



Stefan Arn, CEO  
AdNovum Informatik AG

Liebe Leserin,  
lieber Leser  
Wir wollen der ge-  
wachsenen Kunden-  
zahl Rechnung tra-  
gen und lancieren  
deshalb NOTITIA, die  
zwei- bis dreimal pro  
Jahr über unsere Ak-  
tivitäten und damit  
zusammenhängende  
Themen informieren  
soll. Als Entwicklerin für den Finanzdienst-  
leistungsbereich gehen wir davon aus, dass  
Lösungen wie etwa Portale bald Allgemeingut  
werden, aber die darunter liegenden Soft-  
ware-Systeme ganz und gar nicht. Wenige  
Entwickler unter Schweizer Rechtshoheit  
haben wie wir die Möglichkeit, ihre Produkte  
unter ähnlichen «large scale»-Bedingungen  
einzusetzen. Aber nur auf diese Weise lassen  
sich Basistechniken in Bereichen wie Sicher-  
heit – und damit zusammenhängend etwa  
Single Signon – oder Kapazitätshandling über-  
haupt beherrschen. Im Labor nämlich sind  
diese nicht erlernbar. Denn es handelt sich um  
äusserst transaktionsintensive Lösungen, die  
sich dank der kontinuierlichen Arbeit Woche  
um Woche verbessern.

Unser erstes Hauptthema ist den Portalen  
gewidmet. Sie stellen definitiv keine Einstiegs-  
seiten ins Web mehr dar, zumal es Verknüp-  
fungsmöglichkeiten seit dem Beginn des  
Internets gegeben hat. Portale werden durch  
die vier grossen «S» definiert: ein Single  
Signon für die Authentisierung, eine generelle  
Sicherheit für die Benutzer und Betreiber, eine  
flexible Skalierbarkeit wie etwa ein 16-achsiger  
Sattelschlepper und Services in Form von  
Dienstleistungen. Substanziell neu werden  
digitale Eingangshallen für politische Exeku-  
tiven wie etwa mit Push-Techniken aus-  
gestattete Systeme für die Kommunikation mit  
dem Bürger oder jene mit Pull-Möglichkeiten  
für Ausschreibungen sein. Ähnliches ist  
beispielsweise durchaus auch für die Versiche-  
rungsbranche denkbar. Leute, die sich heute  
dauernd nur darüber beklagen, dass die  
Internet-Blase geplatzt sei, haben nicht ver-  
standen, was die Substanz des Webs ist.  
AdNovum ist gerne Partner von denen, die es  
wissen.

S. A.

Stefan Arn  
CEO AdNovum Informatik AG

# Kontaktvielfalt in den digitalen Schalterhallen

DAS INTERNET IST DRAUF UND DRAN, SICH ZU  
EINEM VOLLWERTIGEN ABSATZKANAL FÜR DIE PRODUKTE  
DER SCHWEIZER FINANZINSTITUTE ZU ENTWICKELN. DER  
TREND GEHT HIN ZUM UMFASSENDE ALLFINANZ-  
PORTAL, AUF DESSEN BREITES DIENSTLEISTUNGS-  
SPEKTRUM DIE BENUTZER ÜBER EINE VIELZAHL VON  
KANÄLEN WIE PC, MULTIMATEN UND MOBILTELEFONE  
ZUGREIFEN KÖNNEN.

VON BORIS SCHNEIDER

In kaum einem anderen Wirtschafts-  
bereich führt das Internet zu derart nach-  
haltigen Veränderungsprozessen wie in der  
Finanzindustrie. Der Grund dafür ist, dass  
das Finanzgeschäft grösstenteils aus der Ver-  
arbeitung, Interpretation und Vermittlung von  
Informationen lebt. Das Internet als Informa-  
tionsbeschleuniger greift daher schonungslos  
in die traditionelle Wertschöpfungskette  
der Banken ein. Mit technisch ausgefeilten  
Lösungen nutzen die Schweizer Banken und  
Versicherungen das Internet immer mehr als  
zusätzlichen Absatzkanal für ihre Produkte.

## Die E-Bank als logische Konsequenz

Bereits in den Jahren vor dem Auf-  
kommen des Internets war der Bankkunde  
nicht zwingend auf den Gang zur Filiale an-  
gewiesen, konnte er doch seine Bankge-  
schäfte bei vielen Geldinstituten auch mittels  
Telefon oder Videotext tätigen. Wie bei vielen

## IN DEN LETZTEN JAHREN SIND WELTWEIT RUND 400 FINANZPORTALE ENTSTANDEN.

ähnlich gelagerten Fällen, etwa dem Online-  
Buchhandel, ist Electronic Banking oder  
E-Banking keineswegs eine Errungenschaft  
der New Economy, sondern lediglich ein  
bewährtes Konzept, das als zusätzlicher  
Dienst für das Internet adaptiert wurde.

Heute unterhalten die meisten Banken zu-  
sätzlich zu bestehenden physischen Schaltern  
und Callcentern richtiggehende elektronische  
Filialen im Internet. Nebst der Möglichkeit des

Wertpapierhandels bieten sie ein ständig  
wachsendes Spektrum an Dienstleistungen  
an, wie etwa die Abfrage des Kontostandes,  
die Aufgabe und Stornierung von Dauerauf-  
trägen und die Abwicklung des Zahlungs-  
verkehrs. Mit der Lancierung ihrer E-Banken  
haben die grossen Institute bewiesen, dass  
sich bestehende IT-Architekturen und Business-  
prozesse effizient auf den neuesten Stand der  
Technologie bringen lassen.

## Finanzportale machten den Anfang

Die erste Art von Diensten, die das  
Internet zur Steigerung der Geschwindigkeit  
des Informationsflusses zwischen den Börsen  
und einer breiten Masse von Anlegern nutz-  
ten, waren die Finanzportale. In den letzten  
Jahren sind weltweit rund 400 solche  
Webseiten entstanden. In der Schweiz ist es  
seit dem Jahr 1997 möglich, die Kurse aller an  
der Schweizer Börse SWX gehandelten

Wertpapiere in Echtzeit online abzufragen.  
Dieser Dienst wurde damals von der Firma  
Swissquote angeboten. Der Begriff Finanz-  
portal etablierte sich in der Folge für  
ein Angebot, das redaktionelle Beiträge rund  
ums Börsengeschehen, Echtzeit-Kursdaten  
verschiedener Börsenplätze, Research und  
Analysen oder auch Werkzeuge zur beque-  
men Verwaltung des Portfolios der Benutzer  
umfasst. Auf dem internationalen Parkett

haben sich insbesondere die Dienste Yahoo  
Finance, MSN Money Central, Quicken oder  
Moetley Fool einen Namen gemacht, in der  
Schweiz zählen Borsalino, Swissquote oder  
Swissinvest zu den Favoriten der Anleger-  
gemeinde, während Neuling Moneycab noch  
versucht, Boden gutzumachen.

## Aktien online kaufen und verkaufen

Ständige Verbesserungen in der Internet-  
Technologie und immer weitergehende  
Anforderungen der Benutzer hatten schon

## DIE SCHWEIZER BANKEN NEHMEN IN SACHEN SICHERHEIT WELTWEIT EINE SPITZENPOSITION EIN.

bald einen breiten Markteintritt von Online-  
Brokern wie E-Trade zur Folge. Zusätzlich  
getrieben vom grassierenden Börsenboom  
sollten diese Dienstleister den Handel mit  
Wertpapieren fast in den Status eines  
Volkssports erheben. Im Wettkampf um  
Kunden zettelten die Discount-Broker einen  
schmerzhaften Preiskrieg an. Dazu waren  
diese Unternehmen, zu deren bekanntesten  
Exponenten die auch in der Schweiz vertrete-  
ne Consors gehört, anfänglich auch in der  
Lage. Für ihren Markteintritt benötigten sie  
weder viel Personal noch ein flächendecken-  
des physisches Filialnetz. Der einzige Kosten-  
faktor nebst den Aufwänden für teilweise  
aggressive Werbung bestand in der Bereit-  
stellung der notwendigen technischen Infra-  
struktur. Die schlechte Stimmung aber, die  
an den Finanzmärkten seit dem Ende der  
Dot-Com-Blase das Klima bestimmt, scheint  
heute den Online-Brokern den Garaus zu  
machen. Die wenigsten erreichen die anvi-  
sierten Transaktionsvolumina und bleiben  
dadurch weit hinter den prognostizierten  
Ertragerwartungen zurück. Auch die rund  
400 Finanzinformations-Portale kommen  
zunehmend unter Druck. Laut dem Markt-  
forschungsunternehmen Forrester Research  
wird rund die Hälfte davon einer anstehenden  
Konsolidierung zum Opfer fallen.

## Skandinavien sind intensivste Nutzer

Online-Banking-Dienste werden gegen-  
wärtig am häufigsten in Skandinavien  
genutzt. Bei den grössten nordischen Banken,  
dem Quartett bestehend aus SEB, Handels-  
banken, Swedbank sowie Merita-Nordbanken,

wickeln mittlerweile 25 bis 30 Prozent der  
Kunden ihre Transaktionen über das Internet  
ab. Den Hauptgrund dafür sehen Experten in  
der hohen Affinität der nordischen  
Bevölkerung zum Medium Internet. Geschätzt  
wird beim Online-Banking insbesondere die  
Möglichkeit, Zahlungen zu jedem beliebigen  
Zeitpunkt durchführen zu können. Die meis-  
ten Transaktionen erfolgen denn auch an den  
Wochenenden. Mit rund sieben Prozent der  
inländischen Kunden von grossen Banken wie  
UBS und Credit Suisse, die Online-Banking-  
Dienste aktiv nutzen, liegt die Schweiz im

europäischen Mittel. Zum Vergleich: Auch in  
den Vereinigten Staaten wird die Möglichkeit

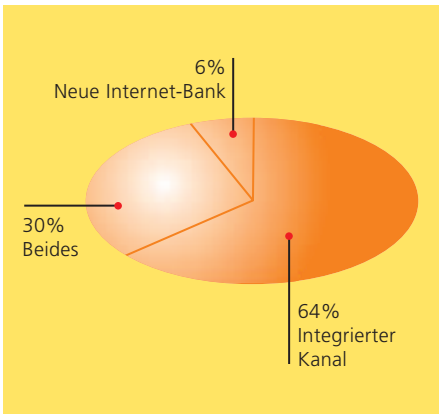
zur Abwicklung diverser Geldgeschäfte via  
Internet noch von weniger als zehn Prozent  
der Bankkunden in Anspruch genommen.  
Doch im Gegensatz zu den reinen Online-  
Brokern verzeichnen die etablierten Finanz-  
institute ein starkes Wachstum bei den  
Kunden, die Online-Banking-Verträge ab-  
schliessen. Laut dem Bundesverband  
deutscher Banken (BDB) ist deren Zahl im  
vergangenen Jahr um 50 Prozent auf über  
15 Millionen gestiegen. Mit einem weiteren  
Anstieg ist trotz der schlechten Börsen-  
stimmung zu rechnen. Schliesslich ist der  
Wertpapierhandel über Internet bei den  
Banken nicht der einzige angebotene Dienst  
und auch nicht der alleinige Umsatzlieferant.

## Benutzer haben Sicherheitsbedenken

Das grösste Hindernis für eine höhere  
Akzeptanz von E-Banking ist zum jetzigen

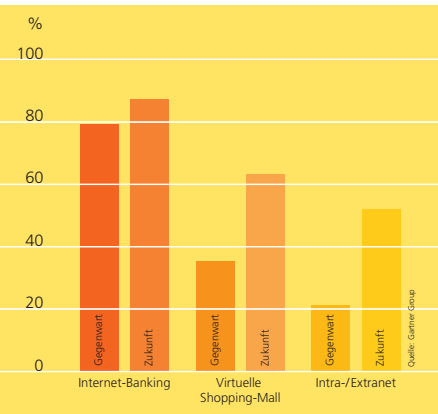


### Trends im Internet-Banking



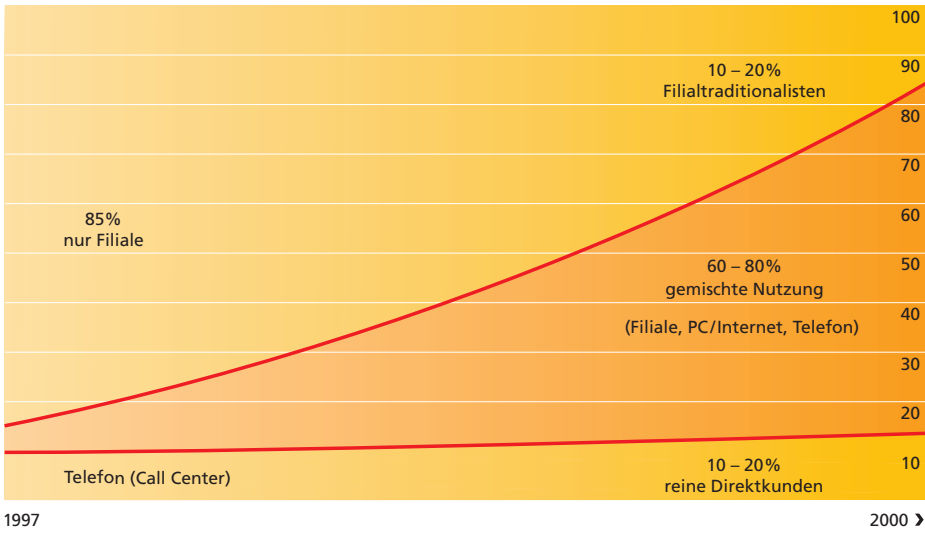
Das von der Gartner Group erarbeitete euro-  
päische E-Commerce-Bankenmodell beweist,  
dass Neulinge im Internet-Banking nur eine  
marginale Rolle spielen werden.

Das renommierte Marktforschungsunter-  
nehmen Gartner Group hat sich in einer  
Studie mit den Veränderungen befasst, die  
Unternehmen aus der Finanzindustrie bis ins  
Jahr 2005 betreffen. So gehen die Forscher  
davon aus, dass Finanzunternehmen einen  
substanziellen Teil ihres Umsatzes im Internet  
erwirtschaften werden. Zu den Mitteln, dies  
zu realisieren, zählen sie die Datenanalyse, die  
laufende Transaktionen in Echtzeit untersucht.  
Dadurch können die Betreiber ihren Kunden  
auf ihren Finanzseiten hochgradig persona-



Gefragt wurde, wie viele traditionelle Bank-  
institute 2005 das Internet als zusätzlichen  
Kanal in ihre bestehende Struktur integrieren  
oder das Web ohne Filialnetz als eigenstän-  
digen Kanal nutzen wollen.

lisierte Angebote machen. Rund 70 Prozent  
der Kunden-Interaktion mit einer E-Bank  
sollen durch sogenanntes Echtzeit-Data-  
Mining ausgelöst werden. Ferner geht Gartner  
davon aus, dass mehr als ein Drittel aller  
Konsumenten ein personalisiertes Allfinanz-  
Portal oder sogar einen intelligenten Agenten  
zur Verwaltung aller benötigten Finanz-  
dienstleistungen benutzen wird. In 64 Prozent  
der Fälle werden E-Banken von etablierten  
Finanzinstituten, die auch über ein Filialnetz  
verfügen, betrieben werden.



Während Bankkunden ihre Geschäfte im Jahr 1997 noch zu 85 Prozent über die Filiale und die restlichen 15 Prozent über Telefon (Call Center) abwickelten, wird sich dieses Verhältnis im Zuge der Entwicklung von Allfinanz-Portalen massiv verschieben. So wird in Zukunft mit einem verhältnismässig kleinen Anteil von 10 bis 20 Prozent «Filialtraditionalisten» gerechnet, während zwischen 60 und 80 Prozent der Bankkunden ihre Geschäfte über mehrere Kanäle wie Filiale, PC (Internet), Telefon (Call Center) und Multimat erledigen dürften. (Quelle: Booz-Allen & Hamilton, Finanzdienstleistungen)

→ Zeitpunkt das nach wie vor mangelnde Sicherheitsgefühl der Kunden. In der Tat steigern Portale, im Speziellen in der Bankenwelt mit ihren sehr hohen Sicherheitsanforderungen, die Komplexität gegenüber herkömmlichen E-Commerce-Lösungen um ein Vielfaches. Rund ein Drittel der deutschen Internet-Benutzer hat sich laut einer Umfrage der Financial Times Deutschland noch gar nie mit der Möglichkeit auseinandergesetzt, Bankgeschäfte online zu tätigen. Solche Ängste werden von den Medien mit teilweise tendenziöser Berichterstattung weiter geschürt. Dabei nehmen gerade die Schweizer Banken in Sachen Sicherheit weltweit eine Spitzenposition ein.

Die Schweizer Finanzinstitute haben schon vor mehr als zehn Jahren angefangen, ihre komplexen Systeme für Transaktionen in Datennetzen verfügbar zu machen. Viren und böswillige Hacker wurden erst dann zum Thema, als Rechner mit «heissen» Kunden-daten ans Internet angeschlossen wurden. Der Albtraum eines jeden Sicherheitsverantwortlichen ist es, dass ein Benutzer sich Zugang zu einem Rechner verschaffen kann und dann im Namen eines anderen eine neue Session eröffnet, ohne derjenige zu sein, für den er sich ausgibt. Andere Arten des unbefugten Eindringens lassen sich mittels Verschlüsselung und Zertifikaten ziemlich effizient bekämpfen.

### Gelebte Schweizer Ingenieurskultur

Dabei führt derzeit noch kein Weg an so genannten Public-Key-Infrastrukturen (PKI) vorbei. Dieses Verfahren ist in der Lage, gleich alle drei Voraussetzungen für die sichere Durchführung eines elektronischen Geschäfts

## DIE ETABLIERTEN FINANZINSTITUTE VERZEICHNEN EIN STARKES WACHSTUM BEI DEN KUNDEN, DIE ONLINE-BANKING-VERTRÄGE ABSCHLIESSEN.

abzudecken: Zugriffsschutz, Schutz der Übertragungsinhalte vor Manipulation und der sichere Austausch von Schlüsseln zur Chiffrierung der Transferdaten. Derzeit stellt aber das grösste Problem aller PKI-Lösungen die Frage dar, welche Instanz letztlich in wessen Auftrag Zertifikate ausstellen und diese zertifizieren soll.

Für die Authentisierung auf einem Trägermedium, wie beispielsweise einer Smartcard, favorisieren Experten jüngst so genannte Class-3-Reader. Das sind plattformunabhängige Geräte, die an keinem Netz hängen und daher resistent gegen Viren sind. Mittelfristig gehen die Fachleute davon aus, dass sich eine gemischte Authentisierungslösung, beispielsweise aus Chipkarten und Zertifikaten, durchsetzen wird.

Die Diskussion über die effizientesten und benutzerfreundlichsten Sicherheitsmassnahmen fürs E-Banking wird aber fortlaufend geführt und stellt ein zeitgemässes Einsatzgebiet für die traditionelle Schweizer Ingenieurspraxis dar. Letztlich kann nur gesagt werden, dass Sicherheit immer ein Spiel mit der Wahrscheinlichkeit ist, bei dem es darum geht, die Risiken zu Gunsten oder Ungunsten des Business abzuwägen.

### Trend zum personalisierten Bank-Portal

Das Marktforschungsunternehmen Meta-group rechnet damit, dass im Jahr 2004 mehr als 80 Prozent der gutverdienenden Einzelpersonen ein personalisierbares Bank-Portal benutzen werden, auf dem sie nebst Wertpapiergeschäften und der Bewirtschaftung des Bankkontos auch Finanzprodukte wie Hypotheken, Kredite und sogar Versicherungen beziehen und verwalten dürften. Ferner darf auch davon ausgegangen werden, dass neue Mobiltelefongenerationen einen weiteren beliebten Zugangskanal zu diesen personalisierten Angeboten darstellen werden. Für die Banken heisst das, dass heute teilweise in Einzelapplikationen verfügbare Dienstleistungen wie etwa Kursinformationen, Zahlungsaufträge, Wertschriftenhandel, Kontoführung und Portfoliobewertungen in eine homogene Lösung mit Single Signon zusammengeführt

werden müssen. Der Bankkunde soll von jedem Ort und Endgerät aus in der Lage sein, in diesen Multichannel-Umgebungen Transaktionen durchzuführen, ohne dass er sich für jede Aufgabe erneut ausweisen muss. Weitere Vereinfachungen in der Kundenkommunikation erhofft man sich vom Einsatz angereicherter E-Mail-Lösungen oder so genanntem Secure Messaging.

Im Rennen um das Allfinanz-Portal von morgen sind die etablierten Geldinstitute klar besser positioniert als die Neueinsteiger. Der Hauptgrund dafür ist, dass sie über grosse Kundenstämme, weitreichende Dienstleistungen, gut eingeführte Marken und viel Vertrauen verfügen. Was im herkömmlichen Bankgeschäft gilt, wird auch im E-Banking zu den wichtigsten Differenzierungsfaktoren werden.

# Sicherheit, Standards und andere Aspekte

KORNEL WASSMER  
ERKLÄRT IM GESPRÄCH MIT  
NOTITIA ENTWICKLUNGS-  
PRINZIPIEN BEI ADNOVUM.

INTERVIEW: PETER RÉVAI

NOTITIA: Was sind die Basisprobleme bei der Entwicklung eines Finanzportals, einer E- oder Internet-Bank?

Kornel Wassmer: Finanzapplikationen werden in der Regel nie auf der grünen Wiese entwickelt. Entwicklungen im Internet-Banking-Bereich, wie sie von einigen Dot-Com-Firmen in Angriff genommen wurden, sind zwar technisch sehr interessant, aber sie stellen die Ausnahme von der Regel dar. In der Praxis kommen solche Internet-Finanzapplikationen eher als neue Dienstleistungen zu bestehenden hinzu und müssen deshalb in eine Basisinfrastruktur eingebunden werden. Unsere Aufgabe ist deshalb die Integration. Dabei gilt es, Standardprozesse wie etwa die Kontenführung oder den Zahlungsverkehr in funktionsfähige Lösungen einzubauen.

### Kornel Wassmer

Kornel Wassmer ist seit August 1996 bei AdNovum tätig. Der diplomierte Informatik-Ingenieur ETH löscht mit Leidenschaft alles, was brennt, egal, ob als stellvertretender Feuerwehrkommandant in seiner basellandschaftlichen Wohngemeinde Gebäude, die in Flammen stehen, oder als Head of Development Entwicklungsknacknüsse, die gelöst werden wollen. Wann immer bei AdNovum Dringliches ansteht, ist Kornel Wassmer zur Stelle. Kein Wunder heisst sein Arbeitszimmer bei der AdNovum «Pyrodrom» und sein Entwicklermotto «Software-Bau ist Ernsteinsatz».

Vielerorts werden mit beträchtlichen Mitteln Finanzportale entwickelt. Sie selbst bauen unter anderem am Zurich FinancePoint mit. Was sind hierbei die besonderen Problemstellungen? Unsere Konzentration gilt der Implementierung von Lösungen in bestehende Systeme. In der Bankenwelt handelt es sich meist um solche, in denen mehrere tausend Mannjahre

## « UNSERE KONZENTRATION GILT DER IMPLEMEN- TIERUNG VON LÖSUNGEN IN BESTEHENDE SYSTEME. »

Arbeit oder 40 Jahre Entwicklung drinstecken und die ihre Anfänge in den frühen 60er Jahren hatten. Datensammlungen dieser Art lassen sich nicht einfach mir nichts, dir nichts wegwerfen. Es ist sehr viel Wissen in diese Systeme eingeflossen. Sie sind sehr gut und unterstützen weiterhin das Tagesgeschäft optimal. Es handelt sich dabei immer um aussergewöhnlich gutes Engineering, das dabei zum Zug gekommen ist.

Was ist Ihre Vorgehensweise an ein Legacy-System?

Die Kunst ist abzuschätzen, wie neue Technologien sich so einbringen lassen, dass das Legacy-System nicht allzu stark vergewaltigt wird. Es gilt also, das Beste aus dem Legacy-System in dem Sinn herauszuschälen, dass es zwanglos auf partnerschaftlichem Fuss mit unseren Lösungen bleibt. Denn jedes Legacy-System enthält Business-Funktionalitäten, mit denen wir arbeiten wollen. Es spricht für die Systeme, dass sie seit Jahren produktiv die höchsten Anforderungen erfüllen. Unsere Hauptarbeit ist daher rein technischer Natur. Die Frage lautet nämlich, wie sich diese

gewaltigen Datenströme auf einer technischen Ebene integrieren lassen.

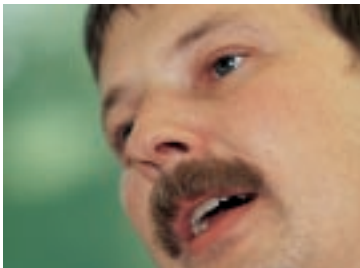
Welche Probleme warten bezüglich Implementierung neuer Technologien auf Sie? Um welche neuen Techniken handelt es sich primär?

Es handelt sich um den ganzen Baukasten, den man gemeinhin mit Web-Technologien

bezeichnet. Dazu zählen Java, HTML, Internet und Sicherheit. Es geht vor allem darum, was in den letzten zehn Jahren in der Forschung gelaufen ist, und das sind primär mit allen Vor- und Nachteilen verteilte Systeme. Es gibt allerdings ein klares Delta zwischen den Möglichkeiten, die die neuen Techniken wie Java oder Servlet-Engines bieten, und der Art und Weise, wie sich die Legacy-Systeme präsentieren. Unsere Kompetenz besteht nun darin, diese Lücke auf eine dem Projekt angepasste Art und Weise zu stopfen und gleichzeitig alle Sicherheitsaspekte abzudecken.

Um welche Lücken handelt es sich im Security-Bereich?

Typischerweise sind diese Legacy-Systeme in sich geschlossene Systeme, die nur bestimmte Sicherheitsfunktionen anbieten. Die Authentisierung erfolgt in der Regel über Terminals, über die sich Benutzer anmelden müssen und worin die Security-Funktionen voll integriert sind. Diese Techniken stehen allerdings in einem gewissen Widerspruch zu den Web-Techniken, zum Internet-Banking und zu den





→ Portalen, bei denen die Sicherheit auch direkt integriert ist. Damit die State-of-the-art-Aspekte der Sicherheit in die Gesamtlösung passen, muss man am Legacy-System selber diesbezügliche Abstriche machen. Zu diesem Zweck muss es Sicherheitsfunktionalitäten delegieren, damit überhaupt die Möglichkeit besteht, Anfragen zu machen.

#### Pflegt AdNovum dafür einen speziellen Ansatz?

Wir propagieren hauptsächlich die Single-Signon-Lösung, dank der sich Benutzer für alle Dienste nur einmal beim Portal anmelden müssen. Die Authentisierung erfolgt auf Basis der modernen Mechanismen mit Zertifikaten in den verschiedenen Formaten oder über bestimmte proprietäre Produkte wie SecurID. Im Idealfall sind dann alle Applikationen hinter dem Portal bereits auf die Bedürfnisse des Anwenders angepasst und ermöglichen dadurch eine personalisierte Sicht auf die verfügbaren Dienste.

#### Erschwert das Ende von Zertifizierungsstellen wie Swiss Key ihre Arbeit?

Aus technischer Sicht ist das kein Problem. Es ist vielmehr eine organisatorische Knacknuss,

Finanzdienstleister sind daran interessiert, einen möglichst grossen Kundenkreis zu erschliessen, wie etwa beim klassischen Telebanking, bei dem Hunderttausende bis Millionen Kunden mit entsprechendem Ver-

kehrsaufkommen und entsprechend hohen Transaktionsvolumina die Regel sind. Es sind diese Transaktionen, die typischerweise auf die Legacy-Systeme zugreifen. So sollte unsere spezielle Integrationslösung in der Lage sein, genau solch hohe Lasten abzufertigen.

#### Was sind schlagwortartig die grossen Probleme bei grossen Transaktionsvolumina?

Wir müssen in der Lage sein, richtig abzuschätzen, wie ein hohes Transaktionsvolumen verarbeitet werden kann. Je mehr Codes es

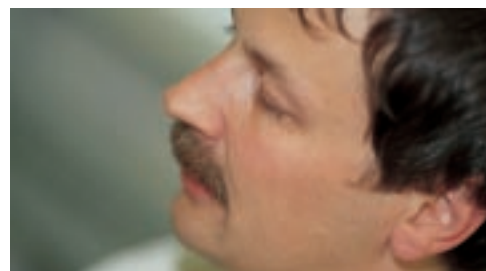
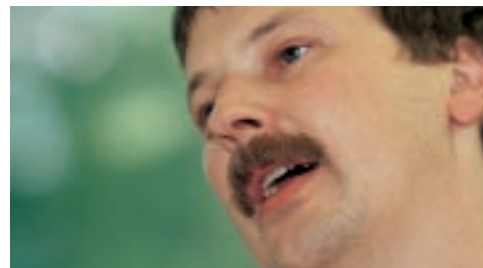
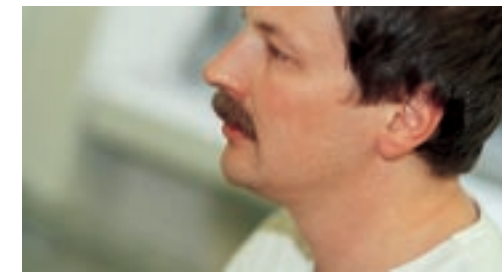
beispielsweise gibt, desto schwerfälliger wird die Lösung. In erster Linie ist deshalb alles eine Frage der richtigen Abstraktionsstufe, wie diese Transaktion vom Portal zum entsprechenden Verarbeitungssystem zu schleusen ist. Es geht um das richtige Abwägen von verschiedenen Faktoren wie Preis, Grösse der Lasten, Anzahl der Konfigurationsparameter oder der Komplexität im Handling.

## « EIN PORTAL MUSS IN DER LAGE SEIN, NACH BEDARF DIE SICHERHEITSSTUFEN ZU ERHÖHEN. »

Typischerweise handelt es sich bei unserer Integrationsarbeit meist um Systeme, die einen äusserst proprietären Charakter aufweisen. Das heisst aber nichts anders, als dass sie in ihrer Ausprägung weltweit einmalig sind. Die Frage von «make it or buy it» muss man also in diesem Kontext immer mit «make it» beantworten.

#### Was sind Ihre Anforderungen?

Für ein Portal-System oder eine Internet-Banking-Lösung muss ganz klar die Skalierbarkeit im Vordergrund stehen. Denn die



#### Wegen der Sicherheit?

Deshalb und wegen des integrativen und gleichzeitig proprietären Aspekts, damit man, falls einmal nötig, bis auf Bits und Bytes die Zugriffskontrolle hat. Wobei natürlich die Sicherheit schon den zentralen Aspekt darstellt.

#### Kann man bei Ihrem Single-Signon-Mechanismus von State-of-the-art sprechen?

Ja, ich denke schon. Es zeichnet letztlich auch gutes Software-Engineering aus, die richtigen Randbedingungen geschickt in einer Entwicklung zu berücksichtigen. Denn es müssen schliesslich Lösungen entstehen, die einerseits skalierbar, sicher und betreibbar sind und andererseits trotz ihrer Komplexität umfänglich nicht ins Unermessliche ansteigen

#### Können Sie das präzisieren?

Wir gehen typischerweise von 3-Monats-Zyklen aus. Im Jahr haben wir also drei bis vier grössere Releases pro Applikation oder pro Portal. Unsere Entwicklung erfolgt beinahe rollend: eine Version ist in Produktion, eine andere im Test, die dritte in der Entstehung, und die vierte befindet sich noch in der Abklärungsphase. So müssen wir immer wieder abwägen, wann wir welche Komponenten lancieren. Das ist auch davon abhängig, zu

Denn für uns gibt es keine Systeme – weder neue noch bekannte –, die uns nicht interessieren.

#### Wie sollen Services gestaltet sein?

Heutzutage melden sich Benutzer für Dienste an. Aber Dienste müssen letztlich zum Benutzer kommen. Denn hinter einem Finanzportal können sich beliebige Dienste verbergen. Deswegen muss ein Portal in der Lage sein, nach Bedarf die Sicherheitsstufen

Die Qualität eines Security-Mechanismus liegt ja gerade darin, dass er nicht proprietär oder geheim ist. Deswegen bauen wir auf Standards wie die Public-Key-Infrastrukturen (PKI) mit SSL und die X.509 Zertifikate sowie auf andere bekannte Mechanismen.

#### Was ist Ihre Spezialität?

Unser Added Value ist, dass die Codebasis unserer Produkte von uns so aufbereitet wird, dass diese im professionellen, sehr sicherheitssensitiven Finanzdienstleistungsumfeld problemlos eingesetzt werden können. Gleichzeitig berücksichtigen wir in unseren Lösungen auch betriebliche und betriebsorganisatorische Aspekte.

## « FÜR UNS GIBT ES KEINE SYSTEME – WEDER NEUE NOCH BEKANNTE –, DIE UNS NICHT INTERESSIEREN. »

welchem Zeitpunkt ein Kunde eine neue Dienstleistung einführen will, zumal dieser sich selbst im Markt bewegt und daher den Wettbewerbsvorteil gegenüber der Konkurrenz für sich beanspruchen will.

Obiges wurde von uns mehrfach unter Beweis gestellt. Zurückzuführen ist das auf die Tatsache, dass wir in unserem Haus zum einen ein sehr breites und tiefes Verständnis für die neuen Technologien haben und auf der anderen Seite auch über ausreichendes Wissen über Legacy-Systeme verfügen. Als Software-Ingenieure haben wir keine Schwellenangst, etwas Neues einzubinden.

zu erhöhen. Es wird möglich sein, verschiedene Einstiegsformen von UserID und Passwort über Zertifikate bis hin zu biometrischen Mechanismen wie Fingerabdruckererkennung anzubieten.

#### Setzen Sie dabei auf Standards?

Wir setzen, wann immer möglich, auf Standards. Denn der Einbau proprietärer Security-Mechanismen widerspricht eigentlich dem Gedanken der Sicherheit. Denn wenn diese proprietär sind, gerät man leicht in den Verdacht, dass mit der Sicherheit etwas nicht stimmen kann.

#### Top-Entwickler im Einsatz

AdNovum ist auf die Entwicklung massgeschneiderter Lösungen für grosse Finanzdienstleistungs- und Telecomunternehmen spezialisiert. Von den rund 90 Mitarbeitern sind 65 Prozent Entwickler. Grösstenteils absolvierten sie die ETH Zürich, die Universität Zürich sowie das MIT in Boston. Ihr Durchschnittsalter beträgt 30 Jahre.

# Mit Wahrscheinlichkeiten umgehen oder Sicherheit in die Praxis umsetzen

DAS INTERNET-BANKING STELLT HEUTE KEIN BESONDERS HOHES RISIKO MEHR DAR, SOFERN GRUNDLEGENDE VORSICHTSMASSNAHMEN BEFOLGT WERDEN. DER SICHERHEITSSTANDARD IN DER SCHWEIZ IST HOCH UND EINHEIMISCHEN ENTWICKLERN ZU VERDANKEN.

VON MATTHIAS LOEPFE

Jeder, der genügend Ressourcen hat, kann sich im Prinzip unbemerkt Zugriff in Netze verschaffen. So beschäftigt sich AdNovum seit der Gründung vor rund 13 Jahren mit Fragen der externen Sicherheit, da die Schweizer Finanzinstitute, AdNovums Stammkundschaft, schon sehr früh angefangen haben, ihre komplexen Systeme für Transaktionen im Netz verfügbar zu machen.

Solange es jedoch kein Internet gab und in diesem Kontext keine Virengefahr bestand, stellten interne E-Mail-Systeme lange kein Problem dar. Die interne Sicherheit wurde erst zum Thema, als Rechner mit «heissen» Daten ans Internet angeschlossen wurden. Interne Sicherheit beginnt bei der ganz realen physischen Absicherung: Serverräume müssen prinzipiell immer abgeschlossen sein. Zunehmend wichtiger wird der Einsatz von Firewalls, IDS (Intrusion Detection Systems), Sicherheitstests wie das so genannte Vulnerability Assessment und starke Authentisierung.

## Kein Verkauf von Quellcode

Trotzdem kann es im Prinzip immer Leute oder Organisationen geben, die sich Zugriff in ein Netz verschaffen können, ohne dass der Betreiber davon etwas merkt. Sie müssen allerdings über grosse finanzielle und ausgefeilte technische Ressourcen sowie über ein sehr gutes Know-how verfügen. Da jedes noch so gute System aus Gründen der Anwendbarkeit in gewissem Umfang durchlässig sein muss, hat es immer einige «Löcher», die nicht dicht zu machen sind.

Grundsätzlich muss man sich dennoch keine übertriebenen Sorgen machen, dass sich jeder, der will, Zugriff in unternehmensweite

Netzwerke verschaffen kann. Allerdings gibt es Organisationen, etwa ausländische Geheimdienste, die dafür finanzkräftig und technisch versiert sind. So verlor Airbus einen Milliarden-Auftrag in Saudi-Arabien, weil die amerikanische Flugzeugindustrie mit Hilfe der NSA (National Security Agency) sämtliche elektronischen Nachrichten der Europäer abhören und entziffern konnte.

Mit solchen Bedrohungen haben wir keine grossen Probleme. Wir leben im Gegensatz zu Herstellern von Standard-Software von unse-

## INTERNE SICHERHEIT BEGINNT BEI DER GANZ REALEN PHYSISCHEN ABSICHERUNG.

rem Wissen und nicht vom Verkauf von Quellcode. Darum geben wir ihn auch immer an Kunden weiter, weil wir nicht glauben, dass uns damit jemand schaden könnte. Denn unser Vorteil ist der Informationsvorsprung.

Wir wenden verschiedene Sicherheitsstufen an, um den Zugriff von Unbefugten auf Kundendaten zu vermeiden. Erstens versuchen wir, das Volumen an Kundendaten bei uns auf ein Minimum zu beschränken. Zweitens sorgen wir dafür, dass «heisse» Daten wie Core-Dumps von produktiven Systemen, in denen sich Schlüssel von Web-Servern oder auch Passwörter oder Schlüssel zu Kundensessions finden lassen, nach Möglichkeit nicht online sind und dass wir drittens nur Testdaten bekommen, aus denen Kunden nicht ersichtlich sind.

Wir behalten die Daten nur so lange bei uns, wie wir sie brauchen. Sobald Core-Dumps

oder Log-Files von uns analysiert sind, werden sie gelöscht. Solange die Daten bei uns sind, bekommen nur die damit befassten Mitarbeiter die Zugriffsberechtigung. Und natürlich schützen wir unser Netzwerk im üblichen Rahmen mit typischen Firewall-Einrichtungen und einer Netzwerktopologie mit Switches.

## Keine vollständigen Tests

Prinzipiell lassen sich aus finanziellen Gründen komplexe Software-Systeme kaum vollständig austesten. Daher weiss man auch nicht mit Bestimmtheit, ob sich ein System immer so verhält, wie es geplant war. Doch wenn alle Regeln und Gepflogenheiten beim Programmieren eingehalten werden, kann man in der Regel davon ausgehen, dass ein System nach dem jeweiligen Wissensstand als sicher gilt. Zu bedenken ist aber auch, dass nicht alle Tests völlig verlässlich sind.

Deshalb sprechen wir heute auch nur noch von den so genannten «Best Practices». Das bedeutet, man ergreift optimale Mittel und Massnahmen, um auf ein vernünftiges Mass an Sicherheit zu kommen, ohne dass es die verfügbaren Mittel sprengt. Komplett massgeschneiderte Sicherheitsmassnahmen für jedes System sind heute nicht mehr machbar.

Zu den «harten» Sicherheitsmassnahmen zählt beispielsweise, nie eine unchiffrierte Datenverbindung vom Internet bis zur Bank



Matthias Loepfe ist Chief Technical Officer der AdNovum. Der gelernte Elektrotechniker und Informatiker ist bei AdNovum seit 1989 für die technischen Entwicklungen verantwortlich.

der Wahrscheinlichkeit, da es nahezu unmöglich ist, ein Risiko mit Bestimmtheit zu beziffern. In den meisten Fällen geht es sowieso um heikle und unquantifizierbare Sachverhalte wie etwa den Ruf einer Bank oder Versicherung, der dabei auf dem Spiel steht.

## Einen Schritt näher

Momentan bewegen wir uns in einem fast avantgardistischen Bereich, in dem es vermehrt um Transaktionen geht. Wir gehen davon aus, dass das Sicherheitssystem und das transaktionelle System gemeinsam funktionieren werden. Die AdNovum-Lösungen lassen sich sehr gut skalieren: Das bedeutet, dass transaktionelle Systeme sowohl für Applikationen mit Minimalanforderungen an die Sicherheit als auch ausfallsichere Anwendungen auf demselben Datenpfad von einem Client via Browser bis auf ein Host-System genutzt werden können.

Damit ist man der sicheren Transaktion ein Stück näher. Aber sicher ist eine Transaktion nur, wenn man genau dann mit grosser

Sicherheit weiss, wer eine Transaktion ausgelöst hat, wenn sie gerade abläuft. Lückenloses Auditing ist gegeben, wenn der Absender als Initiator ebenso erkennbar wird, wie sich der Pfad lückenlos zurückverfolgen lässt, den seine Daten genommen haben. Seine so genannte Schleimspur muss sichtbar bleiben.

Dagegen gilt als «worst case»-Szenario, wenn sich jemand Zugang zu einem Rechner verschaffen konnte und dann im Namen eines anderen eine neue Session eröffnet, ohne derjenige zu sein, für den er sich ausgibt. Der Grosszahl der übrigen Attacken wie etwa der so genannten «Man in the Middle Attack» kann mittels Verschlüsselung und Zertifikaten effizient begegnet werden.

## Sicherheit durch Aufklärung

Die Sicherheit eines privaten PC lässt sich im Grunde nur durch umfangreiche Aufklärung des Anwenders und einige technische Hilfsmittel wie etwa persönliche Firewalls gewährleisten. Sobald ein Virus eindringt, lassen sich die Auswirkungen mit Client-

Zertifikaten auf Chipkarte oder One-time-Passwörtern via Streichlisten auf aufwändige Art eindämmen, zumindest solange diese Daten nicht auf dem befallenen Rechner abgelegt worden sind.

Einen geringen Aufwand für die Anwender würden Class-3-Reader bedeuten. Das sind plattformunabhängige Geräte, in die sich Chipkarten zur Authentisierung stecken lassen und die mittels eines «Challenge-Response»-Verfahrens arbeiten. Nur dieser Akt bewirkt eine Systemantwort, die eine Session möglich macht. Er gleicht einer Willensäusserung, der mit einer «analogen Unterschrift» bekräftigt wird. Wesentlich ist, dass die Reader eigenständige Kleincomputer sind, die an keinem Netz hängen, und man auf deren Anzeige tatsächlich auch das sehen kann, was man unterschreiben soll. Dann ist ein bestimmter Code einzugeben, was als Signatur-Anweisung anzusehen ist.

## Gefahr bei der Implementierung

Nach heutigem Wissensstand sind die verfügbaren Sicherheitslösungen in der Regel genügend sicher. Die Wahrscheinlichkeit, dass ein Fehler passieren kann, ist ausreichend klein. Allerdings halten wir es trotzdem mit dem Sicherheits-Papst Bruce Schneider, der in seinen kürzlich unter dem Titel «Meiden Sie Microsoft» veröffentlichten Tipps für den Computerhausbgebrauch meint, dass es keinen perfekten Schutz gebe. Aber selbst das NT-System und seine Nachfolger sollten relativ sicher sein. Allerdings muss man über ein umfangreiches Wissen darüber verfügen. Denn Microsoft soll als Grossanwenderin ihrer eigenen Produkte nur diejenigen Fehler wirklich beseitigen, von denen sie selbst betroffen ist.

Die wirklichen Gefahren sind Programmier-, Konfigurations- und Operating-Fehler. Die grösste Bedrohung kommt von Algorithmen, die falsch implementiert sind. Wir programmieren deshalb defensiv, so dass, falls etwas schief läuft, nur ein Minimum «in die Hosen gehen» kann. Wir befolgen einige strikte Regeln und wenden gute Werkzeuge an: Schlussendlich entscheidend ist jahrelange Programmiererfahrung im Zusammenspiel mit einem eigentlichen Programmiererethos.

Wichtig ist auch, ein Konzept immer wieder erneut durchzudenken und stichprobenmässig zu prüfen, ob es richtig implementiert ist. Denn bei grossen Systemen ist es, wie bereits erwähnt, heutzutage praktisch unmöglich, jede Zeile zu betrachten und zu verstehen, was sie bewirkt. ■



NEVIS IST EINE IT-ARCHITEKTUR, DIE FÜR SICHERE WEB-APPLIKATIONEN UND PORTALE ENTWICKELT WURDE. SIE KOMMT VORWIEGEND IM FINANZBEREICH ZUM EINSATZ, DA SIE DIE HÖCHSTEN ANFORDERUNGEN AN DURCHGÄNGIGER SICHERHEIT UND FLEXIBLER SKALIERBARKEIT ERFÜLLT. SEIT DEM JAHR 1994 WIRD DAS URSPRÜNGLICHE RAHMENWERK KONTINUIERLICH WEITERENTWICKELT UND LAUFEND DEN AKTUELLSTEN TECHNOLOGISCHEN VERÄNDERUNGEN ANGEPAST.

Grundsätzlich unterscheidet man vier verschiedene Typen von internetfähigen Geschäftsanwendungen. Davon stellen Publishing- und einfache E-Commerce-Anwendungen keine hohen Anforderungen an Skalierbarkeit, Sicherheit, Integration und Session Handling. Ein diesbezüglich höheres Anforderungsprofil weisen Applikationen auf, die wie Finanzpor-

gen zu entscheidenden Erfolgsfaktoren. Bei der AdNovum-Entwicklung Nevis handelt es sich um eine hochmoderne Web-Architektur für diesen vierten und komplexesten Typ einer Internet-Business-Applikation. Bei AdNovum ist Nevis ein Rahmenwerk, das aus drei Kernkomponenten besteht und die transparente und sichere Intranet- und Internet-

**DER DIREKTE UND UNÜBERWACHTE ZUGRIFF AUF  
DIE ORIGINALINFORMATIONEN BLEIBT DEN BENUTZERN  
VERSCHLOSSEN.**

tale Realtime-Börsenkurse anbieten. Handelt es sich jedoch um eine hochvolumige, transaktionsorientierte Anwendung, die darunter liegende Legacy-Systeme mit Oracle- oder DB2-Datenbanken oder sonstigen Mainframe-Applikationen anzapft, wie beispielsweise eine E-Bank oder der Online-Wertschriftenhandel, werden die erwähnten Anforderun-

Integration von Mainframe-Applikationen und Legacy-Datenbanken ermöglicht. Eine typische Transaktion, wie etwa die Abfrage des Kontostandes in der virtuellen Filiale einer Bank oder der Online-Kauf eines Wertpapiers, spannt sich dabei über drei Nevis-Zonen: die Internet-, die Firewall- und die Secure-Service-Zone. Die Architektur von Nevis erlaubt es, dass Benutzer von einer Vielzahl von Endgeräten wie etwa von einem PC via Browser, einem PDA, einem WAP-fähigen Mobiltelefon oder einem Multimat, einem stationären Geldautomaten mit erweiterten Funktionalitäten auf sensible Informationen in der Secure-Service-Zone zugreifen und Transaktionen auslösen können. Dies geschieht unter Einbindung der höchstmöglichen Sicherheit und durchgängig transparenter Benutzer-Authentisierung, wobei letzteres hier über einen so genannten Single Signon, eine einmalige Benutzeranmeldung gegenüber dem Portal, erfolgt.

Das Kernstück von Nevis ist der Secure Reverse Proxy ISIWEB. Es handelt sich um einen Proxy-Server, der ausserhalb der eigentlichen Firmen-Firewall lokalisiert ist. Seine Aufgabe ist es, externen Benutzern die Inhalte aus dem System innerhalb der Firewall zugänglich zu machen. Die Benutzer haben somit lediglich indirekten Zugriff auf diese Inhalte. Der direkte und unüberwachte Zugriff auf die Originalinformationen bleibt ihnen verwehrt. Durch den Einsatz eines solchen Reverse-Proxy-Servers bleiben die Originalinformationen in erhöhtem Masse geschützt, da nur authentifizierte und autorisierte Aufrufe auf Content Server den Proxy passieren dürfen. Der Wap-Proxy-Server ISIWAP kommt zum Einsatz, wenn von einem Mobiltelefon aus mit Hilfe der Wireless Markup Language (WML) auf Legacy-Datenbanken oder Legacy-Applikationen zugegriffen wird.

Namenslieferant von Nevis ist eine Antilleninsel in der östlichen Karibik, die nicht nur von Christoph Kolumbus auf seiner zweiten Amerika-Fahrt, sondern auch vom Ferienreisenden AdNovum-Gründer Stefan Arn entdeckt wurde. Nevis heisst die Insel nach dem spanischen Wort Nieves für Schnee, da Kolumbus fälschlicherweise glaubte, die von einer Wolke umhüllte Inselspitze sei eingeschneit.

Die zweite Kernkomponente von Nevis stellt der generische Authentisierungsservice esAuth dar. Er sorgt für eine transparente Authentisierung der Benutzer vom Browser bis in den Mainframe in einem Single-Signon-Rahmenwerk. Unter Single Signon versteht man den Umstand, dass der Benutzer gegenüber dem Service oder Portal nur eine einzige Identität anzugeben braucht und damit innerhalb des Portals automatisch auf alle berechtigten Dienste oder Informationen zugreifen kann. Systemintern kann diese Identität eine völlig andere sein, die nach aussen nicht erkennbar ist. Sie ist aber strikt an die authen-

tisierte Sitzung des Benutzers gebunden. Die Benutzerkonto-Informationen können in verschiedenen Authentisierungs-Backends (NISplus, ACE, ESAA, DynCA, Smartcard, LDAP) verwaltet werden. Für jedes Legacy-System, aus dem ein Benutzer Informationen beziehen will, wird erneut eine Authentisierung durchgeführt und rückbestätigt. Da die Authentisierungsstärke von Service zu Service oft variiert, sollte das Portal den Benutzer nicht automatisch zur stärksten möglichen Authentisierung beim ersten Anmelden (Login) zwingen. Deshalb unterstützt der Single-Signon-Mechanismus von Nevis so genanntes Session Step-up. Darunter versteht man eine mehrstufige Authentisierung, die den Benutzer im Verlauf einer Sitzung zur Eingabe von Zusatzinformationen, einem PIN-Code beispielsweise, anhält.

Die dritte Kernkomponente ist der Präsentationsdienst esPres, der in der Lage ist, HTML-Inhalte in Echtzeit zu erzeugen. Der Dienst esSpace ergänzt diese Fähigkeiten mit einer klaren Trennung der Präsentationsschicht von der Geschäfts- und Applikationslogik. Die Geschäftslogik-Komponente esXML baut auf modernster Servlet-Technologie auf. Sie ist mit den wichtigsten Standards wie Servlets API, XML und JSP kompatibel, die heute in zeitgemässen Applikationen verwendet werden. Dadurch wird die schnelle und bequeme Einbindung von neuen oder bereits vorhandenen Applikationsservern wie etwa Websphere von IBM ermöglicht. Die Nevis-Architektur erlaubt also, bereits getätigte Investitionen in Internet-Technologien optimal zu schützen. Das Modul esCSP (Channel Specific Presentation) schliesslich sorgt dafür, dass die Applikations- oder Datenbank-Inhalte direkt in ein beliebiges Benutzergerät formgerecht ausgegeben werden. Die gesamte Kommunikation unter den ein-

zelen Komponenten des Präsentations-Services läuft unter XML. Ausserdem ist der Präsentationsdienst kompatibel mit allen wichtigen Applikationsentwicklungsstandards wie J2EE (Java 2 Enterprise Edition) und CORBA (Common Object Request Broker Architecture). Dabei unterstützt Nevis auch durchgängig die eingebauten, sehr hohen Sicherheitsfunktionalitäten dieser Standards. Nevis wartet mit einer schlanken und flexiblen

Architektur, einem modulartigen Aufbau, einer transparenten Authentisierung mit Single Signon und der durchgängigen Sicherheit auf. Damit ist Nevis befähigt, die höchsten Anforderungen von Kunden aus der sicherheitsintensiven Finanzbranche für die Entwicklung von Web-Business-Applikationen vollständig abzudecken.

Das Diagramm zeigt die Architektur einer Web-Service-Integration, unterteilt in drei Zonen:

- INTERNET:**
  - Klienten:** Ein **KLIENT** (links) und ein **KLIENT** (rechts) kommunizieren über **HTTP(S)/IIOP(S) ETC.** mit der Firewall Zone.
  - WAP:** Ein **WAP** (Wireless Application Protocol) kommuniziert über **GSM/CSD** mit der Firewall Zone.
  - Proxy/Firewall:** Ein **KLIENT- ODER PROVIDER- PROXY UND/ODER FIREWALL** fungiert als Zwischenschicht zwischen dem rechten Klienten und der Firewall Zone.
- FIREWALL ZONE:**
  - FIREWALL:** Eine horizontale Firewall, die den Verkehr von der Internet Zone in die Secure Service Zone filtert.
  - PROXI-APLIKATIONSFILTER:** Ein zentraler Filter, der den Verkehr weiterleitet. Er enthält zwei Proxy-Komponenten: **ISI WAP PROXY** und **ISI WEB PROXY**.
  - FIREWALL:** Eine zweite horizontale Firewall, die den Verkehr von der Firewall Zone in die Secure Service Zone filtert.
- SECURE SERVICE ZONE:**
  - SERVICE:** Ein Service-Komponente, die über **GIOP ETC.** mit der Firewall Zone kommuniziert.
  - WWW:** Ein Web-Server-Komponente, die über **HTTP(S)** mit der Firewall Zone kommuniziert.
  - IIOP(S)/HTTP(S):** Ein Kommunikationskanal, der den Verkehr zwischen der Firewall Zone und den Applikationsservern sowie dem Authentisierungsdienst steuert.
  - APPLIKATIONSSERVER:** Ein Block, der verschiedene Applikationsdienste enthält: **SERVLET ENGINE**, **ESCSP**, **ESXML**, **ESPACE**, **ESPRES** und **WEB-SERVER**. Er ist mit **J2EE, CORBA UND ANDERE APPLIKATIONSDIENSTE (PRÄSENTATIONS- UND APPLIKATIONSLOGIK)** beschriftet.
  - AUTHENTISIERUNGSDIENST:** Ein Block, der den Authentisierungsprozess steuert. Er enthält die Komponente **ESAUTH**, die mit dem **AUTHENTISIERUNGS-BACK-END** (bestehend aus **UID/PW**, **ACE**, **NIS+** und **ANDERE**) kommuniziert.
  - DBs, Hosts, Feeds:** Eine Basisdatenkomponente, die mit **(GESCHÄFTSLOGIK)** beschriftet ist und über **IIOP(S)/HTTP(S)** mit den Applikationsservern und dem Authentisierungsdienst kommuniziert.

Bei der AdNovum-Entwicklung Nevis handelt es sich um eine hochmoderne Web-Architektur.

Unter Single Signon versteht man den Umstand, dass der Benutzer gegenüber dem Service oder Portal nur eine einzige Identität anzugeben braucht und damit innerhalb des Portals automatisch auf alle berechtigten Dienste oder Informationen zugreifen kann.

# iForce bündelt umfassendes Wissen

DIE iFORCE-INITIATIVE VON SUN MICROSYSTEMS WILL DIE KOMPETENZEN DES COMPUTERKONZERNS UND DIEJENIGEN IHRER LANGJÄHRIGEN PARTNER ZUSAMMENBRINGEN. ZIEL DER KOOPERATIONEN IST, DASS KUNDEN KOMPLEXE VERTIKALE UND HORIZONTALE LÖSUNGEN SCHNELLER UND EINFACHER IMPLEMENTIEREN KÖNNEN.

VON PETER RÉVAI

Im Frühling dieses Jahres hat Scott McNeally, CEO von Sun Microsystems, iForce angekündigt. Unter dieser Initiative versteht Sun eine intensivierte Zusammenarbeit zwischen dem Computerkonzern und seinen

dukte, Methodologien, Dienstleistungen und Applikationen, die allen Sun-Kunden, sowohl einem Start-up als auch einem Grossunternehmen, den schnellstmöglichen Einstieg ins Internet-Business gestatten sollen. Anlauf-

DIE IDEE HINTER iFORCE IST, DASS SUN-KUNDEN STETS DIE BESTMÖGLICHE IT-LÖSUNG AUS EINER HAND ERHALTEN.

weltweiten Partnern. Die Idee hinter iForce ist, dass Sun-Kunden für ihre Geschäftsprobleme stets die bestmögliche IT-Lösung – von der Analyse und dem Consulting bis zur Applikationsentwicklung – aus einer Hand erhalten. Die Initiative umfasst deshalb erprobte Pro-

punkte dafür sind mehrere weltweit gegründete iForce-Ready-Centers.

Dank den von der iForce-Community erarbeiteten «Best Practices» werden Unternehmen von verkürzten Markteintrittszeiten und der gemeinsamen Erfahrung von Sun und ihren Partnern profitieren können. In der Praxis bewährte Lösungen, so genannte PoCs (Proof of Concepts), werden in den iForce-Ready-Centern weiterentwickelt und an die Bedürfnisse der Kunden angepasst. Sun Microsystems bringt dabei ihre langjährige Erfahrung aus der Entwicklung kritischer IT-Business-Architekturen mit ihrer robusten Client-Server-Hardware, dem Betriebssystem Solaris und der Softwareplattform Java/EJB (Enterprise Java Beans) mit ein. Das erprobte «Sun ONE»-Rahmenwerk erlaubt zudem die bequeme Realisierung von sicheren, transaktionsorientierten Java-Diensten und die nahtlose Integration von Legacy-Systemen in eine Java-Enterprise-Lösung. «Sun ONE» ist offen und unterstützt verschiedene Plattformen. Die Vorteile, die aus der Verwendung von iForce-Komponenten bei der Entwicklung von komplexen Internet-Anwendungen im Finanzbereich resultieren, sind mannigfaltig. Für einen Sun-Partner wie die AdNovum etwa ist es wichtig, dass ein kontrollierter und bereits getesteter Sicherheits-Layer wieder- verwendet und die Implementierungszeit

dank den gemeinsam über die Jahre erarbeiteten «Best Practices» drastisch verkürzt werden kann. Internet-Finanzanwendungen «made in Switzerland» gehören zu den besten der Welt. Diese Tatsache hat Sun auch mit der Eröffnung des Kompetenzzentrums «eFinance-Practice» in Zürich unterstrichen. Unter dem Einsatz von erprobten Lösungen und Methoden sowie fortschrittlicher Technologie werden dort anspruchsvolle Kunden aus ganz Europa und Nordamerika bedient. Involviert ist dabei auch AdNovum als einer der wichtigsten Sun-Partner im E-Finanzbereich mit der IT-Architektur Nevis, die von AdNovum für sichere Web-Applikationen und Portale entwickelt wurde. ■

## Sun Microsystems

Seit 1989 ist AdNovum strategische Partnerin von Sun Microsystems (Schweiz) AG. Sun Microsystems wurde 1982 gegründet und hat sich seitdem mit der Vision «The Network Is The Computer» zu einer führenden Anbieterin von Produkten, Technologien und Dienstleistungen für das Internet entwickelt. Das US-Unternehmen ist heute in über 170 Ländern vertreten, zählt in der Schweiz rund 400 und weltweit 43 000 Mitarbeiter und hat das Geschäftsjahr 2000 mit einem Umsatz von 18,3 Milliarden US-Dollar abgeschlossen.

Im Software-Bereich hat das Unternehmen in diesem Jahr wesentliche Entwicklungen für die iPlanet-Produktlinie und die Java-Technologien geleistet. Die Plattform Solaris 8 wurde mehrfach als bestes unternehmenskritisches Serverbetriebssystem ausgezeichnet. In der Hardware-Sparte wurden neben Datenspeichersystemen die Workstation-Serie Sun Blade 1000, die Netra-Server und die Mittelklasse-Server-Reihe Sun Fire neu eingeführt. In diesem Jahr will Sun die Serie Sun Fire ebenso wie weitere Produkte auf Basis der hauseigenen Chip-Technologie UltraSPARC III lancieren.

## Impressum

### Herausgeber:

AdNovum Informatik AG  
Corporate Marketing  
Röntgenstrasse 22  
CH-8005 Zürich  
Telefon 01 272 61 11  
Telefax 01 272 63 12  
E-Mail [info@adnovum.ch](mailto:info@adnovum.ch)  
[www.adnovum.ch](http://www.adnovum.ch)

### Verantwortlich für diese Ausgabe:

Thomas Schönfelder, Head of Services

### Gestaltung und Realisation:

Rüegg Werbung, Zürich

### Redaktion:

matak (modulare agentur für technologie und kultur) gmbh, Zürich

### Fotografie:

Matthias Auer, Zürich

# NOTITIA

BEMERKENSWERTES VON UND ÜBER ADNOVUM

## Internet-Banking

Die Banken haben einen neuen Vertriebskanal

## Sicherheit mit und ohne Standards

Engineering-Aspekte bei der Entwicklung von Bankapplikationen

## Nevis unter der Lupe

Portale bauen mit der IT-Architektur von AdNovum

HERBST 2001, NR. 1

FINANZPORTALE