Kernkompetenzzentrum
Finanz- & Informationsmanagement

Fraunhofer FIT
Projektgruppe
Wirtschaftsinformatik

Personal Data Environment – die Suche nach der digitalen Zukunft

von

Hans Ulrich Buhl, Alexander Wehrmann

2003

in: Wirtschaftsinformatik, 45, 5, 2003, p. 575-579

Universität Augsburg, D-86135 Augsburg
Besucher: Universitätsstr. 12, 86159 Augsburg
Telefon: +49 821 598-4801 (Fax: -4899)

Universität Bayreuth, D-95440 Bayreuth
Besucher: Wittelsbacherring 10, 95444 Bayreuth
Telefon: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

WI-871

Meinung/Dialog

Personal Data Environment – die Suche nach der digitalen Zukunft

Neue IT-Technologien und die Etablierung offener Standards und Web-Services, die über Systemgrenzen hinweg miteinander kommunizieren und interagieren können, eröffnen ein Spektrum neuer Möglichkeiten, um Kunden – beispielsweise durch individualisierte Dienstleistungen – Value Added Services zu bieten.

Da individualisierte Dienstleistungen meist mit datenintensivem Informationsaustausch verbunden sind, ist eine bequeme und sichere Handhabbarkeit für deren Erfolg entscheidend. Eine vielversprechende Möglichkeit, diesen Anforderungen zu begegnen, ist die Idee des *personal data environment* (PDE). Diese Online-Authentifizierungssysteme ermöglichen, einmal beim PDE-Provider gespeicherte Kundendaten mittels einer Zugriffserlaubnis kontrolliert an andere Unternehmen weiterzugeben.

Doch die Akzeptanz dieser Dienste bleibt bisher weit hinter den Erwartungen zurück. Führenden Anbietern von PDE-Systemen, wie Sun Microsystems mit dem Konzept der Liberty Alliance oder Microsoft mit der .Net Passport-Initiative, um nur zwei zu nennen, ist es bislang nicht gelungen, einen vielgenutzten Dienst zu etablieren.

Vielmehr dominieren immer wieder Negativmeldungen über Sicherheitsmängel und Datenschutzprobleme. In nur wenigen Minuten, so wurde jüngst berichtet, könnte man die Benutzerkonten von Microsoft Passport knacken. Zusammen mit der oftmals unverhältnismäßigen Erhebung von personenbezogenen Daten im Internet führt dies zu einer steigenden Sensibilisierung und Verunsicherung der Menschen im Umgang mit ihren Daten. Derartige Probleme können aber auch schwerwiegende finanzielle Folgen für das Unternehmen nach sich ziehen, wenn nachweislich gegen rechtliche Auflagen verstoßen wurde.

Vor diesem Hintergrund stellt sich nun die Frage, wie erfolgreiche PDE-Dienste in einer komplexen, virtuellen Umgebung in Zukunft aussehen müssen und wie diese den Umgang mit sensiblen Daten managen. Welchen Mehrwert muss *personal data environment* bieten, um sich in Zukunft zu einem weitverbreiteten Dienst zu entwickeln?

Werden Konsumenten künftig – ganz im Sinne von Scott McNealy, CEO von Sun Microsystems: „You have zero privacy anyway – get over it" – den Verlust ihrer Privatsphäre in Kauf nehmen müssen, um bestimmte Dienste in Anspruch nehmen zu können?

Nicht zuletzt an der äußerst unterschiedlichen Herangehensweise an Fragen des Datenschutzes wird die große Spannweite der Auffassungen zum Thema „privacy" ersichtlich.

In den USA existieren, abgesehen von vereinzelten bereichsspezifischen Verordnungen, weder ein einheitliches Datenschutzrecht, noch findet eine nennenswerte staatliche Kontrolle datenschutzrelevanter Vorgänge statt. Vielmehr wird auf die freiwillige Selbstverpflichtung der Industrie vertraut. Staatliche Eingriffe erfolgen nur in Ausnahmefällen, wenn die Selbstregulierung versagt. Die Unternehmen in Europa hingegen sehen sich einem sehr strengen Datenschutzrecht konfrontiert, das aufgrund der zu erwartenden Sanktionen zur Umsetzung von Sicherungsmaßnahmen zwingt, die in den USA nicht oder zumindest nicht in diesem Umfang erforderlich wären. Fehlt es also an rechtlichen Rahmenbedingungen, die international anerkannt und von einer zentralen Instanz überwacht werden? Oder lässt sich dieses Problem tatsächlich auf dem Wege der freiwilligen Selbstverpflichtung der Unternehmen beseitigen?

Noch ist unklar, welche Anbieter die Player auf dem Markt für PDE-Systeme zukünftig sein werden, denn zurzeit scheint keine Strategie erfolgsversprechend.

Zusammenfassend kann festgehalten werden, dass sich nur Systeme durchsetzen werden, die eine sinnvolle Kombination aus wertsteigernden Diensten und dem sorgfältigen Umgang mit persönlichen Daten bieten. Wie diese konzipiert sein könnten, soll Inhalt dieser Diskussion sein. Vertrauen wir in Zukunft unsere Daten Konzernen wie Microsoft mit zentraler Datenhaltung an und erhalten im Gegenzug ein komfortables „Sorglospaket"? Oder müssen wir auf Komfort verzichten, um selbst über den Zugriff und die Speicherung persönlicher Daten verfügen zu können?

Lesen Sie dazu nachfolgend die Gedanken dreier prominenter Vertreter aus Politik und Wirtschaft, die sich als visionäre Vordenker und Autoren einschlägiger Artikel auf diesem Gebiet einen Namen gemacht haben. Dr. Helmut Bäumler setzt sich in seinem Beitrag mit den rechtlichen Rahmenbedingungen und den wirtschaftlichen Herausforderungen, welchen sich PDE-Systeme stellen müssen, auseinander. Anschließend diskutiert Herr Thomas Groth die Gegensätze von proprietärer und Open-Source-Software für PDE-Systeme. Abschließend erörtert Dr.-Ing. Horst H. Henn gängige und mögliche Lösungen zur Ausgestaltung der Sicherheit von PDE-Systemen.

Wie sehen Sie die gegenwärtigen Entwicklungen im Bereich *personal data environment* und welche Auswirkungen werden diese Ihrer Meinung nach auf Wirtschaft und Gesellschaft haben? Werden es PDE-Systeme schaffen, das Vertrauen der Kunden zu gewinnen und welche Implikationen ergeben sich hieraus? Wie müsste der gesetzliche Rahmen gestaltet und Sicherheitsinfrastrukturen beschaffen sein, damit Kunden Vertrauen in die digitale Zukunft fassen und PDE-Systemen der ersehnte Durchbruch gelingt?

Wenn auch Sie zu diesem Thema oder einem Artikel der Zeitschrift Wirtschaftsinformatik Stellung nehmen möchten, dann senden Sie Ihre Stellungnahme (max. 2 DIN A4 Seiten, gerne auch als E-Mail) bitte an den Hauptherausgeber, Prof. Dr. Wolfgang König, Universität Frankfurt am Main,
E-Mail: koenig@wiwi.uni-frankfurt.de.

Prof. Dr. Hans Ulrich Buhl,
Dipl.-Kfm. Alexander Wehrmann,
Lehrstuhl für Betriebswirtschaftslehre,
Wirtschaftsinformatik
& Financial Engineering,
Kernkompetenzzentrum IT
& Finanzdienstleistungen,
Universität Augsburg

Über den Zusammenhang von Datenschutz und Kundenvertrauen von Dr. Helmut Bäumler

Wenn die Regierung mit dem Volk unzufrieden ist, dann muss sie sich ein neues Volk wählen – so oder so ähnlich mag Scott McNealy gedacht haben, als er sich Bürger und Kunden wünschte, denen der Schutz ihrer Privatsphäre egal ist. Gottlob reines Wunschdenken, denn aus Umfragen in den USA, Europa und Deutschland wissen wir, dass die große Mehrheit der Befragten dem Datenschutz eine hohe Priorität einräumt, für McNealys neue Form des Totalitarismus also nicht viel übrig hat.

Aber was verstehen die Leute genau unter Datenschutz? Wo beginnt für sie die Unzumutbarkeit und bis wohin sind sie bereit zu gehen, wenn sie sich davon einen Vorteil versprechen? Aus der datenschutzrechtlichen Praxis wissen wir, dass die meisten Menschen erstaunlich offen und kooperativ sind,

solange sie abschätzen können, worauf sie sich einlassen und ob sie der „anderen Seite“ bzw. der dort eingesetzten Technik trauen können. Beispielsweise sind medizinische Daten für Forschungsvorhaben relativ leicht zu bekommen, wenn die Patienten fair aufgeklärt werden und davon ausgehen, dass ihre Daten nicht missbraucht werden. Je konkreter die Kunden den Nutzen eines neuen Angebots erkennen können und je überzeugender ihnen dargestellt werden kann, dass sie die Kontrolle über die eigenen Daten behalten, desto bereitwilliger werden sie zustimmen.

Vertrauen kann nicht angeordnet werden, es wächst auch nicht über Nacht. Hier zählen langfristig aufgebaute Erwartungen und Erfahrungen. Wer über Jahre die schnell optimierte Performance wichtiger nimmt als Sicherheit und Verlässlichkeit, wer mit Kundendaten lieber schnelle Geschäfte macht, statt mit ihnen sorgsam umzugehen, muss sich nicht wundern, wenn die Menschen auch – und gerade – bei den verlockendsten Serviceangeboten skeptisch reagieren. Microsoft kann sicher ein Lied davon singen, wie schwer man sich tut, ein negatives Datenschutzimage wieder loszuwerden. Zu allem Unglück sind gerade im Hinblick auf die Sicherheit des Passport-Systems von Microsoft von kompetenter Seite Zweifel erhoben worden.

Auch der staatlich organisierte Datenschutz in Deutschland und Europa steht in seiner jetzigen Erscheinungsform keineswegs außerhalb der Kritik. Die Überregulierung des Datenschutzes, seine einseitige juristische Ausrichtung, die bürokratische Handhabung durch viele Amtswalter und vieles mehr haben dazu geführt, dass viele Menschen mit dem real existierenden Datenschutz vor allem Begriffe wie „Bedenken“, „kompliziert“, „unzulässig“, „erfolglos“, assoziieren, also alles Dinge, die irgendwo in der Ecke „langweilig und uninteressant“ angesiedelt sind.

Dabei geht es in Wirklichkeit um spannende Themen der Zukunftsgestaltung. Wie die Informationstechnik morgen aussieht, welche Rechte und Möglichkeiten jeder einzelne hat, ist von elementarer Bedeutung für unser demokratisches System. Sinn und Zweck des Datenschutzes kann es nicht sein, den Menschen hilfreiche Neuerungen und Annehmlichkeiten mit Bedenken zu vermiesen, sondern das Ziel muss sein, beides zu haben: optimale Produkte und Services und trotzdem einen vertrauenswürdigen Umgang mit personenbezogenen Daten. Das ist leichter gesagt als getan und auf dem hier zur Verfügung stehenden Raum allemal nicht erschöpfend auszubreiten. Aber ein paar Dinge müssen sich in jedem Fall ändern, wenn technischer Fortschritt und Datenschutz nicht weiterhin beziehungslos nebeneinander herlaufen sollen:

- Wir brauchen eine grundlegend andere *Datenschutzpolicy* in Deutschland, die sich aus der Verrechtlichungsfalle löst und vernünftige Problemlösungsmechanismen in den Mittelpunkt stellt.
- Das Thema bedarf einer *Rundumerneuerung*, um es aus der Aura der erfolglosen Bedenkenträger zu lösen und zu einer spannenden Angelegenheit der „Zukunftsmacher“ werden zu lassen.
- Datensicherheit im Sinne von Verlässlichkeit *aus der Sicht der Kunden und Bürger* muss bei der Entwicklung und Herstellung von IT-Produkten einen viel höheren Stellenwert bekommen als bisher.
- Den Unternehmen muss klar werden, dass das Thema Datenschutz nicht länger nur die lästige, von außen auferlegte Pflicht betrifft, sondern einen für die langfristige *Imagebildung* und *Kundenbindung* zentralen Faktor, den die Leitungsebene aktiv gestalten muss und nicht auf einen betrieblichen Datenschutzbeauftragten abschieben darf.

Von großer Bedeutung ist auch, die Zusammenhänge zwischen allen Bereichen zu erkennen. So ist mit einer sachgerechten Rezeption des Themas Datenschutz auf betrieblicher Ebene noch nicht viel gewonnen, wenn wie in Deutschland eine über 20 Jahre (und in den USA spätestens seit dem 11. September 2001) betriebene exzessive Gesetzgebung den staatlichen Sicherheitsbehörden via Rasterfahndung etc. den bequemen Zugriff auf betriebliche Daten erlaubt. Selbst wenn die Kunden z. B. darauf vertrauen könnten, dass ein PDE-System von einem Anbieter vertrauenswürdig gehandhabt wird, bleibt die Unsicherheit, wie weit eigentlich die Rechte von Polizei und Geheimdiensten gehen. Grundrechtsfragen sind eben nicht teilbar und so wünschte man sich die Großen der IT-Branche auch dann auf den Barrikaden, wenn es nicht um ihre eigenen Interessen geht, sondern „nur“ um Grundrechte der Bürgerinnen und Bürger gegenüber dem Staat.

Last but not least: Wir brauchen ein Kennzeichnungssystem, damit die Kunden einen guten Datenschutzservice und sichere IT-Produkte auch erkennen und bevorzugen können. In Schleswig-Holstein hat die Zukunft des Datenschutzes bereits begonnen. Das Land hat im Alleingang alle rechtlichen Voraussetzungen für Datenschutzaudits und -gütesiegel geschaffen. Das Unabhängige Landeszentrum für Datenschutz (ULD) ist die zertifizierende Stelle. Da das ULD zugleich die traditionellen Kontrollaufgaben des Datenschutzbeauftragten wahrnimmt, können die Bürger sicher sein, dass eine objektive und im Zweifel kritische Instanz Produkte und Dienstleistungen unter die Lupe nimmt. Den vom ULD vergebenen Audits und Gütesiegeln können die Bürger vertrauen. Dies erkennen auch immer mehr Anwender und Anbieter aus Verwaltung und Wirtschaft. Audits und Gütesiegel könnten der Weg der Zukunft sein, wenn es darum geht, neue Produkte und Dienstleistungen am Markt zu platzieren, von deren Unbedenklichkeit das Publikum erst noch überzeugt werden muss.

Was heißt all dies für *personal data environment*, von dem ja hier speziell die Rede sein soll? Wer mit PDEs Erfolg beim Kunden haben will, muss ihnen plausibel machen, welchen konkreten, zählbaren Vorteil sie persönlich davon haben. Er muss überzeugend darlegen und am besten durch fachkundige, unabhängige Stellen überprüfen lassen, dass das Verfahren sicher ist. Dazu gehört auch, dass die Kunden „sicher“ sein können, dass sie die Kontrolle über ihre Daten behalten und auch vor unvorhergesehenen Zweckänderungen oder -erweiterungen gefeit sind. Denn ich würde Kunden immer raten, beides zu verlangen – *Bequemlichkeit und Sicherheit*.

Dr. Helmut Bäumler,
Leiter des Unabhängigen Landeszentrums
für Datenschutz Schleswig-Holstein, Kiel

Offenheit als Geheimnis der Sicherheit von Thomas Groth

Ist die Offenheit das Geheimnis für Sicherheit? Dieses scheinbare Paradoxon legt offensichtlich die Regeln im Umgang mit Sicherheitssystemen in der Zukunft fest.

Ist Open-Source-Software in Bezug auf die Datensicherheit besser oder schlechter geeignet als proprietäre Software?

Die Open-Source-Bewegung argumentiert, sie sei besser, denn „viele Augen schauen auf den Code, um mögliche Fehler zu entdecken und auszumerzen“. Die Verfechter proprietärer Software hingegen führen zwei völlig andere Argumente ins Feld: Das erste geht dahin, dass sich auch zahlreiche feindliche Augen den offenen Quellcode ansehen können, und das, so behaupten sie, würde den Hackern und Crackern mehr helfen als den eigentlichen Anwendern. Ihr zweites Argument lautet, dass wenige Expertenaugen besser sind als viele wahllose Augen – dass also eine auf Software ausgerichtete Organisation mit Verantwortung für ihr Produkt ein ge-

eigneterer Hüter des Codes ist, als die vielen Augen der Open-Source-Gemeinschaft.

Gibt man Programmierern Zugang zu einer Software, dann besteht keine Garantie, dass sie diese auch gründlich studieren, ihren Charakter und Stil erkennen – in dieser Behauptung steckt sicherlich ein wahrer Kern. Trotzdem gibt es eine Gruppe von Programmierern, bei denen man von großer Sorgfalt ausgehen kann: Programmierer, welche die Software entweder selber benutzen oder für ein Unternehmen arbeiten, dessen Geschäftstätigkeit von der einwandfreien Funktion dieser Software abhängt.

Wenn jemand ein Recht hat und für ihn die Notwendigkeit besteht, den Code zu prüfen und sich von dessen einwandfreier Funktion zu überzeugen, dann sind es die Benutzer selbst. Tatsächlich ist die Prüfung von Programmen, von denen die Sicherheit eines Unternehmens abhängt, eine natürliche Funktion der unternehmenseigenen Datensicherheitsabteilung.

Außerdem – die Tatsache, dass ein Programm aus Open-Source-Software besteht, bedeutet nicht, dass niemand dafür verantwortlich ist. Die Fahrzeugbranche ist dafür ein gutes Beispiel:

Lange, bevor in Automobile Software eingebaut wurde, waren diese eine „Open-Source"-Technologie. Es gab Handbücher, Teilelisten und alles mögliche Zubehör sowie Reparaturteile am Teilemarkt. Abgesehen von den nur in Europa gebundenen Fachwerkstätten und Händlersteuerung hat sich weltweit eine professionelle Gruppe von Mechanikern mit der Technik und Arbeitsweise der einzelnen Autos vertraut gemacht und erfüllte damit eine ähnliche Funktion wie die Prüfer von Softwareprogrammen. Man sollte es so betrachten: Ein Mechaniker, der die Bremsen an Ihrem Wagen überprüft, gewährleistet damit die einwandfreie Funktion eines für Ihre Sicherheit notwendigen Systems.

All das bedeutet jedoch nicht, dass es keine für das Auto verantwortliche Gruppe gibt. Auf einer anderen Ebene verfolgt der Hersteller die Reparaturgeschichte jedes einzelnen Modells. Er gibt Reparaturanweisungen heraus und ruft gelegentlich ein Modell zur Wartung in die Werkstätten zurück, wenn ein ernsthafter Defekt festgestellt wird.

Was jedoch die Ansicht betrifft, dass die vermeintlichen Schwachstellen von Open Source für die Gegner schwerer wiegen als der betreffende Nutzen für die Anwender, der setzt sich mit diesem Argument über einen der wichtigsten Sicherheitsgrundsätze hinweg: ein Geheimnis, das nicht jederzeit verändert werden kann, ist als Schwachstelle anzusehen.

Wenn Ihre Sicherheit von einem Geheimnis abhängt, welche Maßnahmen ergreifen Sie, wenn das Geheimnis entdeckt wird? Wenn es problemlos veränderbar ist, wie z. B. ein Verschlüsselungscode, dann werden sie es anpassen. Wenn es jedoch schwierig zu ändern ist, wie ein Verschlüsselungssystem oder ein Betriebssystem, dann sitzen Sie fest. Sie bleiben angreifbar, bis Sie Zeit und Geld in die Erstellung eines anderen Systems investiert haben.

Es ist nicht so, dass im Bereich Sicherheit niemals Geheimnisse erforderlich wären, vielmehr sind sie nicht wünschenswert. In der Kryptographie hat man dies vor langer Zeit erkannt und das Prinzip der Offenheit bereits in den Siebzigerjahren des 19. Jahrhunderts artikuliert (obwohl es dann noch mehr als ein Jahrhundert dauern sollte, bis das Prinzip Früchte trug). Andererseits wurde im 2. Weltkrieg die Schwierigkeit der Geheimhaltung nur allzu offensichtlich, als die Kriegsparteien das Wissen um ihre Verschlüsselungssysteme zwar mit Erfolg gegenüber der Öffentlichkeit geheim hielten, jedoch viel weniger erfolgreich dabei waren, sie nicht in die Hände ihrer wirklichen Feinde fallen zu lassen.

Heute liegen die Dinge ganz anders, zumindest in der kommerziellen Welt. Alle im Internet benutzten populären Verschlüsselungssysteme sind öffentlich. In den USA wurde kürzlich ein neues, öffentliches System als nationaler Standard eingeführt. Alles spricht dafür, dass dieser Advanced Encryption Standard – auf der Grundlage eines international akzeptierten Algorithmus – in Kürze für den Schutz der Übertragung von sensiblen Daten eingesetzt wird.

Es ist einfach unrealistisch, für die Sicherheit von Computersoftware auf Geheimhaltung zu bauen. Es mag Ihnen gelingen, die technischen Funktionsabläufe eines Programms vor der Allgemeinheit zu verbergen, aber können Sie verhindern, dass ein ernsthafter Gegner Ihren Code per Reverse-Engineering zurückerschließt? Wahrscheinlich nicht.

Das Geheimnis hoher Sicherheit: weniger Geheimnis ist letztlich MEHR.

Thomas Groth,
Chief Visioneer,
Sun Microsystems GmbH

Kundenorientierte Sicherheit
von Dr.-Ing. Horst H. Henn

Persönliche und personenbezogene Daten sind heute an vielen Stellen gespeichert, wobei angenommen wird, dass die Daten angemessen verwendet und gesichert gespeichert werden. Diese Daten sind die Grundlage für alle geschäftlichen Beziehungen mit Privatpersonen und häufig von hohem wirtschaftlichem Wert für Unternehmen. Die Unternehmen haben häufig selbst keinerlei Interesse, diese wertvollen Daten an andere weiterzugeben. Die Benutzer haben meist nur vage Vorstellungen, wo und wie persönliche Daten gespeichert und wozu sie verwendet werden. Das Internet hat diese Situation zunächst nicht grundlegend geändert, jedoch kann auf Daten wesentlich leichter und schneller zugegriffen werden. Der freie unkontrollierte Austausch von Informationen ist das grundlegende Prinzip des Internets und Basis seines Erfolgs. Dies ist auch von Privatpersonen zunächst erwünscht und wird zunehmend zur Selbstdarstellung und zur Kommunikation mit Kunden, Freunden oder Interessengruppen genutzt. Die Vorstellungen, welche Daten privat und welche öffentlich zugänglich sein sollten, variieren dabei sehr stark. Da dabei auch Rechte Dritter tangiert werden können, tut sich speziell in angelsächsischen Ländern ein weites Betätigungsfeld für Juristen auf.

Ein *personal data environment* (PDE) sollte zunächst die Möglichkeiten bieten, persönliche Daten als öffentlich zugänglich oder privat zu kennzeichnen. Dabei sollten die Nutzungsrechte eventuell noch eingeschränkt werden können. Es ist verblüffend, dass sich weder Gesetzgeber noch Standardisierungsorganisationen mit der Bereitstellung zuverlässiger, öffentlich zugänglicher Privatdaten beschäftigen, die für viele Dienstleistungen im Internet benötigt werden und die Benutzer auch gerne zur Verfügung stellen würden. Damit könnte der Benutzer auch steuern und kontrollieren, welche privaten Daten öffentlich verfügbar sind, und gegen die Verwendung anderer privater Daten klagen. Dabei ist es völlig irrelevant, ob diese Informationen auf einer persönlichen Webseite, in einem oder mehreren zentralen Servern oder in Zukunft im persönlichen Webserver gespeichert werden. Das Datenformat und die Nutzung müssen jedoch international standardisiert und in DV-Produkten sowie Unternehmen unterstützt werden. Der Versuch, solche Systeme proprietär mit geschlossenen Benutzergruppen aufzubauen, wird vom Großteil der privaten Benutzern wahrscheinlich nicht akzeptiert.

Weit komplexer ist der Zugriff zu Onlinesystemen (Selbstbedienung) und die Aus-

lösung von Transaktionen, speziell von Bestellungen und Zahlungen. Hierfür ist eine zuverlässige Authentifizierung des Benutzers und die Überprüfung seiner Autorisierung notwendig. Im Internet gibt es wohl Adressierungssysteme (IP-, E-Mail-Adresse) aber keine systemimmanente Authentifizierung oder Autorisierung z. B. für Zahlungen, da das Internet ursprünglich ja nicht kommerziell ausgerichtet war. Jeder Serviceanbieter, der Authentifizierungs- und Autorisierungsdienste anbietet, geht ein unkalkulierbares Risiko ein, da solche Dienste für äußerst risikoreiche Transaktionen genutzt werden können und damit hohe Haftungsrisiken eingegangen werden müssen. Bezeichnenderweise hat die Firma Microsoft den sogenannten Wallet Service in seinem .NET Passport Service sehr schnell zurückgezogen, da Wallets typischerweise für sehr sensitive Informationen wie z. B. Passworte oder Kreditkarteninformationen genutzt werden.

Interessant ist hier der Vergleich mit dem Kreditkarten- und dem Mobiltelefonsystemen, deren Services wie selbstverständlich von Privatpersonen weltweit genutzt werden können.

Das Kreditkartensystem unterstützt zwei Varianten: Zahlung ohne Authentifizierung und Zahlung mit Authentifizierung (PIN), z. B. an Geldautomaten. Die Zahlung ohne Authentifizierung ist für den Kunden wesentlich komfortabler, birgt aber ein wesentlich höheres Risiko, da Magnetkarten leicht kopiert werden können. Dieses Risiko wird durch ausgefeilte Onlineprüfverfahren, Risikomanagement und über höhere Gebühren für den Händler abgedeckt. Dieses Verfahren wird trotz höherem Risiko eindeutig von den Kunden bevorzugt. Die Übertragung der PIN erfolgt weltweit ähnlich wie bei Geldausgabeautomaten verschlüsselt von der Eingabe zum Endsystem, was erhebliche Investitionen in Organisation, sichere Geräte und Bauelemente erfordert. Im Internet ist diese Infrastruktur zur Zeit nicht verfügbar, sodass Kreditkartenzahlungen heute im Internet speziell international mit hohem Risiko und hohen Gebühren für den Händler behaftet sind.

Das Mobiltelefonsystem verwendet eine Chipkarte (SIM-Modul) zur Authentifizierung und zur Autorisierung. Die PIN wird lokal geprüft; weltweite Standardisierung erlaubt weltweite Nutzung inklusive der Abrechnung der Dienstleistungen. Milliarden von Benutzern haben gelernt, mit diesem System umzugehen. Dieses System hat gute Chancen, im Bereich Internetzugang speziell für WLAN zum Standard zu werden, da Hardware und Service über die SIM-Karte unabhängig voneinander vom Kunden ausgewählt werden können.

Hinter beiden Systemen stehen weltweit operierende Clearingunternehmen, welche die Zahlungsströme lenken und Partner (Banken, Telekommunikationsunternehmen), die sich auf gemeinsame Standards und Gebührenordnungen geeinigt haben.

Das Mobiltelefonsystem ist eindeutig das modernere System, da Chipkarten im Gegensatz zu Magnetstreifenkarten nicht kopiert werden können. Deshalb versuchen die Kreditkartenunternehmen weltweit auf Chipkartentechnologie umzustellen, da die Händler nicht mehr bereit sind, die hohen Gebühren, die aus der unsicheren Magnetstreifentechnologie resultieren, zu zahlen. Die Einführung erfolgt aber äußerst zögerlich, da in vielen Ländern die Ausfälle durch Betrug noch immer deutlich niedriger als die Investitionen für die Chipkarteninfrastruktur sind – Sicherheit lohnt sich häufig nicht! Andererseits sind fast alle Versuche, Systeme zur Zahlung mit Mobiltelefonen aufzubauen, gescheitert, da Telekommunikationsunternehmen nicht gewillt sind, das Risiko bei der Zahlung abzudecken.

Es ist offensichtlich, dass im Internet für Authentifizierung und Autorisierung eine ähnliche Organisationsinfrastruktur nicht existiert und wahrscheinlich für Privatpersonen nie existieren wird, da die Interessen von Privatpersonen naturgemäß stark divergieren. Es wird aber sicher kommerzielle Systeme in einzelnen Industrien z. B. für Banken, Gesundheitswesen, Automobilindustrie, Unterhaltung u. a. geben. Solche Systeme sind zum Teil mit Millionen Benutzern bereits in Betrieb. Interessant ist hier vor allem die Entwicklung im Gesundheitswesen, wo sich per USA-Gesetz definierte Regeln für den Betrieb (HIPAA) und ein internationaler Standard für die Identifikation, Autorisierung und Signatur (G8 Health Card Standard) durchzusetzen scheinen. Dabei werden Basistechnologien in Hardware- und Software sowie Regeln für den Austausch von Daten und den Betrieb der Systeme vorgeschrieben. Der Versuch, sichere Systeme ohne Regeln für den Betrieb zu definieren, ist sicher zum Scheitern verurteilt, obwohl natürlich vernünftige Unterstützung in Hardware und Software den sicheren Betrieb erst ermöglicht oder erleichtert.

Eine der Schlüsselanwendungen für PDE-Dienste ist die Authentifizierung, die heute weitgehend auf Benutzeridentifikation (UID) und Passwort (PW) basieren. Diese sind zu einer wahren Seuche im Internet geworden, da immer mehr personalisierte Dienstleistungen nur noch nach Authentifizierung zur Verfügung stehen. Mit zunehmendem Serviceangebot und Vernetzung im Internet führt dies zu einem echten Akzeptanzproblem bei den Endnutzern.

UID und PW sind aber als Sicherung für Systemzugriffe wenig geeignet, weil sie sich weit einfacher als ein Magnetstreifen kopieren lassen. Meist ist den Benutzern nicht bewusst, dass bei den meisten Servern UID und PW unverschlüsselt im Internet übertragen werden. Eine zentrale Speicherung dieser Daten ist sicher höchst problematisch, da nicht nur die sichere Speicherung, sondern auch der sichere Betrieb mit häufigen Änderungen der Passwörter garantiert werden muss.

Professionelle Betriebs- und Officesysteme verwenden bereits seit Jahren digitale Signaturen und Zertifikate zur Zugriffskontrolle – ohne dass der Benutzer das überhaupt bemerkt. Die Verfahren und die Zertifikate (X.509) sind hinreichend standardisiert und werden von allen gängigen Betriebs-, Browser- und Anwendungssystemen unterstützt. Im privaten Bereich ist PGP verbreitet. Dem Benutzer bleibt es dabei überlassen, ob er seine Zertifikate je nach Sicherheitsanforderungen in Software, in der PC-Hardware oder in einer Chipkarte abspeichert und ob er seine Zertifikate selbst erstellt (à la Pretty Good Privacy) oder von einem Unternehmen beziehungsweise einer staatlichen Organisation erhält. In der Regel wird der Benutzer mehrere Zertifikate und kryptografische Schlüssel für private und geschäftliche Zwecke benutzen. Diese müssen entgegen der herrschenden Meinung nicht von großen zentralen PKI-Systemen generiert werden, sondern können sogar vom Endverbraucher für sich und seine Freunde generiert werden. Nicht umsonst ist PGP mit diesem Verfahren zur bevorzugten Sicherheitsinfrastruktur im privaten Bereich geworden.

Deshalb sollten moderne Systeme dem Benutzer erlauben, sich mit einem Zertifikat möglichst seiner Wahl zu authentifizieren. Anstatt einer Vielzahl von Passwörtern wird dann nur noch ein Passwort zum Zertifikatspeicher (Crypto Service Provider) benötigt. Professionelle Systeme werden Crypto Service Provider in Smartcard-Technologie einsetzen, die als Karte (SIM im Mobiltelefon oder PDA) oder z. B. bei IBM-Laptops gemäß dem TCPA-Standard fest eingebaut sind. Damit stehen dem privaten Nutzer bereits heute genügend standardisierte Technologien zur Verfügung, die von Browsern und gängigen Anwendungen unterstützt werden, um sich im Internet zu authentifizieren, Transaktionen zu autorisieren und Daten zu verschlüsseln. Dabei hat der Be-

nutzer die Wahl, ob er selbst seine persönlichen Daten inklusive seiner kryptografischen Schlüssel verwaltet und/oder einem oder mehreren Serviceprovidern, z. B. seiner Bank, seinem Internetprovider usw. die Verwaltung überlässt.

Problematisch ist jedoch, dass die Mehrheit der Internet-Sites nicht standardisierte technische Schnittstellen zur Autorisierung verwendet und den Kunden stark divergierende Geschäftsbedingungen anbietet oder gar diktiert. Es ist nicht anzunehmen, dass sich dies in absehbarer Zeit grundlegend ändert. Viel wahrscheinlicher ist, dass die innerhalb von Unternehmen eingesetzte Portaltechnologie auch für Endverbraucher eingesetzt wird, um größere Funktionseinheiten mit geregelten Schnittstellen und Prozessen und einheitlichen Geschäftsbedingungen zu bilden. Portale erlauben Zugriff zu einer großen Zahl von Anwendungen (Single Sign On) und bieten meist basierend auf Webservices-Technologie eine Plattform für die Kommunikation und die Durchführung von Geschäftsprozessen. Technische Standards sind dabei eine notwendige, aber keine hinreichende Bedingung für attraktive und profitable Serviceangebote. Persönliche Daten können von den Benutzern im eigenen Gerät oder in gesicherten Bereichen des Portals gespeichert werden. Kritische Transaktionen müssen dabei aus psychologischen oder rechtlichen Gründen immer vom Benutzer persönlich frei gegeben werden. Wichtig ist dabei, dass dies für die Benutzer mit größerem Komfort und wählbarer Sicherheit erfolgt.

Die IT-Industrie wäre gut beraten, anstatt endloser häufig wenig qualifizierter Sicherheitsdiskussionen und -versprechen perfekter zukünftiger Lösungen die heute verfügbaren Möglichkeiten zur Sicherung der persönlichen Daten objektiv darzustellen und zunächst in Zusammenarbeit mit den Serviceprovidern die Akzeptanz bei den Benutzern durch standardisierte, einfache Bedienung und persönlich kontrollierbare Sicherheitsinfrastruktur zu erhöhen.

Dr.-Ing. Horst H. Henn,
WebSphere Portal Development,
IBM Deutschland GmbH

Mitteilungen des GI-Fachbereichs Wirtschaftsinformatik

Experten warnen vor überstürzten Outsourcingentscheidungen

Die hohen Erwartungen, die derzeit mit dem Outsourcing von Leistungen verbunden werden, sind in den meisten Fällen überzogen. Damit die Verlagerung einer Aufgabe zu einem externen Anbieter tatsächlich zu langfristigen Kosteneinsparungen führen kann, muss eine Reihe von Voraussetzungen erfüllt sein. Von zentraler Bedeutung ist die Flexibilität der IT-Architektur. Dies sind die Ergebnisse des Workshops „Sourcing“ der Fachgruppe 5.4 (Informationssysteme in der Finanzwirtschaft) der Gesellschaft für Informatik, der am 2003-07-11 in München stattfand.

Prof. Dr. Erhard Petzel von der International University in Germany, Bruchsal, beleuchtete mögliche Ursachen, weshalb ein externer IT-Anbieter eine Leistung kostengünstiger erbringen kann als die interne Abteilung. Neben den oft zitierten Skaleneffekten können nach seinen Projekterfahrungen vor allem versteckte Leerzeiten beseitigt sowie eine Überqualifikation des Personals vermieden werden. Der wichtigste Hebel liege jedoch in der Überarbeitung der Prozesse.

Die zentrale Bedeutung des Reengineerings von Geschäftsprozessen bestätigte Dr. Hans-Gert Penzel von der HypoVereinsbank AG. Im Rahmen des Reengineerings sollte das Outsourcing derjenigen Leistungen erwogen werden, die von der Bank nicht wettbewerbsfähig erbracht werden können, für die ein ausreichender Markt vorhanden ist und bei denen der Aufwand zur Schnittstellenanpassung gering ist. Voraussetzung dafür sei eine Kapselung der zu Grunde liegenden Informationssysteme und die Etablierung von Standardschnittstellen. Damit sich das Outsourcing für beide Seiten lohne, müssen zudem die Kosten des Insourcers 50 % unter denen des Outsourcers liegen.

Die Wechselwirkungen zwischen Sourcingentscheidungen und Informationssystemen vertiefte abschließend Prof. Dr. Robert Winter vom Institut für Wirtschaftsinformatik der Universität St. Gallen. Änderungen in der Sourcingstrategie seien bei vielen Unternehmen aufgrund historisch gewachsener Systemarchitekturen nicht möglich. Die Überarbeitung der Architekturen erfordert die Formulierung detaillierter Businessspezifikationen und dauert oft mehrere Jahre. Da einige Banken bereits mit der Umgestaltung ihrer Systemarchitekturen begonnen haben und zunehmend Standardsoftware wie die der SAP AG eingesetzt wird, erwarten die Workshopteilnehmer die Entwicklung standardisierter Bausteine und Schnittstellen bei den Banken.

Als weiteres Problem wurde in der Diskussion zwischen den Teilnehmern zudem häufig die Kostenintransparenz bei der internen Leistungserstellung genannt. Eine objektive Entscheidungsgrundlage für oder gegen das Outsourcing steht daher in den meisten Unternehmen derzeit nicht zur Verfügung. Hinzu kommen arbeits- und steuerrechtliche Fragestellungen, sodass die Outsourcingentscheidung höchste Komplexität erlangt. Statt überstürzter Entscheidungen sollten daher zunächst die internen Voraussetzungen für Outsourcing geschaffen und anschließend jeder Einzelfall genau geprüft werden.

Über die Fachgruppe 5.4 (Informationssysteme in der Finanzwirtschaft)

Die Fachgruppe 5.4 der Gesellschaft für Informatik beschäftigt sich schwerpunktmäßig mit Wettbewerbsaspekten finanzwirtschaftlicher Informationssysteme und dem Transfer neuer Konzepte und Technologien von der Forschung in die finanzwirtschaftliche Anwendungspraxis. Dies erfolgt mit dem Ziel, der wachsenden Bedeutung der Ressource Information für den Markterfolg der Unternehmungen der Finanzdienstleistungsbranche und ihrer Kunden sowie dem Funktionsbereich Finanzwirtschaft in den einzelnen Unternehmen gerecht zu werden. Sprecher der Fachgruppe ist Prof. Dr. Dieter Bartmann, Universität Regensburg.

Kontakt

Florian Allwein, Institut für Bankinformatik und Bankstrategie an der Universität Regensburg gGmbH,
Tel. 0941 943-1908,
E-Mail: florian.allwein@ibi.de,
http://www.if-news.de/

Aus den Hochschulen

Dr.-Ing. Thomas Barth, Jahrgang 1968, der als Wissenschaftlicher Assistent am Lehrstuhl für Wirtschaftsinformatik im Fachbereich Wirtschaftswissenschaften der Universität Siegen arbeitete, hat zum Jahresbeginn eine Junior-Professur für Wirtschaftsinformatik übernommen. Seine Forschungsschwerpunkte sind Verteilte IT-Systeme zur Unterstützung des virtuellen Produkt- und Prozessentwurfs sowie deren Integration in das Produktlebenszyklusmanagement (http://www-winfo.uni-siegen.de/winfo/deutsch/personal/barth.html).

Prof. Dr. Stefan Kirn, Jahrgang 1956, der an der Technischen Universität Ilmenau am Fachbereich Wirtschaftswissenschaften die Professur für Wirtschaftsinformatik 2, insbesondere für Dienstleistungen und Verwaltung, bekleidete, hat einen Ruf auf die Professur für Wirtschaftsinformatik in der Fakultät Informatik an die Universität der Bundeswehr in München abgelehnt und einen weiteren Ruf auf die Professur für Wirtschaftsinformatik in der Fakultät Wirtschafts- und Sozialwissenschaften der Universität Hohenheim angenommen. Seine Forschungsschwerpunkte sind Informationssysteme im Gesundheitswesen, in Dienstleistungsunternehmen und im E-Government, Verteilte Systeme und Telekooperationssysteme sowie Angewandte Künstliche Intelligenz (http://www.wi.uni-hohenheim.de).

Prof. Dr. Dr. h. c. mult. August-Wilhelm Scheer, Jahrgang 1941, der das Institut für Wirtschaftsinformatik (IWi) im Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) leitet, hat als erster Wirtschaftswissenschaftler den Philip-Morris-Forschungspreis erhalten. Die Laudatio betonte insbesondere seine Leistungen bei Konzeption und Entwicklung der weltweit eingesetzten Prozessmanagement-Software ARIS (Architektur integrierter Informationssysteme).

Prof. Dr. Detlef Schoder, Jahrgang 1966, der den Stiftungslehrstuhl des DaimlerChrysler-Fonds im Stifterverband für die Deutsche Wissenschaft für Betriebswirtschaftslehre, insbesondere Electronic Business, an der Wissenschaftlichen Hochschule für Unternehmensführung (WHU) in Vallendar bekleidet, hat einen Ruf auf eine Professur für Wirtschaftsinformatik, insbesondere Informationsmanagement, an die Wirtschafts- und Sozialwissenschaftliche Fakultät der Universität zu Köln erhalten. Seine Forschungsschwerpunkte sind Electronic Business, Peer-to-Peer- und Ubiquitous Computing (http://www.whu.edu/ebusiness/).

Call for Papers

Schwerpunktthema
WIRTSCHAFTSINFORMATIK Heft 5/2004

Referenzmodellierung –
Konstruktion und Anwendung

In der Anwendungssystem- und Organisationsgestaltung – als wesentliche Gegenstandsbereiche der Wirtschaftsinformatik – ist ein modellbasiertes Vorgehen seit langem etabliert. Referenzmodelle unterstützen die beiden Arbeitsgebiete, indem sie Ausgangslösungen für die Entwicklung projektspezifischer Modelle zur Verfügung stellen. Sie können dabei verschiedene Aufgabenbereiche der Informationssystementwicklung wie z. B. Fachkonzeption, DV-Konzeption und Implementierung fokussieren.
Der Einsatz von Referenzmodellen birgt sowohl für deren Ersteller als auch für deren Anwender umfassende Nutzenpotenziale. Ihre Konstruktion kann z. B. durch die Funktion als Wissensmanagementinstrument motiviert werden. Besonders für Institutionen, die wiederholt ähnliche Projekte durchführen bzw. begleiten, kann die Explikation von Gestaltungsempfehlungen in Form von Referenzmodellen lohnend sein. Referenzmodelle können darüber hinaus als selbstständige Umsatzträger fungieren, als Input für Modellierungswerkzeuge dienen und als Akquiseinstrumente für Entwicklungsaufträge eingesetzt werden. Von herausragender Bedeutung ist ihre Nutzung als Grundlage für eine modellgestützte Anpassung von insbesondere großen Enterprise-Resource-Planning-(ERP-)Systemen an betriebliche Anwendungskontexte (Customizing). Referenzmodelle dieser Art werden auch als Software-Referenzmodelle bezeichnet.

Auf der Anwenderseite sollen Referenzmodelle die Wirtschaftlichkeit der Informationssystemgestaltung erhöhen, indem sie Vergleichsgrundlagen zur Beurteilung der eigenen Lösungen schaffen und übernehmbare Modellteile und Begriffssysteme bereitstellen. Darüber hinaus bieten sie Orientierung bei der methodischen Gestaltung der eigenen Systeme. Den Vorteilen steht der Aufwand der Auswahl und Anschaffung der verwendeten Ausgangsmodelle sowie deren Anpassung an projektspezifische Besonderheiten gegenüber.

Um den Wirkungsgrad von Referenzmodellen zu erhöhen, soll das geplante Schwerpunktheft einen Beitrag dazu leisten, bestehende Probleme in der Konstruktion und Anwendung von Referenzmodellen zu identifizieren und Lösungsansätze zu ihrer Überwindung aufzuzeigen. Beispiele für Themengebiete von Beiträgen lassen sich den folgenden drei Aspekten zuordnen.

Ökonomischer Aspekt

- Analyse der Kosten-Nutzen-Relation der Referenzmodellierung und ihrer Einflussfaktoren
- Produktplanung für Referenzmodelle (z. B. Eingrenzung der zu behandelnden Wirtschaftszweige und Anwendergruppen, Wahl von Modellierungstechniken)
- Vermarktungsformen für Referenzmodelle
- Schaffung von Transparenz über bestehende Referenzmodelle
- Sicherstellung der Weiterentwicklung von Referenzmodellen durch Konstrukteure und Anwender (z. B. durch Anreizsysteme für Feedback, Communitys)

Methodischer Aspekt

- Vergleich von Referenzmodellierungstechniken und Vorschläge zu deren Kombination
- Fortgeschrittene Ansätze zur generierenden Adaption von Referenzmodellen (Konfiguration von Modellen anhand von Parametern, Modelltransformationen entlang der Entwicklungsphasen der Informationssystemgestaltung)
- Alternative Organisationsformen von Referenzlösungen (z. B. Modellbausteinbibliotheken)
- Referenzmodellevaluation
- Vorgehensmodelle zur Konstruktion und Anwendung von Referenzmodellen
- Referenzmodellierungswerkzeuge
- Wissenschaftstheoretische und praktische Analysen zum Einsatz von Referenzmodellen als Wissensmanagementwerkzeuge

Empirischer Aspekt

- Erhebungen zum Bestand von Referenzmodellen (Abdeckungsgrade von Wirtschaftszweigen und Anwendergruppen, Detaillierungsgrade der Modelle, verwendete Referenzmodellierungstechniken etc.)
- Analysen zu Erfolgsfaktoren der Referenzmodellkonstruktion und -anwendung
- Erfahrungsberichte aus konkreten Projekten
- Vorstellung umfangreicher Referenzmodelle (von Gesamtarchitekturen/Ordnungsrahmen bis zu Modellen für einzelne Funktionen) aus unterschiedlichen Domänen

Beiträge, die weitere Aspekte der Referenzmodellierung beleuchten, sind willkommen.

Einreichung von Beiträgen

Sollten Sie beabsichtigen, einen Beitrag einzureichen, so wären wir Ihnen für eine baldige, unverbindliche Mitteilung über den geplanten Arbeitstitel dankbar.

Bitte beachten Sie die Hinweise zu formaler Gestaltung und Umfang von Beiträgen für die WIRTSCHAFTSINFORMATIK. Beiträge sollten bis zu 10 Druckseiten umfassen; das entspricht ca. 50.000 Zeichen einschließlich Leerzeichen, abzüglich 5.000 Zeichen je Seite an Bildern. Beiträge sollten in deutscher oder englischer Sprache verfasst sein und elektronisch (als *.doc oder *.rtf-Dokumente) eingereicht werden. Grafiken von angenommenen Beiträgen werden als separate Dateien in bestimmten Formaten benötigt.

Eingereichte Beiträge werden (anonymisiert) von jeweils drei Gutachtern auf Relevanz, Originalität und fachliche Qualität beurteilt. Neben den Herausgebern des Schwerpunktheftes und jenen der Zeitschrift WIRTSCHAFTSINFORMATIK wirken dabei weitere ausgewiesene Persönlichkeiten aus Wissenschaft und Praxis im In- und Ausland mit.

Ergänzend zu den Aufsätzen sind auch Beiträge zum Schwerpunktthema für andere Rubriken der Zeitschrift WIRTSCHAFTSINFORMATIK willkommen, z. B. für
WI – State-of-the-Art,
WI – Schlagwort,
WI – Innovatives Produkt,
WI – Interview,
WI – Für Sie gelesen und
WI – Für Sie gesurft.
Auch in diesem Fall bitten wir um frühzeitige Kontaktaufnahme.

Zeitplan

2004-03-01: Einreichung von Beiträgen
2004-05-01: Benachrichtigung der Autoren
2004-07-01: Abschluss von Überarbeitungs- und Folgebegutachtungszyklen
2004-10-18: Geplanter Erscheinungstermin

Für Rückfragen steht Ihnen der Herausgeber des Schwerpunktheftes gerne zur Verfügung:

Prof. Dr. Jörg Becker,
Institut für Wirtschaftsinformatik,
Westfälische Wilhelms-Universität Münster,
Leonardo-Campus 3,
49149 Münster,
Tel. 0251 83-38100,
Fax 0251 83-38109,
E-Mail: becker@wi.uni-muenster.de