

Die neuen Möglichkeiten

– innovative Anwendungsfelder für Webtechnologien

■ Von Steffen A. Müller



Photocase.com

Aus der Verbindung zwischen einer Handvoll Rechnern 1969 an amerikanischen Universitäten hervorgegangen, vollzog das Internet in den folgenden Jahren eine rasante Entwicklung. Das Internet wurde schnell zum Inbegriff moderner, grenzenloser, weltweiter Kommunikation. Informationstechnologien wurden in immer schnellerer Abfolge in marktreife Produkte umgesetzt. Es entstand der „neue Markt“ – erst nach dem „Platzen der Dotcom-Blase“ im März 2000 und der daraus folgenden Ernüchterung wurde es etwas ruhiger um das Internet. Gleichwohl entwickelten sich gerade in den letzten Jahren innovative Möglichkeiten, die Inter- und Intranetlösungen (Webtechnologien) für Unternehmen noch interessanter zu machen¹. Der folgende Beitrag zeigt dazu einige Entwicklungsfelder auf.

1) Die Unterscheidung zwischen Inter- und Intranet ist dabei eher zweitrangig. Ein Intranet bezeichnet ein auf derselben Technologien wie das Internet basierendes Netzwerk, das jedoch nur innerhalb eines begrenzten Nutzerkreises – meist einem Unternehmen – eingesetzt wird. Zusammenfassend wird daher hier der Begriff „Webtechnologien“ verwendet.

Netzabdeckung – wachsende Verbreitung

Ein wesentlicher Aspekt für die Nutzung von Webtechnologien ist die Verfügbarkeit von Internetanschlüssen. Breitband-DSL-Anschlüsse haben in den letzten Jahren stark zugenommen. Derzeit ist DSL auf 47 Prozent der Gesamtfläche Deutschlands verfügbar². Versorgungslücken bestehen noch in ländlichen Gebieten. Bis 2008 soll die Verfügbarkeit laut Bundesregierung auf 98 Prozent ausgebaut werden.³

Kabellose Netzwerke (WLAN) setzten sich in den vergangenen Jahren immer mehr durch. Mittlerweile können mit einem minimalen finanziellen Aufwand komplette Betriebsgelände mit einem WLAN abgedeckt werden.

Auch die Akzeptanz des Internet innerhalb der Bevölkerung (Endkunden, Customer) nimmt rasant zu: 2006 sind bereits 58 Prozent der Deutschen regelmäßig online⁴ – bis 2008 wird eine Nutzung von 76 Prozent prognostiziert.⁵ Dabei ist laut einer Untersuchung von TNS Infratest die Gruppe der Internet-Verweigerer klar umrissen: vor allem ältere Menschen, haupt-

sächlich Frauen, mit vergleichbar niedrigerer Bildung und geringem Einkommen.

Da die Infrastruktur für Webtechnologien mittlerweile günstig und an nahezu jedem Ort verfügbar und die Akzeptanz bei potenziellen Anwendern deutlich gestiegen ist, sind Lösungen praktikabel geworden, die bisher nicht realisierbar waren (Bild 1).

Software – Open Source auf dem Vormarsch

„Die besten Dinge im Leben bekommt man geschenkt.“ – Diese Volksweisheit bewahrt sich im Softwarebereich für Webtechnologien: Die benötigte Basis-Softwareausstattung von Webservern – also Rechnern, die über ein Inter- oder Intranet Dienste zur Verfügung stellen – ist vielfach kostenlos verfügbar. Für einen Großteil der Einsatzszenarien für Webanwendungen besteht ein sinnvoller Unterbau für die Anwendung aus einem kostenlosen Betriebssystem wie Linux, auf dem ein so genannter Webserver wie Apache dynamische Webseiten erstellt und zur Verfügung stellt. Der Anteil der mit Apache betriebenen Webseiten an der Gesamtzahl der im Inter-

net verfügbaren Webseiten betrug im August 2006 weltweit 61 Prozent⁶.

Bei dieser „Open Source“-Software kann jeder Interessierte die Entwicklungsunterlagen (den Quelltext) der Software einsehen und verwenden, ja sogar an der Entwicklung der Software aktiv teilnehmen. Die Entwickler dieser Software programmieren aus Begeisterung, Lerneifer und Spaß – ohne finanzielle Entschädigung.

Große Open-Source-Projekte wie Linux und Apache bieten durch ihr Konzept überzeugende Vorteile: Die Anschaffungskosten bzw. Lizenzgebühren fallen weg, Aktualisierungen sind auf unbegrenzte Zeit kostenlos erhältlich und die Software gilt prinzipiell als sicher, da viele Experten den offenen Quelltext der Programme analysieren und frühzeitig auf Sicherheitslücken hinweisen.

Der Einsatz von Open-Source-Software birgt jedoch auch Risiken: So stellt die zur Einrichtung der Software benötigte Arbeitszeit einen häufig unterschätzten Kostenpunkt dar. Außerdem bietet Open-Source-Software keinerlei Ga-

rantien. Wird Unterstützung benötigt, muss meistens ein Spezialist zu Rate gezogen werden, der wiederum Kosten verursacht.

Da die Entwickler nicht verpflichtet sind, ihre Projekte zu Ende zu bringen, schief schon so manches kleinere Open-Source-Projekt einfach ein, weil der Hauptentwickler sein Amt niederlegte. Diese Gefahr besteht bei so großen Projekten wie Linux oder Apache nicht, dennoch sollte man stets genauestens prüfen, an welche Open-Source-Software man sich bindet.

AJAX – komfortables Arbeiten

Einer der größten Kritikpunkte an Webanwendungen war und ist die im Vergleich zu herkömmlichen Windowsanwendungen ungewöhnliche und träge erscheinende Bedienung. Bei Webanwendungen wird der gesamte Inhalt der Anwendung auf einem anderen Rechner, dem Webserver, generiert und lediglich im Browser (z. B. Internet Explorer, Firefox oder Opera) auf dem lokalen Rechner angezeigt. Daher erfordert jeder Seitenwechsel und jede Benutzereingabe eine Rückfrage beim Webserver. Die Übertragung erfolgt über das Inter- oder Intranet. Der Benutzer empfindet hier eine aus normalen Windowsanwendungen nicht gekannte Systemträg-

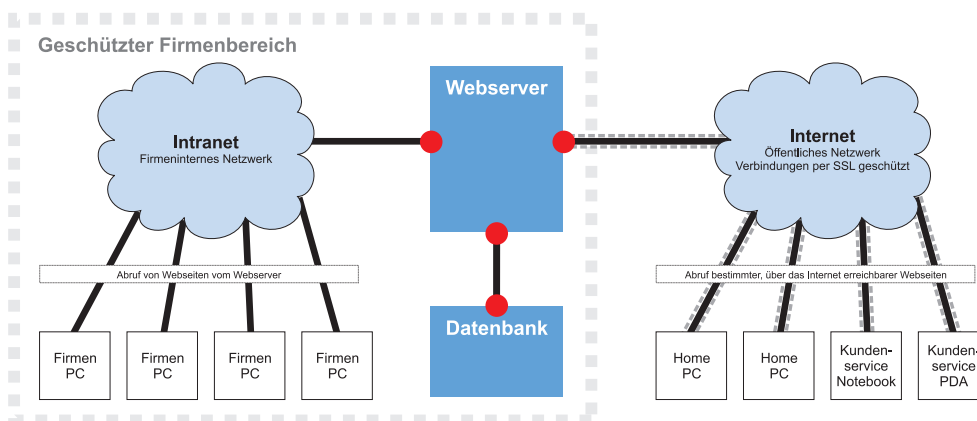


Bild 1: Schematischer Aufbau einer Webanwendung

2) Bundesministerium für Wirtschaft und Technologie – Bericht zum Breitbandatlas 2006_01

3) Pressemitteilung des Bundesministeriums für Wirtschaft und Technologie vom 14. März 2006

4) (N)Onliner-Atlas der Initiative D21 und TNS Infratest

5) European Information Technology Observatory März 2005

6) Netcraft Web Server Survey September 2006

heit, die ihn in seiner Arbeitsproduktivität beeinträchtigt.

Abhilfe schaffte hier erst die Möglichkeit zur lokalen, clientseitigen Programmierung des Webbrowsers. Die in JavaScript geschriebenen Programme werden von den Webbrowsern einheitlich interpretiert, verschiedene Webbrowser kommen also zu denselben Ergebnissen. Dagegen war es bis vor kurzem nötig, für jeden Browser eine eigene Version des Programms zu schreiben, um gleiche Ergebnisse zu erzielen.

Diese neuen, verbesserten Bedingungen führen dazu, dass die Programmierung per JavaScript immer größere Teile der Webanwendung übernehmen kann und quasi einen Teil der Programmintelligenz auf den lokalen Client verlagert. Eine herausragende Technik dieser Entwicklung ist „AJAX“ (*Asynchronous JavaScript and XML*). Hiermit wird das Anfordern komplett neuer Webseiten überflüssig: Die Webseite kann neue Informationen im Hintergrund vom Webserver anfordern und diese dann innerhalb der vorhandenen Seite darstellen. Das zu übertragende Datenvolumen ist wesentlich geringer, der Server wird weniger belastet.

Damit können Webanwendungen bereitgestellt werden, die sich nahezu wie normale Windowsanwendungen bedienen lassen. Neben der gesteigerten Produktivität für den Anwender führt das zu einer höheren Akzeptanz der Webanwendungen im Benutzerkreis, da sich die Einarbeitungs- und Umgewöhnungsphase verkürzt. Ein weiterer Vorteil: Einige rechenintensive Aufgaben der Webanwendung können auf den Webbrowser „ausgelagert“ werden. Dadurch werden die Webanwendungen insgesamt leistungsfähiger.

AJAX birgt jedoch auch Risiken: Die Verteilung der Webanwendung auf zwei getrennte Bereiche (den Webbrowser und den Server) macht die Entwicklung deutlich komplizierter. Auch bietet sie zusätzliche Angriffsfläche für Hacker. Unterstützt ein Webbrowser kein JavaScript, kann die Webanwendung nicht eingesetzt werden. Gerade Webbrowser für spezielle Nutzergruppen, wie zum Beispiel Sehbehinderte, unterstützen JavaScript nicht. Außerdem kann es bei großen Datenmengen oder komplexen Anwendungen zu Leistungsproblemen mit dem langsamen JavaScript kommen.

ANZEIGE

Ist man sich dieser Aspekte jedoch bewusst, kann mit Hilfe der Programmierung auf Clientseite eine neue Qualität in Webanwendungen erreicht werden, die vor einigen Jahren noch undenkbar war und neue Einsatzgebiete erschließt.

XML – Datenspeicherung für die Zukunft

Ein weiteres großes Schlagwort im Internetbereich der letzten Jahre lautet „XML“. Das Kürzel steht für „Extensible Markup Language“ (erweiterbare Auszeichnungssprache). Mit XML lassen sich beliebige Datenstrukturen ausdrücken und abspeichern. Diese Daten sind für andere Anwendungen wieder leicht einzulesen und zu verarbeiten.

Die Unabhängigkeit von einem bestimmten Programm wissen viele Unternehmen insbesondere angesichts von nicht mehr lesbarem „Datenmüll“ aus den letzten Jahrzehnten zu schätzen. In XML gespeicherte Daten können sicher auch in 20 Jahren noch ohne großen Aufwand gelesen werden.

Ein Hauptanwendungsgebiet von XML ist der Datenaustausch zwischen verschiedenen Systemen und Standards. Da in XML vorliegende Daten von allen Beteiligten problemlos verarbeitet werden können, lassen sich dadurch unterschiedliche Datenhaltungssysteme verbinden. Anwendungsspezifische Datenformate, die bei einem Datenaustausch mit z. B. einem Lieferanten oder Kunden immer eine Schnittstellenproblematik beinhalten, gehören also mit XML der Vergangenheit an.

XML ist jedoch nicht immer das optimale Datenformat. Gerade zur Speicherung von Daten, die aktiv in Anwendungen eingesetzt werden, ist XML – bezogen auf den verbrauchten Speicherplatz als auch auf die Geschwindigkeit von Lese- und Schreibvorgängen – nur bedingt geeignet.

Szenario des Machbaren

Wie lässt sich nun die aktuelle Internet-/Intranet-Technik in den Unternehmensprozessen zur Steigerung von Transparenz und Effizienz einsetzen?

Beginnen wir beim Wareneingang. Die mit einem RFID-Chip ausgestatteten Wareneingänge werden über einen RFID-Leser am Eingang des Lagers erkannt und erfasst. Der Leser übermittelt die Daten über das Netzwerk an den zentralen Unternehmensserver. Nicht mit RFID ausgezeichnete Waren werden manuell über ein BDE-Terminal erfasst und ebenfalls an den Server übermittelt.

Sensoren an den Fertigungsmaschinen in den Werkshallen liefern per Netzwerk Informationen über den Status der Maschinen. Über BDE-Terminals an den Maschinen wählen die Mitarbeiter Aufträge zur Bearbeitung aus, die ihnen über ein ERP-System mit angeschlossenem MES im Rahmen eines integrierten Auftragsmanagements angeboten werden.

Die Auftragsdaten werden von einer zentralen Webanwendung, die auf dem Unternehmensserver läuft, analysiert und aufbereitet. Die Webanwendung stellt im Intranet des Unternehmens ein Monitormodul zur Verfügung, das die aktuellen Auftrags-

und Kapazitätsdaten visualisiert. Die Darstellung im Webbrowser wird dabei automatisch aktualisiert. Für verschiedene Zielgruppen stehen die jeweils relevanten Ansichten zur Verfügung: Management-Summaries für das Management, dezidiertere Informationen je Abteilung für die Abteilungsleiter. Die Mitarbeiter in der Werkshalle sehen auf einer per Beamer projizierten Ansicht, ob alles im Plan liegt.

Das Monitormodul als Webanwendung steht nicht nur auf speziell dafür hergerichteten Rechnern zur Verfügung – es kann von jedem PDA, Handy mit WAP-Funktion und Pocket-PC mit entsprechenden Zugangsberechtigungen abgerufen werden. Über das Management-Summary kann das Management jederzeit auch von unterwegs aus beurteilen, ob der Betrieb reibungslos läuft.

Durch das integrierte Auftragsmanagement ist jederzeit bekannt, welche Aufträge sich in welcher Bearbeitungsphase befinden. Über eine komfortable Suche können die Details zu Aufträgen gefunden und angezeigt werden. Dabei wird der aktuell zu erwartende Zeitpunkt der Fertigstellung errechnet. Kunden können so bei Nachfragen detaillierte Informationen über den Bearbeitungsstand ihrer Aufträge erhalten – online und in Echtzeit.

Der Außendienst greift auf eine Zusammenfassung dieser Daten von unterwegs per PDA zu und kann so direkt im Kundengespräch den Stand der Aufträge erörtern. Bei Bedarf können Prioritäten bei den Aufträgen verändert und Zusatzinformationen hinterlegt werden.

Eine ständige Analyse der eingehenden Daten versetzt die Webanwendung in die Lage, Probleme frühzeitig zu erkennen. In Grenzen kann die Anwendung dann selbst Prozessparameter verändern, um den Gesamtprozess optimal ablaufen zu lassen.

Bei größeren Abweichungen und Problemen werden die Entscheidungsträger direkt per SMS oder E-Mail benachrichtigt.

Die betriebsinterne Bestellung von Arbeitsmitteln wie Büromaterial oder Werkzeugen kann über eine E-Procurement-Lösung rationell erledigt werden.

Jeder Mitarbeiter kann von überall – auch von seinem PC zuhause aus – auf seine persönliche Seite zugreifen. Dort kann er seinen Dienstplan und sein Mehrarbeitskonto einsehen, Urlaubsanträge können ebenso wie Krankmeldungen oder Reisekostenabrechnungen abgewickelt werden.

Aufgrund der wertvollen Informationen wird die Seite von den Mitarbeitern häufig besucht, so dass ein an die Webseite gekoppeltes Forum für Verbesserungsvorschläge zahlreiche und wertvolle Anregungen für das Management einbringt.

An einem virtuellen „schwarzen Brett“ können die Mitarbeiter auch nach Mitfahrgelegenheiten in einer Fahrgemeinschaft suchen oder Treffen der Betriebssportgruppe planen. Damit können über die Webanwendung nicht nur das Personalmanagement wirkungsvoll unterstützt, sondern auch wesentliche Beiträge zur Förderung der Unternehmenskultur geleistet werden.

Sicherheitsaspekte

Die neuen Möglichkeiten der Webtechnologien bergen auch neue Gefahren. Für einen Datendiebstahl muss nicht mehr in das Betriebsgebäude eingebrochen werden: Der Einbruchversuch erfolgt über das Internet. Zwar ist nur ein nicht an ein Netzwerk angeschlossener Computer ein sicherer Computer, damit entfällt jedoch der Nutzen für Webanwendungen. Hier gilt wie beim Schutz von Firmengebäuden vor Einbruch: Mit den richtigen Gegenmaßnahmen kann man sich effektiv vor Angriffen schützen.

Für eine effektive Abwehrstrategie müssen zunächst die potenziellen Angriffsweg bekannt sein. Prinzipiell sind schlecht abgesicherte Webserver ein beliebtes An-

griffsziel. Bekannt gewordene Sicherheitslücken in der Software, die auf dem Webserver betrieben wird, können ausgenutzt werden, um vollen Zugriff auf die Daten des Webservers oder den kompletten Webserver zu erhalten. Dagegen kann der Webserver geschützt werden, indem die Anzahl der über das Netzwerk erreichbaren Anwendungen möglichst klein gehalten wird. Je weniger Software erreichbar ist, desto geringer ist die Wahrscheinlichkeit einer gefährlichen Sicherheitslücke.

Über ein ausgefeiltes System zur Vergabe von Zugriffsrechten auf dem Server lassen sich die Auswirkungen einer Sicherheitslücke eingrenzen. Die eingesetzte Software sollte dabei stets auf dem aktuellen Stand gehalten werden.

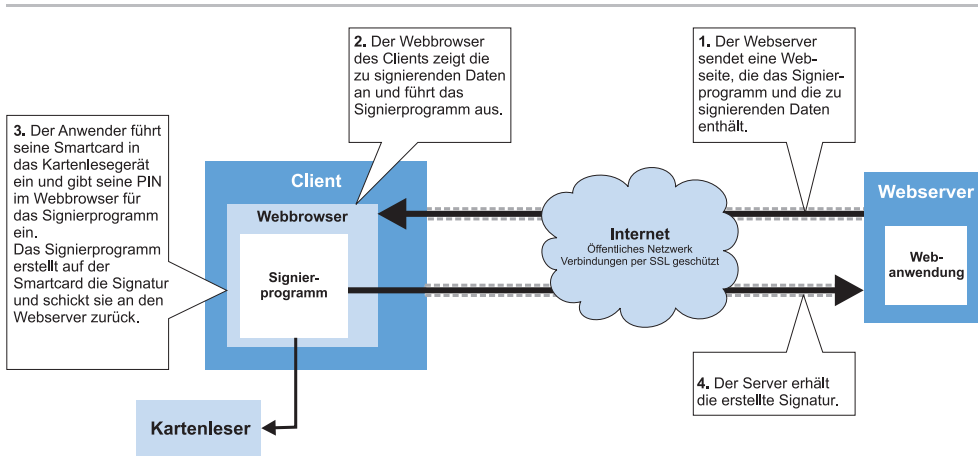


Bild 2: Erstellung einer digitalen Signatur

Häufiger als Angriffe auf den Webserver selbst sind Versuche, Passwörter von Benutzern der Webanwendung auszuspiionieren oder zu erraten. So kann zum Beispiel Spezialsoftware eingesetzt werden, um Wörterbücher von Tausenden möglichen Passwörtern zu testen, bis ein Zugang gefunden

wird. Die Webanwendung kann dagegen geschützt werden, indem nur eine begrenzte Anzahl falscher Anmeldeversuche zugelassen wird. Doch auch das „Belauschen“ von Anmeldungen legitimer Benutzer durch Mithören des Netzwerkverkehrs ist ein verbreiteter Angriffsweg. Dem

kann durch SSL-verschlüsselte Verbindungen entgegengewirkt werden (SSL = Secure Sockets Layer, Verschlüsselungsprotokoll für Datenübertragungen im Internet).

Ein weiteres, für gewöhnlich größeres Sicherheitsrisiko stellt der Faktor Mensch dar. Die Weitergabe von vertraulichen Zugangsdaten, das Notieren von Passwörtern auf Zetteln unter der Tastatur und ähnliche Vorgehensweisen sind bei größeren Nutzergruppen kaum auszuschließen. Diese Risiken lassen sich wirkungsvoll durch eine „2-Faktoren-Authentifizierung“ umgehen, also eine Authentifizierung des Benutzers, die zwei verschiedene Aspekte kombiniert: für gewöhnlich etwas, das der Benutzer weiß (ein Passwort), und etwas, das der Benutzer besitzt. Das Passwort wird hier mit einem zweiten Aspekt kombiniert, beispielsweise wie beim Online Banking mit einer TAN-Liste, also einer langen Liste von durchnummerierten Zahlenkombinationen. Bei der Anmeldung wird die Eingabe einer bestimmten Zahlenkombination von der Liste verlangt.

Noch sicherer, da nicht kopierbar, sind so genannte Se-

curity Tokens, kleine Geräte für den Schlüsselanhänger, die eine jede Minute wechselnde Zahl anzeigen. Die Zahl ist pseudo-zufällig, es lässt sich also nur von dem Security Token selbst und der Webanwendung die nächste Zahl bestimmen. Der Benutzer, der sich mit Passwort und der aktuellen Security-Token-Zahl anmelden kann, ist also sehr sicher der berechtigte Benutzer.

Wenn solche Systeme zu aufwändig sind, kann eine stärkere persönliche Bindung zu den Anmeldedaten das Sicherheitsbewusstsein der Benutzer erhöhen. Wird in der Webanwendung jeder aktuell angemeldete Benutzer mit vollem Namen angezeigt oder ist bei Datensätzen der Bearbeiter der letzten Änderung mit vollem Namen ersichtlich, scheuen sich Benutzer mehr davor, andere unter ihrer Identität die Webanwendung nutzen zu lassen.

Digitale Unterschriften: Wege zur rechtlichen Verbindlichkeit

Ein weiterer Sicherheitsaspekt ist die rechtliche Verbindlichkeit von Benutzereingaben. Zum Beispiel könnte ein Unternehmen seinen Kunden anbieten, Aufträge selbstständig über die Weboberfläche zu erteilen. Doch wer haftet, wenn Aufträge generiert werden, von denen der Kunde angeblich keine Kenntnis hat?

Der Vermerk in der Datenbank der Webanwendung, dass der Kunde den Auftrag eingestellt hat, ist zwar hilfreich, aber nicht Beweis genug. Schließlich könnte die Datenbank von der IT-Abteilung des Unternehmens manipuliert wor-

den sein. Lösungen für solche Fälle beschränkten sich bislang auf Verträge, die die Anwendung als sicher anerkennen, oder das Betreiben der Anwendung durch einen neutralen Dritten (was wieder andere Risiken mit sich bringt). – Ein schaler Beigeschmack bleibt.

Eine neue Möglichkeit bietet die digitale Signatur (Bild 2). Dabei verfügt jeder Benutzer über ein Schlüsselpaar: ein privater Schlüssel, der nur dem Besitzer bekannt ist, und der dazugehörige öffentliche Schlüssel. Unterschreibt der Benutzer mit seinem privaten Schlüssel, wird eine nicht reproduzierbare Prüfsumme der unterschriebenen Daten generiert. Diese Prüfsumme kann mit Hilfe des öffentlichen Schlüssels auf Echtheit geprüft werden. Die Unterschrift kann nicht gefälscht werden, ist also ein eindeutiger Beweis für die Echtheit der Daten. Denn werden die unterschriebenen Daten manipuliert, schlägt die Überprüfung der Unterschrift fehl.

Die Lösung sähe also praktisch so aus: der Kunde generiert wie gewünscht Aufträge. Vor dem Abschluss der Einstellungen präsentiert ihm die Webanwendung noch einmal eine Zusammenfassung der zu unterschreibenden Daten. Ein spezieller clientseitiger Teil der Webanwendung, der also nur im lokalen Webbrowser läuft, fordert den Benutzer zur Signierung der angezeigten Daten auf. Der Kunde führt seine Smartcard, eine Karte im Scheckkartenformat, in einen Kartenleser neben seinem Rechner ein und gibt in der Webanwendung seine PIN für

den auf der Karte gespeicherten privaten Schlüssel ein. Der clientseitige Teil der Webanwendung hat nun die Möglichkeit, mit dem jetzt verfügbaren privaten Schlüssel des Benutzers die Unterschrift zu erstellen. Dabei hat die Webanwendung aber keinen direkten Zugriff auf den privaten Schlüssel, dieser verlässt nicht die Smartcard. Die Unterschrift wird an den Server übermittelt und wird dort zusammen mit den neuen Aufträgen gespeichert. Nun ist also sicher beweisbar, dass der Mitarbeiter des Kunden die Zusammenfassung des Auftrags unterschrieben hat und damit auch der Auftraggeber ist.

Diese technischen Möglichkeiten machen Webanwendungen für Bereiche nutzbar, in denen bislang ein zeitraubender persönlicher Kontakt zum Kunden notwendig war.

Web 2.0 und die Zukunft

Im Zusammenhang mit neuen Webanwendungen ist das Schlagwort „Web 2.0“ derzeit in aller Munde. Für Unternehmen ist Web 2.0 vor allem eine neue Herangehensweise an den Umgang mit Unternehmensdaten und mit der IT-Struktur. Absehbar ist, dass immer mehr Funktionalitäten von klassischen Desktop-Anwendungen verlagert werden auf Anwendungen, die im Web liegen – zur Nutzung wird nur noch ein Browser benötigt. Die Dokumente und Daten werden nicht mehr auf dem lokalen Rechner gespeichert, sondern auf zentralen Webservern.

Ein eindrucksvolles Beispiel ist die Browser-Textverarbeitung Writely, die sich zu einem Ersatz für klassische Textverarbeitungssysteme entwickelt.⁷

Die Vorteile dieser Vorgehensweise liegen auf der Hand: die Kosten für die Pflege der lokalen Softwareinstallationen auf den PCs des Unternehmens entfallen. Datenverluste durch beschädigte Festplatten auf lokalen Rechnern können ausgeschlossen werden. Das gemeinsame Bearbeiten von Dokumenten und Daten mit mehreren Mitarbeitern wird problemlos möglich. Neuerungen in der Software sind ohne Umstände sofort auf allen Rechnern verfügbar, jeder Mitarbeiter nutzt dieselbe Arbeitsumgebung.

Natürlich birgt diese zentralisierte Struktur wieder die bereits beschriebenen Risiken. Außerdem steht die Entwicklung in diese Richtung noch an ihrem Anfang. Blinder Enthusiasmus ist unangebracht.

Eine behutsame und verantwortungsbewusste Evaluation und Einführung neuer Lösungen ist der Schlüssel dazu, den Anschluss an die technologische Entwicklung zu behalten – schließlich ist der Zug der digitalen Revolution in voller Fahrt.

■ VERFASSER



Steffen A. Müller
Leiter Geschäftsbereich
Software
dogmaConsult, Gladenbach
Kontakt:sam@dogmaconsult.de

7) Writely, the web word processor – www.writely.com