zuständen in den Speichern vorhanden. Im täglichen Leben wird sie oft lediglich durch eine Schachtel repräsentiert, die einen oder mehrere Datenträger sowie ein mehr oder weniger umfangreiches Handbuch enthält. Bezieht man die Software über ein Netz, hat man oft nicht mehr in der Hand als einen Lizenzschlüssel – und auch der kommt in elektronischer Form. Im Betrieb „materialisiert" sich die Software eigentlich nur in der Hardware, die man benötigt, um sie zu verwenden. Schon angesichts dieser Überlegungen hat Software an sich mehr von einem Dienst als von einer Ware. Wenn heute von „Software as a Service", SaaS, die Rede ist, werden diese Gedanken noch weiterentwickelt. Hier verbleiben auch die wesentlichen Hardwarekomponenten, auf denen die Software zum Leben erweckt – sprich betrieben – wird, bei einem Lieferanten. Der Anwender bedient sich lediglich der Funktionen über ein Netz.

Für SaaS gibt es zwei technische Grundmodelle: Entweder wird die Software über eine Terminalanwendung genutzt oder per Webbrowser. Der erste Ansatz eignet sich eher für geschlossene Benutzerkreise – etwa innerhalb eines Unternehmens oder einer Verwaltung. Der zweite Ansatz bietet insbesondere die Möglichkeit, Software per Internet zur Verfügung zu stellen. In einigen Definitionen von SaaS werden ausschließlich diese letztgenannten Szenarien berücksichtigt. In beiden Fällen besteht die Motivation für den Einsatz von SaaS aber darin, Software bzw. die entsprechenden Dienste kostengünstig bereitstellen zu können. Indem Hardware, Betriebspersonal und Know-how zentral vorgehalten werden, sind die Anwender davon befreit, neue Versionen von Software zu beschaffen, sie zu installieren und zu betreiben. Ausfälle von Hardware und Softwarefehler werden ebenfalls zentral beseitigt, und im Idealfall merken die Anwender nicht einmal, dass es eine Störung gab. Zudem lässt sich die Software überall dort nutzen, wo ein entsprechender Netzzugang vorhanden ist. Schließlich lassen sich auch solche Preismodelle einfach verwirklichen, die auf der tatsächlichen Nutzung basieren – sei es bezüglich der Anzahl der Nutzer oder der Nutzungszeiträume – und nicht auf der Zahl installierter Lizenzen bzw. potenzieller Nutzer.

Für die Anbieter von Software ergeben sich neue, erweiterte Geschäftsmodelle: Sie werden in die Lage versetzt, nicht nur Lizenzen und Pflegeleistungen zu verkaufen, sondern auch noch den Betrieb. Dafür müssen sie zwar die Aufwände für die entsprechende Infrastruktur und die Dienste – Server, Datenhaltung, Energie, Sicherheit, Support usw. – tragen, haben auf der anderen Seite aber auch einen sehr direkten Draht zu den tatsächlichen Nutzern.

Schließlich stellt SaaS auch noch ein Geschäftsmodell für reine Dienstleister dar, die zwar ihrerseits die Anwendungen lizenzieren müssen, dann aber für Kunden den Betrieb übernehmen. Dieses Modell ist zum einen für Nutzer interessant, die den Betriebsaufwand selbst nicht leisten können oder wollen. Zum anderen bietet es sich für Organisationen an, die ihre IT-Dienstleistungen möglichst weitgehend an zentraler Stelle bündeln wollen – sei es in einem eigenen Bereich oder bei einem externen Dienstleister.

Unabhängig von dem Modell, nach dem SaaS eingesetzt wird, muss sich der Nutzer über einige Dinge Klarheit verschaffen. Bei SaaS besteht eine hohe Abhängigkeit der Nutzer vom Dienstleister, der die Software zur Verfügung stellt. Maßgeschneiderte Sonderinstallationen wird es in der Regel nicht geben, da der Anbieter damit die Vorteile der leichten zentralen und einheitlichen Pflege einbüßen würde. Damit unterliegt der Nutzer auch den Vorgaben des Serviceanbieters bezüglich eingesetzter Versionen, Einschränkungen im Funktionsumfang sowie installierter Patches und Sicherheitsvorkehrungen. Zudem muss dem Anwender klar sein, wo seine Daten tatsächlich verarbeitet werden. Das kann eventuell beim Dienstleister geschehen, und es ist daher sicherzustellen, dass alle einschlägigen Sicherheits- und Datenschutzbestimmungen eingehalten werden. Diese Aspekte der Leistungserbringung wie auch Betriebszeiten und andere Serviceparameter können über entsprechende Servicevereinbarungen, englisch „Service Level Agreement", SLA, definiert werden. Besondere Bedeutung kommt bei allen SaaS-Model-

len den Netzen zu, über die die Dienste zum Einsatz kommen. Sie müssen entsprechend dem vereinbarten Servicelevel verfügbar und vertrauenswürdig sein. Die Vertrauenswürdigkeit lässt sich über geeignete Verschlüsselungsverfahren herstellen, und in dedizierten Netzen lässt sich auch die Verfügbarkeit steuern. Es ist jedoch schwierig, eine Verfügbarkeit für das Internet sicherzustellen, da es hier in der Regel Netzabschnitte gibt, die weder der Kontrolle des Nutzers noch der des Dienstanbieters unterliegen. Kommt es im Internet oder in anderen betroffenen Netzsegmenten zu Störungen, bedeutet das eventuell, dass viele Nutzer nicht auf die Anwendung zugreifen können. Ob sich auf Nutzerseite schließlich auch Hardwarekosten einsparen lassen, weil die Anwendungen, die als Service bereitgestellt werden, vergleichsweise ressourcenschonend sind, hängt davon ab, ob neben den SaaS-Anwendungen auch noch weitere – lokal installierte – Software benötigt wird. Sogenannte Thin Clients können nur da eingesetzt werden, wo alle ressourcenintensiven Funktionen auf die zentralen Komponenten der Serviceinfrastruktur verlagert werden können.

Die Palette der Anwendungen, die für einen SaaS-Einsatz infrage kommen, ist breit. Sie reicht von kleinen Tools mit wenigen spezifischen Funktionen, die mit weiteren Diensten kombiniert werden, über ganze Office-Pakete bis hin zu komplexen Spezialanwendungen. Populär sind solche Anwendungen, die dazu dienen, elektronische Inhalte zu erstellen und zu publizieren. Verschiedene Blog- und CMS-Anwendungen werden bereits als Service betrieben. Auch Kommunikations- und Kollaborationsplattformen sowie Office-Pakete, die über das Internet genutzt werden können, finden zunehmend Verbreitung. Als die großen Wachstumsmärkte für SaaS-Anbieter werden aber Anwendungen für die Kundenpflege, englisch „Customer Relationship Management“, CRM, und für die Planung der Unternehmensressourcen, englisch „Enterprise Resource Planning“, ERP, angesehen.

Die Antwort auf die Frage, ob in einer Organisation SaaS genutzt werden soll oder nicht, hängt von mehreren Faktoren ab. Neben dem Aspekt der Wirtschaftlichkeit ist insbesondere zu prüfen, ob ein vertrauenswürdiger Anbieter zur Verfügung steht, der in der Lage ist, die benötigte Leistung zu erbringen und die benötigte Sicherheit zu gewährleisten. In großen Organisationen lohnt es sich gegebenenfalls, entsprechende Dienste zentral zu betreiben, also selbst SaaS anzubieten und leistungs- bzw. verbrauchsgerecht abzurechnen.

Bewertung

Verwaltungen üben eine Reihe immer wiederkehrender Tätigkeiten aus, bei denen sich eine zentrale Bereitstellung von Funktionen über ein SaaS-Modell anbietet. Dabei muss sichergestellt werden, dass die verwendete Infrastruktur für diesen Einsatz geeignet ist. Aufgrund der zu verarbeitenden Daten, die oft einen Personenbezug haben, empfiehlt es sich, einen zentralen verwaltungsinternen Dienstanbieter mit der Leistungserbringung zu beauftragen. Dies hat neben der Datensicherheit auch den Vorteil, dass in der Regel die dabei verwendeten Netze in stärkerem Maß der Kontrolle der Verwaltung unterliegen, als dies der Fall ist, wenn öffentliche Netze einbezogen sind.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Aller guten Dinge sind fünf! Neue Version von HTML

Seit HTML – die Sprache, in der Webseiten beschrieben werden – 1989 das Licht der Welt erblickte, gab es eine Reihe von Änderungen in der Sprache. Konzipiert wurde die „Hypertext Markup Language“ seinerzeit, um Textdokumente miteinander durch sogenannte Hyperlinks zu vernetzen. Inzwischen werden im Internet komplexe Informations- und Funktionsangebote mit verschiedensten Medientypen unter Verwendung von HTML präsentiert. Für viele Spezialanwendungen sind neue Sprachen und Werkzeuge entstanden, die die Fähigkeiten von HTML ergänzen. So wurden mit der letzten Version, HTML 4, z. B. Skripte und Stylesheets eingeführt, die es erlauben, Funktionen zu programmieren respektive wiederkehrende Gestaltungselemente zentral zu definieren.

Der derzeit aktuelle Standard HTML 4.01 weist demgegenüber nur kleinere Korrekturen auf. Auch diese Fassung ist inzwischen zehn Jahre alt, und seit der Einführung im Jahr 1999 haben sich mit den technischen Möglichkeiten – insbesondere den heute üblichen Bandbreiten von Netzen – auch die Erwartungen und Anforderungen der Nutzer an Webseiten vervielfacht. Allein die allgemeine Verfügbarkeit von schnellen Netzzugängen hat dazu beigetragen, dass Ton- und Videomaterial aus dem Internet zum Standardangebot gehört. Leistungsfähige Rechner und Grafikkarten tun ein Übriges dazu. Dabei geht es den Nutzern nicht mehr um reinen Konsum – also das Aufnehmen der dargebotenen Inhalte. Die Interaktion mit anderen – z. B. Firmen, Verwaltungen oder anderen Nutzern – tritt immer stärker in den Vordergrund. Geschäftsbeziehungen und soziale Kontakte werden häufig ins Netz verlegt.

All das weckt natürlich auch das Bedürfnis, die entstandenen Wünsche, Ansprüche und Anforderungen an Webseiten möglichst einfach befriedigen zu können. Dem trägt die Entwicklung der neuen Version der Websprache, HTML 5, Rechnung. Sie soll insbesondere die Verwendung von „gehaltvollen“ Informationen, englisch „Rich Content“, und die Entwicklung von Webanwendungen vereinfachen. Dazu wurde eine ganze Reihe von Sprachelementen verändert, von denen im Folgenden einige vorgestellt werden sollen.

Die Elemente **audio** und **video** sollen es künftig ermöglichen, entsprechende Medien direkt in HTML einbinden zu können, ohne dass dafür zusätzliche Komponenten im Browser – sogenannte Plug-ins – benötigt werden. Über das Element **canvas**, englisch für „Leinwand“, sollen Zeichenflächen realisiert werden. Die Entwicklung von Webanwendungen wird u. a. durch die Spezifikation von Eingabe- und Parametertypen unterstützt. So kann etwa über das Typelement **datetime** festgelegt werden, dass eine Eingabe ein Datum oder eine Uhrzeit sein soll. Man kann es dann der Anwendung überlassen, wie sie die Bearbeitung der Eingabe behandelt und ob sie dazu eventuell einen interaktiven Kalender verwendet, der ein Datum im entsprechenden Format übergibt.

Heutzutage bestehen viele Webangebote nicht mehr aus monolithischen Informationsseiten oder einzelnen Anwendungen. Im Zeitalter von Content Syndication, Mash-ups, „Mitmach-Web“ und werbefinanzierten Angeboten bestehen viele Internetangebote aus einer Zusammenstellung von mehr oder weniger lose verbundenen Gestaltungsblöcken. Auch dies spiegelt sich in neuen Sprachelementen von HTML 5 wider. Dort gibt es nun eine ganze Reihe von Möglichkeiten, Strukturen zu beschreiben. So kann das Element **section** verwendet werden, um größere Inhaltsbereiche gegeneinander abzugrenzen – etwa bei der Trennung von Inhalten und Kontaktinformationen. Solche Bereiche können jeweils mit einem Kopf- und einem Fußbereich versehen werden; die Elemente dafür heißen **header** und **footer**. Der Unterbringung von Navigationselementen dient der Bereich **nav**. Für inhaltlich eigenständige Informationsblöcke, die aber mit weiteren derartigen Blöcken einen Informationsbereich bilden können, gibt es das Element **article**. Anwendungsmöglichkeiten dafür wären z. B. Blogeinträge oder Pressemitteilungen. Randbemerkungen, die zwar inhaltlich zum übrigen Angebot einer Seite passen, aber doch unabhängig davon präsentiert werden sollen, können als **aside**-Element gestaltet werden. Die Verbindung zwischen Medien und erläuternden Unterschriften wird durch das **figure**-Element hergestellt.

Bei einigen Sprachelementen aus dem schon bestehenden Vokabular von HTML ändert sich in der neuen Version die Bedeutung. Zum Beispiel diente das Element **i** bisher lediglich der optischen Hervorhebung durch Schrägstellen der Schrift. Bei HTML 5 steht es nun allgemein für eine in der Art des markierten Textes begründete Hervorhebung, z. B. für einen technischen Begriff oder eine idiomatische Redewendung. Diese Interpretation trägt dem Umstand Rechnung, dass solche Hervorhebungen in verschiedenen Sprachen unterschiedlich gehandhabt werden.

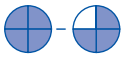
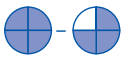
Weitere Sprachelemente werden ganz abgeschafft, da sie selten verwendet wurden bzw. ihre Funktion von anderen Elementen übernommen werden kann (z. B. **acronym** oder **applet**). Andere entfallen, da ihre Funktion besser in Stylesheets untergebracht wird (z. B. **font**, **center** oder **tt**). Und schließlich wurden die umstrittenen Frames (Elemente **frame**, **frameset** und **noframes**) aus dem Sprachumfang entfernt, da sie die Nutzbarkeit verschlechtern und Barrierefreiheit erschweren.

Der Reifegrad der einzelnen Sprachelemente in der neuen Spezifikation ist unterschiedlich. Einige davon sind schon so weit beschrieben, dass sie zur Verwendung freigegeben wurden. Dies führt zu einem neuen Kleinkrieg der Browserhersteller: Während die einen die freigegebenen Elemente auch schon sinnvoll präsentieren bzw. verarbeiten können, nutzen die anderen sie noch nicht. Google hat entsprechende Fähigkeiten in seinen Browser Chrome eingebaut und verwendet HTML-5-Elemente intensiv in seinem Wave-Framework (⇨ Artikel „Kollaboration heute und morgen“). Da andere Hersteller dies nicht im gleichen Maße tun, hat Google sogar ein Chrome-Plug-in für ihre Browser veröffentlicht, das diese Produkte in die Lage versetzt, die HTML-5-Elemente angemessen zu verarbeiten. Der Browserhersteller warnt natürlich vor der Verwendung des Plug-ins.

Bis die Spezifikation insgesamt als stabil angesehen werden kann, wird noch einige Zeit vergehen. Man rechnet damit für das Jahr 2012. Wie sich bis dahin die Webtechnik insgesamt und die Browser weiterentwickeln, bleibt abzuwarten.

Bewertung

Auch die webbasierten E-Government-Angebote der Verwaltungen werden von den Entwicklungen der Technik und von den veränderten Gewohnheiten der Internetnutzer beeinflusst. HTML 5 bietet zahlreiche Sprachelemente, die die Strukturierung der Angebote erleichtern und damit auch deren Pflege und Änderungen vereinfachen. Auf die Dauer wird die neue HTML-Version also auch Einzug in den Verwaltungsportalen halten. Der derzeitige Reifegrad der Spezifikation erlaubt aber höchstens das Experimentieren in einzelnen Bereichen. Die Umstellung ganzer Portale sollte mindestens noch so lange zurückgestellt werden, bis der Standard weitestgehend stabil und die Technik darauf abgestimmt ist.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Code Clone Reduction

Im Sommer bekam ich einen freundlichen Brief von der Stadtverwaltung, in dem ich gefragt wurde, ob ich nicht als Wahlhelfer bei der Kommunalwahl im September dabei sein wolle. Nun war die Kommunalwahl gerade erst kurz vorher gewesen, und eigentlich stand im Herbst die Bundestagswahl an. Offenbar gab es einige Rückmeldungen zur Terminlage, und so kam kurze Zeit später ein Schreiben, in dem man unter Verweis auf ein „drucktechnisches Versehen“ den Irrtum korrigierte. Derartige Pannen, die durch das Kopieren und Einfügen, englisch „copy and paste“, entstehen, kennt vermutlich jeder. Was jedoch im Schriftverkehr oft nur erheiternd bis peinlich ist, kann zu schwerwiegenden Fehlern führen, wenn es im Programmcode passiert: Vermeintlich gleiche Fragmente werden in einen neuen Kontext gebracht, gegebenenfalls noch leicht modifiziert und sollen dort eine andere Aufgabe verrichten. Geht man hierbei nicht sorgfältig vor, sind Fehlfunktionen – im wahrsten Sinne – vorprogrammiert, deren Wirkungen eventuell erst spät auffallen. Daher beschäftigt sich ein Zweig der Softwareforschung intensiv mit solchen Code Clones genannten Wiederholungen in Programmtexten. Dabei stehen die Fragen im Vordergrund, wie sie erkannt, frühzeitig vermieden oder im Nachhinein entfernt werden können, denn – so weit herrscht Einigkeit – Code Clones sind Fehlerquellen und erschweren die Softwarepflege allein schon durch das Mehr an Programmtext.

Schon die Frage, wie Code Clones erkannt werden können, ist viel komplexer, als es auf den ersten Blick scheint. So gibt es in der Fachwelt nicht einmal eine allgemein anerkannte Definition, wann man von Code Clones sprechen kann bzw. muss. Man ist sich schnell einig, wenn Codezeilen identisch wiederholt oder lediglich andere Bezeichnungen für Variablen, Funktionen usw. verwendet werden. Doch schon hier ist Vorsicht geboten, denn es kann vom Kontext abhängen, auf welche Objekte zugegriffen wird. Wenn man dann noch Ergänzungen, Änderungen oder Streichungen im Programmtext berücksichtigen will, sodass man nur noch von ähnlichem Code sprechen kann, scheiden sich schon die Geister: Ab welchem „Grad“ von Ähnlichkeit kann bzw. muss man von Code Clones sprechen? Solange man sich auf der lexikalischen bzw. syntaktischen Ebene bewegt, kann man sich noch relativ einfache Hilfsmittel bauen, die bei der Identifizierung von Code Clones helfen. Auf der semantischen Ebene wird es sehr schwierig, „ähnliche“ Funktionen zu identifizieren. Diese Schwierigkeit bedeutet nicht nur, dass man viel Aufwand treiben muss, um zum Erfolg zu kommen. Diese Frage ist grundsätzlich nicht entscheidbar. In der Sprache der Informatik heißt das: Es kann zwar Fälle geben, in denen ein Prüfmechanismus feststellen kann, dass zwei Codesegmente ähnliche oder die gleiche Funktion haben, es gibt aber keinen universellen Prüfmechanismus, der in jedem Fall sicher entscheiden kann, ob dies für je zwei beliebige Codesegmente zutrifft. Die Arbeit, die bei einer derartigen Prüfung zu verrichten ist, kann jeder nachvollziehen, der schon einmal versucht hat, eine nicht triviale rekursive Funktion in eine iterative Funktion zu übersetzen. Einfache Beispiele für semantisch ähnliche bzw. gleiche Funktionen sind verschiedene Implementierungen von Such- oder Sortierverfahren. Auf etwas abstrakterer Ebene kann man auch Gerätetreiber z. B. für Drucker als ähnliche Codesegmente sehen, die – ergänzt um spezifische Parameter und zusätzliche Funktionen – die gleiche Arbeit leisten.

Es werden viele mögliche Ursachen für Code Clones genannt, die oft einen negativen Beigeschmack haben – etwa schlecht organisierte Prozesse für die Wiederverwendung von Code, verteilte Entwicklungsteams oder schlechte Produktivitätsmaße auf der Basis von Codezeilen pro Tag. Dabei gibt es auch gute Gründe, Programmtext zu wiederholen – z. B. bei querschnittlichen Aufgaben wie dem Protokollieren von Programmabläufen, englisch „Logging“, oder der einheitlichen Handhabung von Parameterprüfungen in Funktionen. Auch Designprinzipien wie die möglichst geringe funktionale Kopplung von Programmmodulen können dazu führen, dass zusätzlich Code Clones entstehen. Und ob die Vermeidung von Code Clones tatsächlich zu leichter wartbarem Code führt, ist umstritten, da gegebenenfalls mehrere Instanzen eines Codesegments mit leichten Änderungen einfacher zu pflegen sind als eine universelle, aber abstrakt formulierte gemeinsame Funktion, die alle möglichen Varianten implementiert.

Unabhängig von der Frage, wie man mit Code Clones umgeht – Vermeidung bei der Implementierung oder auch automatische bzw. manuelle Reduktion im Nachhinein –, besteht die wichtigste Aufgabe darin, Code Clones sicher zu erkennen. Es gibt verschiedene Ansätze und dazu passende Werkzeuge, um diese Aufgabe zu automatisieren. Die Erfolgs- bzw. Fehlerquoten sind unterschiedlich, und es hängt stark davon ab, wie man die Ähnlichkeit von Code definiert und in welchem Kontext man die Clones identifizieren möchte, wie erfolgreich die Suche verläuft. Die Forschung auf diesem Gebiet wird wohl noch eine Weile benötigen, bis anerkannte und qualitativ hochwertige Verfahren bzw. Werkzeuge für Code Clone Detection und Removal bereitstehen.

Bewertung

Der unmittelbare Nutzen einzelner Softwareentwicklungsmethoden für die Verwaltung lässt sich nur schwer ermitteln – zumal wenn diese noch nicht klar erkennen lassen, wie sie anzuwenden sind. Das Thema der Code Clones hat aber das Potenzial, mittelbar auf verschiedene Art zum Tragen zu kommen. Im direkten Softwareumfeld können die Forschungsergebnisse zu besseren Programmen sowie zuverlässigeren Anwendungen und damit zu mehr Kundenzufriedenheit führen. Eventuell lassen sich künftige Methoden, gerade der Erkennung, auch auf andere Anwendungsfelder übertragen wie etwa die Erkennung von Datenduplikaten oder gar redundanten Informationen. Ob sich dadurch „Büroirrtümer“ wie das einleitende Beispiel vermeiden lassen, ist allerdings noch überhaupt nicht absehbar.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

IT-Sicherheit und Datenschutz

Wie das Übel in den PC kommt – „Malware" überall

In der griechischen Mythologie kommt das Schlechte in die Welt, als die „Büchse der Pandora" geöffnet wird. Ob Pandora selbst oder ihr Mann Epimetheus das verhängnisvolle Gefäß – entgegen der ausdrücklichen Warnung von Göttervater Zeus – öffnet, lässt sich den Geschichten nicht eindeutig entnehmen. Auf jeden Fall entweicht das Übel, und das Schicksal nimmt seinen Lauf.

„Öffnen oder nicht?" – die Frage stellen sich offenbar viele PC-Anwender, wenn sie nur lange genug mit Virenwarnungen belästigt werden, obwohl sie sich eigentlich in Sicherheit wähnen, und zugleich ein weiteres Sicherheitsprogramm angeboten wird. Die Furcht vor ernsthaften Schäden durch Viren, Trojaner und andere Schadsoftware nutzen Hersteller sogenannter Scareware (englisch „to scare" = „Angst einjagen") aus und bringen die Anwender durch vorgetäuschte Systemscans und gefälschte Sicherheitswarnungen dazu, ihre Produkte zu erwerben und auf dem Computer zu installieren. Im günstigsten Fall hat das Programm keine Funktion und dient „lediglich" dazu, Geld zu erschwindeln. Aber das Spektrum möglicher Schäden, die durch solche Scareware entstehen, ist weitaus größer. Neben dem Missbrauch der beim Erwerb verwendeten Konto- oder Kreditkartendaten stellt das Einschleusen von Schadsoftware eine weitere mögliche Bedrohung dar. Viren oder andere Schädlinge können z. B. Daten ausspähen und versenden, oder der infizierte Computer kann zum Spamversand missbraucht werden. Das Geschäft mit der Angst scheint sich zu rechnen, denn binnen eines Jahres nahm die Zahl derartiger Programme fast um das Siebzigfache zu, und ein großer Softwarehersteller reinigte vor einiger Zeit rund eine Million PCs binnen weniger Tage von künstlicher Sicherheitssoftware. Weiterer Schaden entsteht dadurch, dass die Hersteller echter Antivirenprogramme nennenswerte Zeit und Energie investieren müssen, um ihren Produkten beizubringen, Scareware zu erkennen.

Das Vorgaukeln von Bedrohungen ist eine Möglichkeit, Computernutzer dazu zu bewegen, Anwendungen aus unsicheren Quellen zu starten. Die Warnungen vor dubiosen E-Mail-Anhängen hat wohl inzwischen nahezu jeder gelesen, sodass die Verbreitung von Schadsoftware auf diesem Weg inzwischen deutlich schwieriger geworden sein dürfte. Insofern erfordert es schon besondere Maßnahmen – wie das Vorspiegeln wichtiger oder interessanter Inhalte –, um die Hemmschwelle für das Öffnen von Anhängen und Anwendungen herabzusetzen.

Eine weitere Technik zur Verbreitung von Schadsoftware zielt darauf, das explizite Eingreifen des Nutzers ganz zu umgehen. Hierbei können durch das bloße Öffnen von Webseiten Schädlinge aktiviert werden. Auch die oben dargestellte Scareware kann sich auf diesem Weg verbreiten. Der Angreifer nutzt dabei Sicherheitslücken in Browsern oder Browserzusätzen – sogenannten Plug-ins – aus, um manipulierten Code beim Laden der Seite einzuschleusen. Da dies gewissermaßen im Vorbeigehen bzw. -fahren geschieht, heißen diese Schädlinge „Drive-by Malware" oder „Drive-by Downloads". Oft vergehen nach Bekanntwerden einer Sicherheitslücke mehrere Wochen, bis ein Patch zur Verfügung steht, der sie schließt. Das bietet den Herstellern von Drive-by Malware ausreichend Gelegenheit, derartige Schwachstellen zu nutzen. Insbesondere wenn zeitgleich mit den Informationen zu Schwachstellen auch direkt Angriffsmöglichkeiten veröffentlicht werden – sogenannte Zero-Day-Exploits –, spielt die Zeit für die Angreifer. Sie müssen dabei nicht einmal eigene Seiten präparieren und potenzielle Opfer mit Lockangeboten dorthin locken oder mithilfe weiterer Angriffstechnik dorthin leiten. Gegebenenfalls kann der Schadcode in Seiten von populären öffentlichen Medien, von sozialen Netzwerken oder von anderen Anbietern mit vielen Lesern eingepflanzt und so über die vermeintlich sauberen Kanäle verbreitet werden. Selbst der vorsichtige Umgang mit Dateianhängen aus E-Mail oder mit Applikationen und besonderen Seiten aus dem Web schützt also nicht mehr zuverlässig vor Schädlingen auf dem eigenen PC.

In der griechischen Göttergeschichte kommt durch erneutes Öffnen der berühmten Büchse auch die Hoffnung in die Welt. Der PC-Anwender sollte jedoch nicht darauf hoffen, dass er durch mehrfaches

SEMINARE
siehe Seite 44/45
- IT-Sicherheit am Arbeitsplatz
- IT-Sicherheit von mobilen Kommunikationsgeräten
- Das Web vergisst nichts

Anwenden dubioser Software seinen PC in einen sicheren Zustand versetzen kann.

Bewertung

Verwaltungen sind von den neuen Trends bei Schadsoftware in zweierlei Hinsicht betroffen. Zum einen stellen sie mit ihrer großen Zahl von Computeranwendern, die sich in vermeintlich sicheren Umgebungen befinden, ein gutes Feld für die Verbreitung von Schädlingen dar. Zum anderen fungieren sie oft auch als Informationsanbieter, die in der Öffentlichkeit eine hohe Reputation bezüglich der Seriosität ihrer Angebote haben. Das Einschleusen von Schadcode auf Webseiten der öffentlichen Verwaltungen kann daher in besonderem Maße Probleme verursachen. Die permanente und konsequente Sicherung der Verwaltungsnetze und -systeme hat daher einen hohen Stellenwert.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Trügerische Sicherheit?

Virtualisierung – insbesondere das Einrichten von virtuellen Servern auf Hostsystemen – ist seit einiger Zeit ein Trendthema (⇨ HZD-Trendbericht 2006), da ressourcenschonender Umgang mit IT heute zunehmend wichtiger wird. Sei es aus ökologischen Gründen – Stichwort „Green IT“ –, sei es, um dem wachsenden Platzbedarf im Rechenzentrum zu begegnen oder um Personal und Know-how effizient einsetzen zu können: Die Aussicht, auf einem Hostsystem auf einfache Art viele virtuelle Server einrichten und betreiben zu können, stellt für viele eine Verlockung dar, entsprechende Maßnahmen schnell umzusetzen. Und auch für die Sicherheit der IT-Systeme verheißt dieser Ansatz zunächst Gutes. Ein kompromittierter Server kann durch „Klonen“ eines unversehrten Masters schnell wiederhergestellt werden, und daher können virtuelle Server insbesondere sehr einfach als „Locksysteme“ für Schadsoftware und Angreifer eingesetzt werden. Durch solche sogenannte „Honeypots“ – oder bei mehreren vernetzten Systemen „Honeynets“ – können mögliche Angriffe von außen analysiert und die operativen Systeme davor geschützt werden. Diese Sicht stellt jedoch die einzelnen virtuellen Systeme in den Vordergrund und vernachlässigt die Hostebene sowie die Kopplung von Host und virtueller Maschine. Das kann aber fatale Folgen haben, denn mit zusätzlichen Komponenten wächst die Komplexität von Systemen. Und gerade eine derart zentrale Komponente wie der Host, der die virtuellen Server beherbergt, bietet dabei Chancen wie auch Risiken für den Betrieb.

Um die Chance nutzen zu können, von einer übergeordneten Stelle – dem sogenannten Hypervisor – aus die „Gastsysteme“ überwachen und steuern zu können, muss der Host mit den spezifischen Gegebenheiten der einzelnen Server umgehen können – z. B. mit dem jeweiligen Betriebssystem, uneinheitlichen Patchleveln, unterschiedlichen Applikationen oder verschiedenen Netzen. Schon die Kommunikation verschiedener Server untereinander zu überwachen, kann hier schwieriger werden als in einem System separater Maschinen, da hier diese Kommunikation allein im Host abläuft und klassische, netzwerkbasierte Monitore hier nicht eingesetzt werden können. Ebenso müssen die sonst üblichen Schutzmechanismen zur Abgrenzung von Servern gegeneinander in der virtuellen Landschaft nachgebildet werden, damit sich Störungen von einem Server aus nicht ungehindert auf alle anderen Gastsysteme ausbreiten können. Dies ist umso wichtiger, wenn die einzelnen virtuellen Systeme unterschiedliche Aufgaben und Funktionen haben, da dann ein Fehler oder ein Schädling, der für einen Server harmlos ist, auf einem anderen System verheerende Folgen haben kann. Hier gilt in besonderem Maß, dass die Sicherheit eines Gesamtsystems der Sicherheit des schwächsten Gliedes entspricht. Problematisch wird das zentrale System auch dann, wenn der Hypervisor selbst Fehler enthält – z. B. in der emulierten Hardware wie einem Netzwerkadapter. Derartige Fehler

wirken sich dann oft auf alle virtuellen Maschinen aus, und der Schaden ist größer, als wenn eine entsprechende Komponente eines einzelnen Servers fehlerhaft ist.

Auch für Schadsoftware stellt das Nervenzentrum der virtuell vernetzten Serverlandschaft ein attraktives Ziel dar. Die Aussicht, durch Manipulationen an Funktionen des Hypervisors die Kontrolle über viele Server zu erlangen, ist für Angreifer verlockend. Und so sind Schädlinge inzwischen durchaus in der Lage, in die sogenannte „Sandbox" einzudringen, die für den virtuellen Server eine geschützte Laufzeitumgebung darstellen soll. Der Hypervisor selbst gilt bisher noch als besonders geschützt. So scheint es nur theoretisch möglich, dass ein manipulierter Hypervisor vollständig die Kontrolle übernimmt und das Originalsystem ausgrenzt. Allerdings kann der Hypervisor durch Denial-of-Service-Angriffe lahmgelegt werden.

Die wesentliche Bedrohung für virtuelle Architekturen scheint aber aus schnell bzw. nachlässig umgesetzten Virtualisierungsmaßnahmen zu resultieren. Zumindest erwecken die Empfehlungen der Sicherheitsexperten in den einschlägigen Publikationen diesen Eindruck. Dort findet man nur wenige spezifische Sicherheitsmaßnahmen wie etwa das Härten des Hypervisors durch Deaktivieren bzw. Entfernen nicht benötigter Funktionen oder die Implementierung virtueller Switches zur Abgrenzung der Gastsysteme voneinander. Ansonsten werden vor allem klassische Maßnahmen genannt, die in einem geordneten und strukturierten Betrieb selbstverständlich sein sollten: Berechtigungskonzepte mit klaren Zuständigkeiten – „Separation of Duties" – und die Beschränkung auf die notwendigen Rechte sowohl auf Host wie auf virtuellen Maschinen werden ebenso eingefordert wie ein abgestimmtes Patchmanagement. Auch wird empfohlen, sicherheitsrelevante Hinweise und Dokumentationen der Hersteller zu lesen.

Da die Absicherung allein des Hostsystems gegen externe Komponenten aufgrund der internen „Vernetzung" und Kommunikation mit gemeinsamen Speicherressourcen nicht ausreicht, müssen Schutzfunktionen von sonst üblichen Systemen wie Firewall oder Spamfilter in die virtuelle Umgebung übertragen – sprich virtualisiert – werden. Selbst wenn die Anwendungen der einzelnen Schritte in einer Prozesskette auf unterschiedlichen Instanzen einer virtuellen Umgebung laufen, können Sicherheitslücken zum Ausfall ganzer Produktionen führen, wenn sich ein Schädling ungehindert zwischen den virtuellen Servern bewegen kann.

Hier wird als weitergehende Maßnahme die Aufteilung der verschiedenen Anwendungen auf separate physikalische Hosts vorgeschlagen, selbst wenn dadurch die Vorteile der Virtualisierung nicht gänzlich ausgeschöpft werden können. Arbeitet man mit mehreren Sicherheitszonen, ist eine solche Aufteilung fast zwingend, da dann die Abgrenzung der Zonen gegeneinander mit Standardmitteln bewältigt werden kann. An dieser Maßnahme der Aufteilung wird auch deutlich, dass – gerade unter Sicherheitsaspekten – die Virtualisierung umfangreicher Systemlandschaften sorgfältig und vorab geplant werden muss. Die Ziele der Virtualisierung müssen in das entsprechende Sicherheitskonzept einfließen, das durchgängig sein und die vollständige Zielarchitektur abdecken muss. Die Erzielung „schneller Gewinne" durch Virtualisierung ist also mit besonderen Risiken behaftet, da es in der Regel viel aufwendiger ist, die Sicherheit einer Architektur im Nachhinein herstellen zu wollen, insbesondere wenn man erst durch einen sicherheitsrelevanten Vorfall dazu veranlasst wird.

Bewertung

Skalierbare Systeme mit konsolidierten Hardwarearchitekturen gewinnen aus Effizienzgründen auch in der öffentlichen Verwaltung an Bedeutung. Virtualisierung kann dazu beitragen (⇨ HZD-Trendbericht 2006). Aufgrund der verschiedenen Aufgaben – von der Finanzverwaltung über Verfahren zur Unterstützung der Wirtschaft bis hin zu Systemen für die innere Sicherheit – spielt die IT-Sicherheit dabei eine besonders wichtige Rolle. Sie muss dabei frühzeitig bei der Planung und Einrichtung virtueller Architekturen berücksichtigt werden.

SEMINARE
siehe Seite 45

- IT-Sicherheit von mobilen Kommunikationsgeräten
- Das Web vergisst nichts

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Informationszentrierte Sicherheit und Cloud Computing

Die Wolke, englisch „Cloud“, ist ein Modell für eine IT-Systemarchitektur, die darauf ausgerichtet ist, Ressourcen zu bündeln und deren Leistungen über definierte Schnittstellen zur Verfügung zu stellen. Solche Leistungen können von der Bereitstellung von Speicherplatz über die Nutzung von spezieller Peripherie bis hin zu mehr oder weniger komplexen Anwendungen reichen, die als Service genutzt werden. Ein wichtiges Verkaufsargument für diese Architektur bzw. die darauf aufsetzenden Leistungen ist die hohe Skalierbarkeit der Leistungen. Diese sorgt dafür, dass die Anwender zum einen nahezu immer ausreichend Leistung zur Verfügung haben, zum anderen aber nur das bezahlen, was sie auch wirklich nutzen. Das Modell ist dann wirtschaftlich sinnvoll, wenn eine große Zahl von Nutzern mit wechselndem Bedarf sich das Angebot teilt und nicht alle Nutzer gleichzeitig die individuelle maximale Leistung benötigen. Solange man diese Architektur in einer geschlossenen Nutzerumgebung – z. B. einem Unternehmen oder einer Verwaltung – nutzt, ist sie relativ gut kontrollier- und steuerbar – insbesondere im Hinblick auf die Sicherheit. Schwieriger wird dies, wenn verschiedene Nutzergruppen mit unterschiedlichen Sicherheitsanforderungen sich die Ressourcen teilen. Schon allein das Bedürfnis eines Kunden, seine Daten und Anwendungen dem Blick der Konkurrenz zu entziehen, kann Auswirkungen auf die zu implementierenden Sicherheitsmaßnahmen haben. Dabei muss man sich vor Augen führen, dass diese Forderung nach scharfer Trennung der Nutzerbereiche der Forderung nach möglichst flexibler Ressourcenzuteilung zuwiderläuft.

Für den Anbieter von sogenanntem Cloud Computing stellt sich also die Frage, wie er mit diesen Widersprüchen umgeht. Es reicht auf jeden Fall nicht aus, die Wolke gegenüber der Umwelt abzusichern. Es müssen auch Maßnahmen ergriffen werden, die für die „innere Sicherheit“ sorgen. Dazu können gehören: Identitätsmanagement, starke Authentisierung per Token, Ende-zu-Ende-Verschlüsselung, Data Loss Prevention oder Virenerkennung innerhalb der Cloud.

Für den Anwender, der die technischen Sicherheitsmaßnahmen in der Cloud nicht direkt steuern kann, hat dieses Architekturmodell zur Folge, dass er sich Gedanken über den Schutzbedarf seiner Daten machen muss, nicht allein den von Geräten und ganzen Anwendungen. Dieser Ansatz von informationszentrierter Sicherheit wird deshalb notwendig und sinnvoll, weil die verarbeitenden Systeme – Hard- und Software – immer weniger eine Einheit bilden, die zu schützen ausreicht. Das zu erreichende Sicherheitsniveau hängt dabei zwar mehr von den Daten ab als von technischen Komponenten an sich, konkrete Bewertungen lassen sich aber erst in Zusammenspiel von beiden abgeben. In diesem Zusammenhang spricht man davon, dass Sicherheit im Kontext entsteht. Dabei hat weniger das Format, in dem eine Information vorliegt – z. B. als Datenbankeintrag, in einem Wiki oder in einer Mail –, eine Bedeutung als vielmehr der Zustand der Information. Drei mögliche relevante Zustände unterscheiden sich danach, ob die Information „in Ruhe“ – also gespeichert –, in Benutzung – also in einer Anwendung – oder „in Bewegung“ – sprich in einem Netz unterwegs – ist. In Verbindung mit diesem Zustand gewinnt dann die Sicherheit einzelner Geräte an Bedeutung, und es reicht in der Regel nicht mehr aus, ganze Cluster von Geräten bzw. Netzsegmente zu betrachten.

Die Strategie der sogenannten End Point Security, die darauf baut, dass jedes Gerät für seine Sicherheit zuständig ist, findet einen extremen Ausdruck in einem Konzept namens Jericho. Es stammt von Mitgliedern der Open Group, einem Industriekonsortium, das an technikunabhängigen Standards arbeitet. Sie schlagen in dem Konzept vor, die äußeren Firewalls – Perimeterfirewalls – einer IT-Architek-

tur abzuschaffen. Dieser ungewöhnliche Vorschlag wird damit begründet, dass es das klassische Innen und Außen heute eigentlich nicht mehr gäbe. Häufig gibt es zahlreiche Kommunikationsbeziehungen mit Partnern, die sich außerhalb der Organisation und damit außerhalb der zu schützenden Systemlandschaft befinden. Das können Kunden, Lieferanten, Behörden, Organisationen oder Privatpersonen sein, und man kann mit ihnen sehr unterschiedlich kommunizieren – von einfacher Mail über Webanwendungen bis hin zum Fernzugriff auf interne Systeme. Lenkt man all diese Kommunikationsströme über eine einzige zentrale Sicherheitskomponente, eröffnet jede Kommunikationsart einen neuen Kanal durch die Schutzmechanismen. Es ist aber nicht immer einfach sicherzustellen, dass dieser Kanal ausschließlich von zugelassenen Partnern in genau spezifizierten Anwendungsszenarien genutzt werden kann. So kann z. B. der Zugriff nur dann anhand von IP-Adressen begrenzt werden, wenn der externe Kommunikationspartner immer mit derselben IP-Adresse arbeitet. Wird ein Kommunikationskanal unerlaubt genutzt, um in einen geschützten Bereich einzudringen, kann der Angreifer sich dort ungehindert bewegen, wenn es innerhalb des Bereichs nicht weitere Schutzmechanismen gibt. Das Jericho-Konzept schlägt entsprechend vor, auf allen Geräten die Firewallfunktionen mit auf den spezifischen Zweck zugeschnittenen Regeln zu aktivieren, starke Authentisierung und Protokolle mit Verschlüsselung und gegebenenfalls IPsec-Verbindungen zu nutzen. Außerdem sollen nur definierte Kommunikationskanäle zugelassen und ausführliche Logging- und Monitoringprozesse etabliert werden. Der Zugewinn an Sicherheit auf Basis der jeweils maßgeschneiderten Maßnahmen scheint offensichtlich. Trotzdem wird man in der Praxis jeweils beweisen müssen, dass das Konzept tragfähig ist und entsprechende Systeme mit vertretbarem Aufwand zu betreiben sind, bevor die Sicherheitsverantwortlichen guten Gewissens der Abschaltung der äußeren Firewalls zustimmen können. Und auch wenn viele einzelne Sicherheitstechniken wohlbekannt und am Markt etabliert sind, dürfte der Aufwand für die umfassende Umsetzung dieses Konzeptes in Umgebungen mit verschiedenen Systemen und Anwendungen erheblich sein, und auch auf Dauer ist die Pflege der Kommunikationsbeziehungen arbeitsintensiv. Das heißt, dass die Schwellen für die Umsetzung von Jericho sehr hoch sind.

Beim Cloud Computing widerspricht der Ansatz verstärkter End Point Security sogar dem Ziel, Ressourcen möglichst flexibel einsetzen zu können, um sie sogar gemeinsam für verschiedene Kunden zu nutzen. Die „kommerzielle Offenheit“ von Cloud Computing lässt sich nur dann aufrechterhalten, wenn Leistungen schnell und flexibel verteilt werden können. Das Nachführen individueller und kundenspezifischer Sicherheitskonfigurationen würde dies erschweren. Trotzdem werden Anbieter von Cloud Computing nicht umhinkommen, neben der Abschirmung ihrer Systeme nach außen auch die Abschirmung der verschiedenen Kunden im Inneren gegeneinander zu gewährleisten. Bisher lautet die Einschätzung der Experten, dass sicherheitskritische Anwendungen in der Wolke noch nichts verloren haben.

Bewertung

Die Auslagerung von Verwaltungsverfahren oder Daten in eine „kommerziell offene“ Cloud dürfte in vielen Fällen schon aus rechtlichen Gründen nicht in Frage kommen. Innerhalb einzelner Verwaltungen – aber auch durch die Zusammenarbeit verschiedener Verwaltungen – gewinnt das Thema flexibler Ressourcennutzung im Sinne einer Verwaltungs-Cloud an Bedeutung. Gleichzeitig nehmen in einer immer stärker vernetzten IT-Welt auch für Verwaltungen die verschiedenartigen Kommunikationsbeziehungen zu, und es entstehen neue Notwendigkeiten oder Begehrlichkeiten, auch verwaltungsexternen Partnern Zugriff auf schützenswerte Systeme zu gewähren. Auch wenn der Aufwand für informationszentrierte Sicherheitskonzepte sehr hoch ist und ihre Einführung und dauerhafte Anwendung damit kostenintensiv sind, werden Verwaltungen nicht umhinkommen, sich mit Mechanismen der lokalen Sicherung auf Kosten allumfassender Schutzwälle intensiv zu befassen.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

„Data Loss Prevention" – Kampf gegen Windmühlen?

Wenn Unternehmen oder Organisationen Daten verlieren und dies publik wird, findet das zunehmend das Interesse der Presse. Wenn es sich dabei auch noch um sensible Daten handelt, wird schnell ein „Datenskandal" daraus, der zu einem erheblichen Imageschaden führen und Manager ihren Posten kosten kann. In der jüngeren Vergangenheit gibt es einige Beispiele dafür, dass Daten in großem Stil an Stellen auftauchen, an denen sie nichts verloren haben. Dabei geht es nicht um Fälle, in denen sich externe und unbefugte Personen unberechtigt Zutritt zu den Daten eines Unternehmens oder einer Organisation verschafft haben, sondern um solche, bei denen offenbar jeweils interne Mitarbeiter mit Zugang zu den Daten eine wesentliche Rolle spielten. Diese Beteiligung berechtigter Personen ist ein wesentliches Merkmal der Szenarien, die man bei dem Thema Schutz vor Datenverlust betrachtet. Im Englischen werden dafür die beiden Bezeichnungen „Data Loss Prevention" und „Data Leakage Prevention" verwendet – in der Regel synonym. Jedoch wird hin und wieder die Bezeichnung „Data Loss Prevention" für solche Fälle reserviert, in denen der Verlust von Daten tatsächlich stattfindet und Schaden verursacht, während „Data Leakage Prevention" für Szenarien verwendet wird, in denen Daten nur verloren gehen können und man es eventuell noch nicht einmal bemerken würde. Diese – für den praktischen Gebrauch vielleicht etwas zu feinsinnige – Unterscheidung gibt zumindest Hinweise darauf, dass es verschiedene Arten des Datenverlustes gibt.

Die einfachste Art, in der Daten verloren gehen können, besteht darin, sie tatsächlich irgendwo liegen zu lassen. Das zeigt eine der Schattenseiten zunehmend mobiler Kommunikation: Rechner, Smart Phones und PDAs, die man überallhin mitnehmen kann und muss, können mehrere Gigabyte an Daten enthalten. Vergisst man so ein Gerät im Eifer des Gefechts im Zug oder fällt einem ein Datenwinzling unbemerkt aus der Tasche, können schnell sensible Geschäftspapiere oder Anwendungsdaten in Umlauf geraten. Dieses Verlustszenario ist vorhersehbar, und der potenzielle Schaden kann durch entsprechende Maßnahmen reduziert werden. So sind die Verschlüsselung aller Daten auf mobilen Endgeräten und ihr Schutz durch Authentisierungsfunktionen vergleichsweise einfache Methoden, die zwar nicht vor dem Verlust der Geräte schützen, aber zumindest verhindern, dass die Daten ohne größeren Aufwand – um nicht zu sagen „ohne ausreichend viel kriminelle Energie" – zugänglich sind.

Eine weitere Art des Datenverlustes, die auch immer wieder in der Presse erwähnt wird, ist die unsachgemäße Entsorgung von Datenträgern. Die unachtsam in den Müll geworfene Daten-CD oder Magnetbänder, die vermeintlich ja sowieso keiner mehr lesen kann, sind immer wieder Auslöser von Datenskandalen. Diese Rolle steht aber nicht allein elektronischen Datenträgern zu. Auch wenn es etwas mühsamer ist, ausgedruckte Daten in großem Stil weiterzuverwerten, können auch klassische Papierakten im Müllcontainer zum Problem werden, wenn sie von dort aus in die falschen Hände geraten.

Dass es schließlich auch ganz ohne Verlust eines Mediums geht, zeigt ein Fall, der zum Rücktritt eines hohen britischen Polizeibeamten führte. Als der bei der Londoner Polizei für Terrorbekämpfung zuständige Beamte zu einem Termin in der berühmten Downing Street Nr. 10 eintraf, trug er ein Papier offen unter dem Arm, das als geheim gekennzeichnet war und Namen und Informationen im Zusammenhang mit einem geplanten Antiterroreinsatz enthielt. Diese Informationen wurden dadurch kompromittiert, dass Fotographen das Papier ablichteten. In der Folge war die Polizei gezwungen, den Einsatz vorzuziehen; der Beamte trat von seinem Posten zurück.

Dieser Fall zeigt besonders deutlich, dass die Information an sich den Wert darstellt und nicht unbedingt das Trägermedium, selbst wenn es sich um ein teures elektronisches Gerät handelt.

In den bisher beschriebenen Szenarien kann man wirklich davon sprechen, dass Daten verloren gehen. Wenn auch mal mehr, mal weniger fahrlässig gehandelt wird, so gelangen hier die Daten doch immer unbeabsichtigt in die falschen Hände. Data Loss Prevention befasst sich über solche Fälle hinaus aber auch noch mit der gezielten Weitergabe von Informationen durch Personen mit Zugriff auf die Daten an unberechtigte Stellen. Die Motivation dabei kann unterschiedlich sein und auch aus einer falschen Einschätzung des Schutzbedarfs resultieren. Die Bandbreite reicht von der gut gemeinten, aber nachlässigen Weitergabe von Informationen an Dritte bis hin zu gezieltem Geheimnisverrat, dem Verkauf von Daten oder der Erpressung des Unternehmens. Solche Fälle zu unterbinden ist sehr schwierig, da hier die handelnde Person zunächst einmal berechtigt ist, auf die Daten zuzugreifen.

Im Folgenden werden wir uns auf den Umgang mit elektronischen Daten konzentrieren. Vieles kann aber auch sinngemäß auf papiergebundene Daten übertragen werden. Verschlüsselung der Informationen und Authentisierung der Nutzer bieten hier – im Gegensatz zum erstgenannten Szenario – keinen zusätzlichen Schutz. Technische Unterstützung für den Schutz der Daten bietet allenfalls die Beschränkung des Zugriffs. So kann man z. B. externe Datenträger deaktivieren, die Weitergabe per E-Mail unterbinden oder alle Datenbewegungen protokollieren. Abgesehen davon, dass der Aufwand für derartige Maßnahmen sehr hoch sein kann, wenn sie nicht nur punktuell umgesetzt werden sollen, sind sie mit zwei Problemen behaftet: Zum einen unterscheiden sie nicht hinsichtlich der Sensibilität einzelner Informationen, und zum anderen stellen sie alle betroffenen Personen unter „Generalverdacht“. Um dem ersten Problem zu begegnen, kann man die Daten hinsichtlich ihres Schutzbedarfs klassifizieren und die Maßnahmen entsprechend fallbezogen anwenden. Doch auch hierfür ist der Aufwand erheblich. Und der Schutz – zumindest vor beabsichtigter Weitergabe – ist nur bedingt effektiv, da Daten gegebenenfalls in Dokumente mit geringem Schutzbedarf eingebettet werden können. Nicht zuletzt vor diesem Hintergrund gewinnt das zweite Problem an Bedeutung. Wenn technische Maßnahmen den Schutz nur verbessern, aber nicht garantieren können, ist man bei dem Versuch, sich vor dem Verlust von Daten zu schützen, auf die Unterstützung aller Beteiligten angewiesen. Überzogene Sicherheitsmaßnahmen und technische Beschränkungen können aber dies gerade verhindern – zumal dann, wenn sie die tägliche Arbeit erschweren. Das Schützen von Daten muss daher einfach sein. Die technischen Maßnahmen müssen sich einfach in die täglichen Abläufe einbinden lassen, möglichst ohne zusätzliche Arbeitsschritte zu erzwingen, wenn man die Unterstützung der Mitarbeiter beim Thema Data Loss Prevention gewinnen möchte.

Die Rolle der Mitarbeiter und die Bedeutung der organisatorischen Abläufe sowie des Schutzbedarfs einzelner Daten für Data Loss Prevention machen deutlich, dass sich das Thema nicht mit der Installation eines entsprechend deklarierten Systems abhandeln lässt. Data Loss Prevention ist auch weder eine Technologie noch ein Framework oder eine Architektur, die die unzulässige Nutzung sensibler Daten durch berechtigte Personen verhindert. All diese Definitionen wären zu einseitig technisch orientiert. Der Begriff „Data Loss Prevention“ sollte vielmehr für ein Bündel von technischen und organisatorischen Maßnahmen verwendet werden, die darauf ausgerichtet sind, alle Beteiligten vor eigenen – unbewussten wie auch beabsichtigten – Fehlern im Umgang mit Daten zu schützen. Für solche Maßnahmenbündel werden folgende fünf Punkte genannt:

Die **Dokumentation** dessen, was mit Daten gemacht wurde, kann zwar Fehlverhalten nicht direkt verhindern, dient aber der Klärung in Fällen von Datenverlust. Präventiv kann diese Maßnahme nur dann wirken, wenn sie bekannt und akzeptiert wird und ihrerseits im Einklang mit datenschutzrechtlichen und arbeitsrechtlichen Regelungen steht.

Durch **Sensibilisierung und Information** sollen Anwender auf mögliche kritische Situationen aufmerksam werden. Dies kann grundsätzlich oder

fallorientiert – z. B. mit Hinweisdialogen in Anwendungen – erfolgen.

Hinweisdialoge können durch zusätzliche Elemente ergänzt werden, die den Nutzer zur expliziten **Bestätigung** zwingen, dass er eine bestimmte Funktion gerade auf die ausgewählten Daten anwenden will.

Die stärkste Maßnahme besteht in der **Blockierung** aller nicht unbedingt benötigten Funktionen.

Schließlich müssen noch Schritte für den Verlustfall vorgesehen werden: Durch entsprechende **Alarmierung** müssen weitere Maßnahmen ausgelöst werden, die den Schaden durch den akut drohenden oder bereits eingetretenen Datenverlust begrenzen. Dies kann z. B. im Falle verlorener Geräte die Deaktivierung von Systemzugängen oder die Fernlöschung von Daten umfassen.

Bei der Umsetzung von Maßnahmen der Data Loss Prevention raten Experten dazu, mit Augenmaß vorzugehen. Oft reichen vorhandene Maßnahmen schon aus, wenn sie nur konsequent umgesetzt werden. Der Versuch, absolute Sicherheit anzustreben, führt in der Regel nur zu Aktionismus und ist von vornherein zum Scheitern verurteilt. Das liegt schon allein daran, dass man im Zusammenhang mit Sicherheit immer Wahrscheinlichkeiten dafür betrachtet, dass gewisse Schäden entstehen. Dabei geht man von einer großen Anzahl von Ereignissen mit zufälligem Ausgang aus und stellt Fragen der Art: „Wie wahrscheinlich ist es, dass ich durch einen Virus in einer meiner ganz vielen E-Mails meine Daten verliere?“ Beim Thema Data Loss Prevention geht man immer von Einzelfällen aus und stellt die Möglichkeit eines Schadens in den Vordergrund. Man fragt also z. B.: „Welcher Schaden kann entstehen, wenn ich meinen Rechner am Bahnhof liegenlasse?“ Bei der Umsetzung von Maßnahmen im Zuge von Data Loss Prevention sollte daher auch immer ihre Angemessenheit bedacht werden.

Bewertung

Verwaltungen haben seit jeher mit vielen und sensiblen Daten zu tun. Der Datenschutz für den Umgang mit personenbezogenen Daten ist hier seit langem etabliert. Doch die Menge an elektronischen Informationen, die sehr einfach weiterverarbeitet und genauso einfach verbreitet werden können, wird immer größer, und die Themenfelder, aus denen diese Daten stammen, weiten sich ständig aus. Dies schließt auch sensible Daten ein, und Verwaltungen sind folglich gezwungen, immer mehr Informationen zu schützen, die nicht personenbezogen sind. Daher wird auch für Verwaltungen Data Loss Prevention zunehmend ein Thema von Bedeutung. Während technische Schutzmechanismen hier in der Regel schon recht weit verbreitet sind und gegebenenfalls nur in kritischen Bereichen spezifisch und angemessen ergänzt werden müssen, sollten Maßnahmen, die auf das angemessene Verhalten der Mitarbeiter ausgerichtet sind, etabliert bzw. verstärkt werden. Es ist wichtig, die Risiken im Umgang mit sensiblen Daten zu kennen und dementsprechend damit umzugehen.

Verwaltungsrelevanz:	
Umsetzungsgeschwindigkeit:	
Marktreife/Produktverfügbarkeit:	

Seminare zum Trendbericht

Das Schulungszentrum der HZD bietet eine breite Palette von aktuellen Seminaren. Nachfolgend finden Sie einige ausgewählte Seminare, die Ihnen als Ergänzung und Vertiefung zu den Artikeln des Trendberichts dienen können. Weitere Seminare zu diesen und anderen Themen finden Sie im Seminarprogramm 2010 und unter www.schulung.hzd.de. Auf Anfrage bieten wir Ihnen die Seminare auch zu individuellen Terminen und mit an Ihre Anforderungen angepassten Inhalten an.

MOSS Hands On Seminar

Sie erhalten einen praxisorientierten Überblick über Aufbau und Einsatzmöglichkeiten eines MOSS-Teamraums. Sie erfahren, wie Sie Elemente in verschiedene Bibliotheken und Listen einstellen bzw. bearbeiten und wie Sie die Funktionen der Aufgaben-, Terminplanung und -verfolgung in MOSS nutzen. Einige Übungen runden das Seminar ab.

Seminar-Nr.: 1-EG-MO-SS-HO-10 **Termin: 25.02.2010** **Dauer: 1/2 Tag, 9–13 Uhr**

Kleine und mittlere Projekte in MOSS verwalten

Der Einsatz von Standardwerkzeugen in MOSS kann die Grundlage für eine gelungene Projektverwaltung bilden. Geeignet sind dafür kleine und mittlere Projekte. So reichen oft Aufgabenlisten aus, in die Mitarbeiter/-innen den Fortschritt eintragen, um Projekte gezielt zu steuern. Verbindungen mit Dokumenten, Listen etc. und Projektübersichtsseiten ermöglichen mit wenig Aufwand Zusammenstellungen und zeigen Zusammenhänge auf. Lernen Sie in diesem Seminar diese Werkzeuge anhand eines Projektbeispiels kennen, und sichern Sie sich damit eine erfolgreiche Projektverwaltung.

Seminar-Nr.: 1-ED-MO-SS-PRJ-10 **Termin: 04.05.2010** **Dauer: 1 Tag, 9–16 Uhr**

IT-Sicherheit am Arbeitsplatz

Abgestimmte Richtlinien zur Sicherung der Verfügbarkeit, zur Vertraulichkeit und Integrität von Informationen haben in der hessischen Landesverwaltung eine hohe Priorität. Wichtig ist dabei, dass definierte Sicherheitsrichtlinien im entsprechenden Kontext umgesetzt und gelebt werden. Im Seminar lernen Sie typische Risiken im Umgang mit moderner Informationstechnologie kennen. Sie kennen wichtige Grundsätze für den sicheren IT-Einsatz (u.a. die Vorgaben der IT-Sicherheitsrichtlinie des Landes) und werden zum sorgfältigen Umgang mit IT-Ressourcen an Ihrem Arbeitsplatz angeregt.

Seminar-Nr.: 1-AM-RE-IT-ÜB-10 **Termin: 12.04.2010** **Dauer: 1 Tag, 9–16 Uhr**

IT-Sicherheit von mobilen Kommunikationsgeräten

Mobile Kommunikationsgeräte werden auch in der öffentlichen Verwaltung verstärkt eingesetzt. Im Seminar lernen Sie typische Risiken im Umgang mit modernen Kommunikationsgeräten (z. B. Handy, BlackBerry) kennen. Nach dem Besuch des Seminars kennen Sie mögliche Schutzmaßnahmen zum sicheren Gebrauch moderner Kommunikationsgeräte.

Seminar-Nr.: 1-AM-RE-IT-MG-10 **Termin: 13.4.2010** **Dauer: 1 Tag, 9–16 Uhr**

Wikis – eine Einführung

Das Seminar gibt eine Einführung in das Grundkonzept von Wikis und zeigt Möglichkeiten für den Einsatz im Projektalltag. Anhand von praktischen Beispielen werden technische, organisatorische und rechtliche Fragen diskutiert.

Seminar-Nr.: 1-IN-AB-ES-WIKI-10 **Termin: 18.01.2010** **Dauer 1/2 Tag, 9–13 Uhr**

Das Web vergisst nichts

Welche Spuren hinterlassen wir im Internet? Was können andere dadurch über uns erfahren? Wie können wir Einträge aufspüren, und was sollte man beachten? Generelle Informationen, eine Personensuche und Ratschläge geben Ihnen einen umfassenden Eindruck vom Thema.

Seminar-Nr.: 1-IN-AB-ES-RE-10 **Termin: 22.01.2010** **Dauer: 1/2 Tag, 9–13 Uhr**