# NOTITIA

AdNovum

Bemerkenswertes von und über AdNovum

## Sharing Experience

Neupositionierung bewährter Beratungsdienstleistungen

## Modern Threats – Risiken im E-Business

Mit integraler Analyse zu kundenspezifischen Lösungsansätzen

## Experimentalanalyse in Projektreviews

Verhaltensforschung an komplexen verteilten Systemen

Herbst 2006, Nr. 11

Sharing Experience

Liebe Leserin, lieber Leser

Chancen soll man bekanntlich packen. Im Januar 2007 übernehme ich bei der UBS AG die Leitung eines IT-Ressorts. Nach 19 Jahren AdNovum widme ich mich damit einer neuen Aufgabe, dem Corporate IT-Development im internationalen Umfeld eines global tätigen Finanzunternehmens.
Der Zeitpunkt ist ideal: In der AdNovum hat sich in den letzten Jahren eine neue Führungsschicht etabliert, welche das Projektgeschäft in gewohnter Zuverlässigkeit und Qualität weiterführen und ausbauen wird. Führungseinheit und Motor der AdNovum bleibt das Projekt.

# Sharing Experience

In Zusammenhang mit IT-Projekten sind vermehrt fundierte Beratungsleistungen gefragt. Aufbauend auf ihrer umfangreichen Erfahrung in End-2-End-Umsetzung positioniert sich AdNovum auch in diesem Bereich mit einem Premium-Angebot.

Von Tobias Murer

Die Durchführung anspruchsvoller Software-Engineering-Projekte ist die Kernkompetenz der AdNovum. Die konsequente Ausrichtung auf dieses Kerngeschäft wird AdNovum auch in Zukunft weiterverfolgen. Ein zentraler Erfolgsfaktor ist die in den Projekten gewonnene immense Umsetzungserfahrung der Mitarbeiter, verbunden mit der Fähigkeit, diese kontinuierlich weiterzuentwickeln und über Projekte hinweg zu teilen und zu nutzen.

In den vergangenen zwei Jahren hat die AdNovum ihre Erfahrung vermehrt im Rahmen von Beratungstätigkeiten eingebracht, nicht zuletzt auch getrieben durch Umbrüche und Trends im IT-Markt und die entsprechend ausgerichtete Entwicklung des Unternehmens. Als Konsequenz davon bietet AdNovum Engineering orientiert am Leitgedanken «Sharing Experience» neu hochwertige Beratung als klar positionierte Dienstleistung an, um die Kunden und die AdNovum auch ausserhalb von Umsetzungen von der Erfahrung profitieren zu lassen. Dieser Artikel skizziert die Motivation und die Positionierung dieser Beratungsdienstleistung.

## IT-Markt Schweiz im Umbruch

Der IT-Markt in der Schweiz ist im Umbruch. Zu den beobachtbaren Trends gehört einerseits die teilweise Auslagerung der reinen Softwareentwicklung (Codier-Arbeiten) ins Ausland (Near- und Offshoring). Andererseits ist heute auf Seite der Anwender grosses IT-Fachwissen vorhanden, die Kunden können damit präziser einschätzen, inwiefern die IT ihr Geschäft unterstützen kann und mit welchen Kosten und Risiken dies verbunden ist. Noch mehr als früher ist man sich heute bewusst, dass IT nie Selbstzweck ist.

> Kunden können heute die Vorteile, Risiken und Kosten der IT für ihr Geschäft präziser einschätzen.

Als Konsequenz der Geschäftsverlagerung und der erhöhten Marktreife wird neben der Umsetzung von IT-Projekten zunehmend auch hochstehende Beratung nachgefragt. Um erfolgreich zu sein, muss ein Schweizer Softwaredienstleister demnach beide Bedürfnisse berücksichtigen und die entsprechenden Kompetenzen pflegen:

- Umsetzungskompetenz

Kompetenz zur nachhaltigen und effizienten Lösung einer konkreten Problemstellung: Dies bedingt eine Art «Industrialisierung» des Softwareentwicklungsprozesses. Einzelne Prozessschritte können ausgelagert oder ins Ausland verlegt werden, um die entsprechenden Kosten zu senken. Die Umsetzung zu niedrigen Kosten bei hoher Qualität erfordert jedoch unter anderem eine sehr hohe Projektmanagementkompetenz und rationelle Prozesse.

- Beratungskompetenz

Kompetenz zur Identifikation einer der Umsetzung vorgelagerten oder übergeordneten Problemstellung und zur Skizzierung möglicher Lösungsansätze: Beratungskompetenz impliziert eine hohe fachliche Kompetenz kombiniert mit einer hohen sozialen Kompetenz (Zuhörfähigkeiten u.a.). Es ist sehr wichtig, dass der Kunde verstanden wird und dass durch genügend Erfahrung die «richtigen» (auftragsrelevanten) Probleme erkannt werden. Der Kunde verlässt sich bei einem Beratungsauftrag sehr stark auf die Erfahrung und Kompetenz seines Lieferanten.

Meine operativen Tätigkeiten übergebe ich an ein Team langjähriger Mitarbeiter und Mitglieder der Geschäftsleitung und einen extern rekrutierten CEO-Nachfolger in der Gewissheit, dass diese zusammen mit den 140 Mitarbeitenden die Weiterentwicklung der AdNovum bestens meistern werden. Mit einer reich gefüllten Projektpipeline und entsprechend guter Auslastung für mindestens 12 Monate hat die AdNovum eine solide Basis für Wachstum und Erfolg in ihrem dynamischen Umfeld.
Mit der nahtlosen Übernahme meiner Kundenkontakte durch das neue Leitungsteam gewährleisten wir unseren Kunden klar definierte Ansprechparter und eine einwandfreie Kontinuität der Geschäftsbeziehungen.
Der Titel der vorliegenden Notitia lautet «Sharing Experience» – unter diesem Leitgedanken positionieren wir unsere bewährten Beratungsdienstleistungen neu als offiziellen Teil unserer Angebotspalette auf dem Markt. Tobias Murer erläutert Ihnen die Grundsätze dazu, danach folgen Anwendungsfelder: über Sicherheit im E-Business gibt Michael Müller Auskunft, Thomas Klemm und Tom Sprenger berichten über neue Methoden in Projektreviews. Auf der Heftrückseite stellt Prof. Urs Gasser von der HSG die Forschungsstelle für Informationsrecht vor.
Bei Ihnen als Leserinnen und Leser der Notitia möchte ich mich für Ihre Treue herzlich bedanken und wünsche Ihnen für diese und alle zukünftigen Ausgaben gute Lektüre.

Stefan Arn

CEO AdNovum Informatik AG

## Umsetzungserfahrung

Dank einem Wachstum von gegen 100 Prozent in den vergangenen fünf Jahren ist die AdNovum heute in der Lage, eine eindrückliche Menge und Vielfalt an Leistungen zu erbringen. 140 Personen an drei Standorten wickeln bisweilen über 30 Projekte parallel ab und stellen durchschnittlich über zwei Softwarelieferungen pro Arbeitstag bereit. In Teams von bis zu 20 Mitarbeitern werden Projekte beachtlicher Grösse bearbeitet. Für ihr Kerngeschäft, die Durchführung und End-2-End-Unterstützung anspruchsvoller IT-Projekte, kann AdNovum deshalb auf einen eindrücklichen Erfahrungsschatz und ein umfassendes und in der Art und Abdeckung einzigartiges Portfolio an abgestimmten Kompetenzen zurückgreifen.

Zum Beispiel bildet die Erfahrung aus der eigenen Middleware-Entwicklung die entscheidende Know-how-Grundlage, um Anwendungen und die Anwendungsplattform mit denjenigen Eigenschaften auszustatten, welche für die Produktion erforderlich sind: Betreibbarkeit, Zuverlässigkeit, Sicherheit und Performanz.

Die Applikationsentwicklung und die Entwicklung von Middleware und Sicherheitskomponenten bieten wiederum unterschiedliche Herausforderungen und eine entsprechende Varianz an gewonnenen Erfahrungen: Während bei Applikationen, wenn die Geschäftsanforderungen einmal bekannt sind, in exakter Serienarbeit eine grosse Menge von Code-Zeilen bereitgestellt werden muss, erfordern Middleware-Komponenten für nur wenige Zeilen eines sehr anspruchsvollen Codes einen grossen Aufwand inkl. ausführlicher Reviews und Tests. Bei einem Vergleich repräsentativer Projekte fiel pro Codezeile Middleware fünfmal mehr Aufwand an als beim Anwendungscode.

Die Erfahrung aus dem Betrieb zeigt zudem, wie sich Lösungen betreibbar realisieren lassen. Dedizierte Expertinnen und Experten für Qualitätssicherung, Testing, System- und Release Engineering bringen ihre Erkenntnisse und Erfahrungen darüber ein, wie sich die Qualität über den ganzen Softwarelebenszyklus

## Applied Experience

In den letzten Jahren hat AdNovum ihren Erfahrungsschatz unter anderem in folgenden Beratungsmandaten angewendet:

- Für das Generalsekretariat eines Bundesdepartements erstellte AdNovum eine Roadmap (Planungstool zur Unterstützung der kontinuierlichen Evolution der IT-System- und Anwendungslandschaft) und eine sichere J2EE-Architektur (ab 2003).
- Für einen grossen Finanzdienstleister übernahm AdNovum die technische Leitung und Koordination eines Security-Programms (ab 2004), d.h. die Beratung und Gesamtleitung der IT-Sicherheitsprojekte. Organisation, Prozesse und Technologien im Security-Bereich werden so aufeinander abgestimmt, dass sie sich gemeinsam an der durch die IT-Sicherheitsstrategie vorgegebenen Richtung orientieren.
- Für die internationale Ausbreitung von Authentisierungsmitteln und des Authentisierungs-Backends (2006/07) eines anderen grossen Finanzdienstleisters entwickelt AdNovum zusammen mit dem Mandanten die neuen Businessprozesse. Dabei werden sowohl die bestehenden Prozesse als auch die lokalen Regulationen berücksichtigt. Gestützt auf die neuen Businessprozesse werden die Anforderungen an die lokalen Softwarehersteller für das Verwalten und Benutzen der Authentisierungsmittel definiert.
- Für einen Servicedienstleister und einen grossen Finanzdienstleister evaluierte AdNovum diverse Sicherheitsmittel wie Authentisierungs-Token etc. (2005/2006). Mit dem Ziel einer Single-Sign-on-Lösung für diverse heterogene Komponenten wie Mainframe, Web-Applikationen und Fat Clients wurden zuerst Lösungsvarianten analysiert und bewertet, um danach für die beste Variante in einem mehrstufigen Verfahren die optimalen Anbieter zu wählen.
- Für verschiedene Kunden wurden im Rahmen von Reviews unter anderem die Qualität von Architektur, Code, Deployment und Performance beurteilt und entsprechende Verbesserungsmassnahmen aufgezeigt.

## Dependent by Design

Von Beratung wird in der Regel Unabhängigkeit gefordert.

AdNovum kann für sich in Anspruch nehmen, unabhängig von Produktanbietern zu sein. Damit kann AdNovum in jedem Fall die für den Kunden individuell optimale Lösung vorschlagen, unbeeinflusst von irgendwelchen Produktebindungen.

Die AdNovum-Beratungsleistung ist hingegen bewusst nicht unabhängig von der AdNovum-Umsetzungsleistung. Das Spezifische und Interessante am Angebot der AdNovum liegt eben gerade darin, dass bei Beratungen der immense Fundus an Umsetzungserfahrung genutzt werden kann.

Falls die Erkenntnisse aus der Beratung eine Umsetzung nahelegen, bietet sich dem Kunden zudem die interessante Möglichkeit, AdNovum auch dafür in Anspruch zu nehmen.

## Focused Experience

Der Hauptfokus der Beratungsmandate liegt in den Bereichen, in denen die AdNovum optimal Umsetzungserfahrung einbringen kann. Die Beratungsthemen betreffen oft die Umsetzung selbst, können ihr jedoch auch vorgelagert oder übergeordnet sein.

- Architektur (verteilt, sicher, Service-orientiert, betreibbar usw.)
- Sicherheit, Compliance: Politik, Konzept, Konsequenzen und technische Umsetzung
- Engineering (Organisation/Prozess), Tools/Technik, Technologiemanagement, Umsetzung
- Reviews (Beurteilung und Massnahmen hinsichtlich Qualität von Architektur, Code, Deployment, Engineering-Prozess, Betreibbarkeit)
- Strategie und Umsetzung (Roadmap)
- Software Lifecycle: Information und Kennzahlen (Configuration/Change Management, Application Web usw.)

## Experience from the Source

In der Beratungsbranche werden häufig Hochschulabgänger als Berater eingesetzt, die sich quasi «on the job» Erfahrungen aneignen. Dies steht jedoch mit dem Anbieten von Beratung mit Erfahrung als Qualitätsmerkmal systembedingt im Widerspruch. AdNovum setzt daher im Beratungsbereich explizit Mitarbeiter ein, die über einen eigenen, soliden Erfahrungsfundus verfügen, einen guten Überblick über den Erfahrungsschatz der AdNovum haben und beide aus erster Hand auch am besten anwenden können. Dies impliziert jedoch auch, dass die Berater nicht als separate Gruppe losgelöst von der Umsetzung agieren. Erfahrene Mitarbeiter sind normalerweise in wichtigen Rollen im Rahmen von Umsetzungsprojekten aktiv und übernehmen bei Bedarf gezielt im Rahmen eines Mandats die Rolle eines Beraters.

hinweg halten lässt. Dank dem AdNovum-Team in Ungarn profitieren Kunden mit ähnlichen Kooperationsszenarien von der spezifischen Erfahrung im Bereich Softwareentwicklung über örtliche und kulturelle Grenzen hinweg.

Auf der Basis ihrer Erfahrungen hat die AdNovum in letzter Zeit als Schwerpunkt weiter in die Entwicklung und Pflege dieser Softwareengineering-Kompetenz investiert.

### Tobias Murer

*Tobias Murer hat bis zu diesem Sommer die Entwicklung des Java-Engineering-Bereichs der AdNovum verantwortet. Den promovierten ETH-Informatiker mit zusätzlichem Wirtschaftsabschluss interessiert das Zusammenspiel von technischen, organisatorischen und wirtschaftlichen Aspekten des Software Engineering. Er war in letzter Zeit vor allem in Beratungsmandaten tätig und ist seit Sommer für den Aufbau und die Entwicklung des Beratungsbereichs der AdNovum verantwortlich. Seinen Ausgleich findet er mit sportlichen Aktivitäten in der Natur.*

## Beratungserfahrung

Die bisherigen Beratungsmandate der AdNovum sind meist einer Umsetzung vorgelagert oder begleiten sie (siehe Kasten «Applied Experience»). Sie werden mit Schwerpunkt in den Bereichen Sicherheit, Architektur, Qualität und Strategie in Form von Konzepten, Reviews, Workshops und Schulungen ausgeführt. Nicht überraschend entspricht dies auch genau den Bereichen, in denen die AdNovum mit Umsetzungen tätig ist und entsprechend über vertieftes Wissen und Erfahrung verfügt.

Der umfassende Fundus an Umsetzungserfahrung der AdNovum-Mitarbeiter erweist sich bei der Ausführung solcher Beratungsmandate immer wieder als wichtiger Qualitätsfaktor. Dies lässt sich zum Beispiel anhand der Beurteilung neuer Technologien und Buzzwords illustrieren. Während die IT sich immer wieder neu erfindet, sind viele der IT-Herausforderungen systeminhärent und bleiben relativ konstant. Als Beispiel dafür sei SOA (Service-Oriented Architecture) genannt: Ein Wechsel der Technologie macht die Bewältigung der impliziten Herausforderungen, welche Entwurf, Realisierung, Betrieb und Evolution eines verteilten IT-Systems bieten, nicht a priori einfacher. Dank ihrer Umsetzungserfahrung ist die AdNovum rasch und gut in der Lage, neue Konzepte und Technologien im Vergleich zu etablierten einzuordnen, ihre Stärken und Schwächen zu beurteilen und auf ihrer Basis Lösungen abzuleiten.

Da der Erfolg eines IT-Projekts nicht nur von technischen, sondern auch von strategischen, organisatorischen und rechtlichen Aspekten abhängt, ist der Rückgriff auf Umsetzungserfahrung auch in entscheidenden technologiefremden Fragestellungen von Vorteil. Entsprechender Beratungsbedarf existiert z.B. bei der Evolution einer IT-Service und Anwendungslandschaft entlang einer Strategie/Roadmap oder in der Frage, wie sich Sicherheitsregulatorien und -risiken sinnvoll berücksichtigen lassen, das heisst, welche technischen Massnahmen sich lohnen und welche nicht.

> Die IT erfindet sich laufend neu, viele ihrer Herausforderungen sind jedoch systeminhärent und relativ konstant.

## Sharing Experience

Der Erfahrungsschatz («Experience») und damit das vereinte Know-how der AdNovum

wird entsprechend dem Leitgedanken «Sharing Experience» vermehrt im Rahmen von Beratungsmandaten für die Lösungsfindung genutzt und mit dem Kunden geteilt («shared»). Hochwertige Beratung wird neu als klar positionierte Dienstleistung mit den folgenden Kerneigenschaften angeboten.

- Leitgedanke «Sharing Experience»
- Hochstehende IT-Beratung
- Anbieter: AdNovum Engineering
- Unabhängig von Produkten, aber stark abhängig vom AdNovum-Erfahrungsschatz (siehe Kasten «Dependent by Design» und Abschnitt «Umsetzungserfahrung»)
- Hauptfokus auf Themen, in denen dank Umsetzung Erfahrung anfällt (siehe Kasten «Focused Experience»)
- Beratung durch erfahrene Mitarbeiter (siehe Kasten «Experience from the Source»)
- Intensiver Erfahrungsaustausch zwischen Umsetzung und Beratung (AdNovum-internes «Sharing Experience»)
- Beratungstätigkeit zeichnet sich durch einen starken Praxisbezug und entsprechende Umsetzbarkeit aus

Mit den skizzierten Eigenschaften ihres Ansatzes bietet AdNovum auch im Beratungsbereich eine hochstehende und interessante Dienstleistung an, welche den Kunden Mehrwert bringt.

# Modern Threats – Risiken im E-Business

Michael Müller sprach mit Notitia über den richtigen Umgang mit Risiken im E-Business.

Interview: Manuel Ott

*NOTITIA:* E-Business Security, ein uraltes Thema. Ist dies heute noch aktuell?

Gerade das Thema E-Banking-Authentisierung ist in letzter Zeit wieder hochaktuell. Am häufigsten und daher auch am bekanntesten sind Phishing-Attacken. Bei einer Phishing-Attacke versucht der Angreifer, das Opfer via E-Mail dazu zu bringen, das Passwort und eine oder mehrere Streichlistennummern in einer gefälschten Website einzugeben. Doch auch

andere Angriffsformen wie etwa Man-in-the-Middle-(MITM-) und Malware-Attacken sind auf dem Vormarsch.

Bei einer MITM-Attacke schaltet sich der Angreifer zwischen die beiden Kommunikationspartner, ohne dass diese etwas davon merken. Er kann so die gesendeten Informationen nach Belieben einsehen und manipulieren. Dabei wird häufig auch Malware eingesetzt. Das sind Computerprogramme, die vom Benutzer unentdeckt schädliche Funktionen ausführen.

Wo droht aktuell die grösste Gefahr?

Das ist schwer zu sagen. In den nächsten Jahren wird aus meiner Sicht die Problematik der meist schlecht geschützten Kunden-PCs in den Vordergrund rücken. Die organisierte Kriminalität wird weiter zunehmen und ihre Attacken vermehrt auf einzelne Unternehmen richten. Dabei wird immer raffiniertere Malware entstehen, die zielgerichtet und mit hoher Erfolgswahrscheinlichkeit angreift und mittels der heutigen Abwehrmethoden wie Virenscanner kaum mehr detektiert werden kann.

Auch komplexe Man-in-the-Middle-Attacken werden zunehmend automatisiert und damit sehr schnell erfolgen. Heute noch als relativ sicher eingestufte Methoden wie kurzzeitig gültige Einmalpasswörter (z.B. SecurID) werden bald einmal nicht mehr genügen, weil der Angreifer bzw. die Malware gleichzeitig mit dem Opfer online ist und in dem Moment reagieren kann, in dem das Opfer seine Zugangsdaten resp. Credentials eintippt.

> «Der grösste Nutzen einer Risikoanalyse ist Transparenz.»

Müssen sich die Kunden also Sorgen um ihr Geld machen? Gibt es Sorgfaltspflichten zu beachten?

Grundsätzlich regeln die Vertragsbedingungen inkl. AGB zwischen Kunde und Bank die Verteilung der Sorgfaltspflichten. Dazu wird heute postuliert, dass die Banken die Pflicht haben, den Kunden über allgemeine und internetspezifische Risiken des E-Bankings vor Vertragsabschluss explizit aufzuklären. Doch unabhängig davon, ob der Kunde seine Sorgfaltspflicht verletzt hat oder nicht, musste er sich um sein Geld bislang kaum Sorgen machen. Bis anhin haben sich die Finanzinstitute in den bekannten Fällen kulant gezeigt.

Was ist aktuell der Stand bezüglich Security im Bereich der Kundenauthentisierung?

Nach unserer Beobachtung bewegen sich die Banken immer in «Sicherheitsbändern». Ein Band definiert den Bereich der nach der aktuell vorherrschenden Meinung in der Finanzbranche «genügend» sicheren Mechanismen. Je nach strategischer Ausrichtung positioniert sich eine Bank zum Beispiel als «First Mover» oder als «Late Follower» im aktuellen Sicherheitsband. Bewegt sich eine Bank aus dem Sicherheitsband hinaus nach oben, so müssen die anderen Banken überlegen, ob sie aus Wettbewerbsgründen nachziehen wollen. Bewegen sich viele Banken, so verschiebt sich das Sicherheitsband. Bewegt sich nur eine einzelne Bank weiter, so bedeutet dies für sie nach unserer Erfahrung nicht unbedingt einen Wettbewerbsvorteil. Zieht jedoch eine Bank nicht mit, wenn sich das Sicherheitsband nach oben verschiebt, so kommt sie in den Fokus von Angreifern und sollte nur schon aus Reputationsgründen sehr schnell nachziehen.

Läuft bei den Finanzinstituten aktuell etwas im Bereich Security?

Ein Finanzinstitut kann es sich heute kaum mehr leisten, keine E-Business-Sicherheitsstrategie zu verfolgen. Viele Finanzinstitute überlegen sich aktuell, ob sie angesichts der neuen Bedrohungen wie Online-MITM-Attacken zusätzliche Massnahmen ergreifen sollten.

Welches Vorgehen empfehlen Sie den Banken bei dem Angehen der Probleme/Bedrohungen?

Ich empfehle jeweils die Durchführung einer umfassenden und präzisen Risikoanalyse. Der grösste Nutzen der Risikoanalyse ist die

Transparenz, die auf dem Weg zum Ziel geschaffen wird. Man wird sich der tatsächlichen Risiken bewusst und betrachtet die Lösungsansätze immer unter dem Aspekt der Risikoverminderung.

### Welche Art von Risikoanalyse hat sich bewährt?

In der Vergangenheit setzte man vor allem auf qualitative Analysen. Vor dem Hintergrund internationaler Regulierungen wie Basel II und Sarbanes-Oxley jedoch kommt der quantitativen Risikoanalyse eine immer grössere Bedeutung zu.

Die für die Risikoquantifizierung in der Regel verwendeten Top-down-Ansätze stützen sich häufig auf so genannte Risikoindikatoren, sagen aber nicht viel über die Ursachen aus. Im Gegensatz dazu stehen bei Bottom-up-Verfahren die Zusammenhänge zwischen Ursache und Wirkung von Ereignissen im Zentrum. Wenn es gelingt, die Komplexität von Bottom-up-Analysen zu meistern, sind sie ein wertvolles Hilfsmittel, um Investitionen vor dem Business zu begründen.

Generell fehlen momentan aussagekräftige statistische Zahlen zu Eintretenswahrscheinlichkeiten und Schäden. Es ist jedoch anzunehmen, dass solche Zahlen in Zukunft verfügbar sein werden.

Um das heutige Wissen trotz Mangel an Zahlen optimal nutzen und für die Zukunft verfügbar machen zu können, empfiehlt sich bei der quantitativen Risikoanalyse der Einsatz von Methoden, welche die Kombination statistischer Grundlagen mit Expertenwissen erlauben. Das Expertenwissen dient dabei als Basis für die Modellierung der Kausalzusammenhänge der involvierten Komponenten.

Im Rahmen eines Projekts haben wir hierfür ein vereinfachtes Modell entwickelt, das speziell darauf ausgelegt ist, die Wirksamkeit möglicher Massnahmen miteinander zu vergleichen.

### Kann man denn Aussagen zur Wirksamkeit von Massnahmen machen?

Ja, das kann man, wenn man die Zusammenhänge sichtbar macht. Bei einer Attacke muss ein Angreifer in der Regel verschiedene Schwachstellen gleichzeitig nutzen, um erfolgreich zu sein. Die Bedrohung lässt sich aufzeigen, indem mögliche Angriffsszenarien als so genannte Attack Trees modelliert werden. So können relevante von irrelevanten Bedrohungen unterschieden und die Wirksamkeit von Massnahmen beurteilt werden. Die Massnahmen wirken verschieden auf die Schwachstellen und unter Umständen auch direkt auf den Angreifer, indem sie etwa die Motivation des Angreifers senken.

Eine herkömmliche Offline-Phishing-Attacke zum Beispiel kombiniert die Schwachstelle, dass der Kunde seine Credentials auf einer gefälschten Website eingibt, mit der Schwachstelle, dass sich ein Angreifer mit fremden Credentials überhaupt authentisieren kann. Dazu kommt die Schwachstelle, dass der Angreifer nach erfolgreicher Authentisierung beliebige Transaktionen ausführen kann, sowie unter Umständen weitere applikationsspezifische Schwachstellen.

Um die Wirksamkeit quantifizieren zu können, werden die erwarteten Schäden und die Häufigkeiten der unerwünschten Ereignisse in Expertenworkshops geschätzt und ins Modell integriert.

> «An einer Risikoanalyse müssen Vertreter aus Business, IT, Sicherheit und Recht beteiligt sein.»

### Wer muss auf Kundenseite bei der Durchführung einer Risikoanalyse involviert sein?

Die Risikoanalyse muss unbedingt von einem Team aus Vertretern aller relevanten Bereiche gemacht werden, also Business, IT, Sicherheit, Rechtsdienst und bei Bedarf auch zusätzlichen Leuten, etwa vom Endbenutzer-Support. Nur so können die kritischen Aspekte identifiziert und adäquat gewichtet werden.

Mindestens ebenso wichtig wie die Resultate der Analyse ist dabei der Weg dorthin. Im Verlauf der Workshops ergeben sich oft spannende Diskussionen, etwa wenn die Juristen die Informatiker über die Höhe von Gerichtskosten oder die Bedeutung der allgemeinen Geschäftsbedingungen informieren.

Umgekehrt wird den Juristen zum Beispiel bewusst, dass Sicherheit kein dauerhaftes Gut ist. Heute noch als sicher geltende Technologien können unter Umständen schon bald nicht mehr genügen.

**Michael Müller**

*Michael Müller, diplomierter Vermessungsingenieur ETH, arbeitete nach dem Studium als Managementberater in ganz Europa. Sein vertieftes IT-Sicherheits-Know-how erwarb er als Softwareentwickler in der AdNovum, im Nachdiplomstudium Informatik an der ETH Zürich und vor allem durch die Leitung mehrerer Sicherheitsprojekte bei AdNovum. Seine CISSP-Zertifizierung gibt ihm den nötigen Überblick zum Thema. Neben der Arbeit treibt er Sport und übt fleissig Spanisch, um die Kenntnisse aus seiner letztjährigen Südamerikareise aufzufrischen.*

Sie haben ja eine quantitative Risikoanalyse für eine E-Banking-Authentisierung durchgeführt. Was ist nun die optimale Authentisierungsvariante?

Dies muss für jede Bank im Detail betrachtet werden. Dabei werden in einem ersten Schritt die zu erwartenden Schäden und deren Eintretenswahrscheinlichkeit abgeschätzt. Dabei müssen nebst den direkten Kosten durch Schadenersatzzahlungen unbedingt auch zusätzliche Kosten wie etwa die betrieblichen Mehraufwände bei einem Ausfall der Online-Bank berücksichtigt werden (Helpdesk, Belegverarbeitung usw.).

Dann werden die verschiedenen Lösungsansätze wie Einmalpasswörter, PKI-basierte Verfahren oder Transaktionssignaturen nach Schadensminderungswert kategorisiert. Dieser Wert wird mit qualitativen Kriterien kombiniert und gegen die entstehenden Kosten abgewogen. Bei den qualitativen Kriterien fallen häufig nicht in erster Linie die technischen, sondern die organisatorischen und prozessbezogenen Aspekte ins Gewicht. So erfordert etwa der Einsatz von PKI/Smartcards die Installation von Software auf den Endgeräten. Dies ist vor allem ein Problem des Supports. Die Kosten für den Endbenutzer-Support explodieren, wenn der Kunde auf seinem Rechner Software selber installieren und aktualisieren muss.

Vom Kosten-Nutzen-Verhältnis her gesehen kommt eine eher günstige Lösung wie zum Beispiel mTAN (mit Anzeige der Transaktion auf dem Handy) recht gut weg. Bei PKI-basierten Verfahren, bei denen Smartcards und Leser auf Kosten der Bank ausgebreitet werden müssen, ist das Kosten-Nutzen-Verhältnis dagegen eher schlecht. Die EMV-CAP-Authentisierung auf der Basis einer EC-Karte kombiniert mit Transaktionssignaturen wiederum ist sehr wirksam und ausserdem vergleichsweise günstig, da bereits bestehende Karten und Prozesse genutzt werden können und die Leser mittlerweile für unter 10 Franken pro Stück zu haben sind. Neben den reinen Kosten-Nutzen-Überlegungen müssen auch Aspekte wie Image/Reputation, Standardkonformität und Benutzerkomfort einbezogen werden. So sind zum Beispiel Transaktionssignaturen für Einzelkunden und Firmenkunden unterschiedlich geeignet. Während das Eintippen der Transaktionen für Einzelkunden kein Problem darstellt, werden Firmenkunden mit zuweilen Hunderten von gleichzeitig auszulösenden Transaktionen nicht jede einzelne Zahl in einen Offline-Kartenleser eingeben wollen.

Aufgrund der geschilderten Erfahrungen empfehlen wir unseren Kunden heute vermehrt, verschiedene Authentisierungsmittel anzubieten, die dann je nach Einsatzzweck und Sicherheitsanforderungen der Kunden eingesetzt werden können. Durch den gleichzeitigen Einsatz mehrerer Mittel entstehen allerdings Mehrkosten, die sorgfältig gegen den Nutzen abgewogen werden müssen.

Wie wird die E-Banking-Authentisierung in der Schweiz in fünf Jahren aussehen, wie in der weiteren Zukunft?

In den nächsten fünf Jahren werden sich vermutlich vor allem PKI-basierte Lösungen und Lösungen mit Offline Tokens mit der Möglichkeit zur Transaktionssignierung (z.B. EMV CAP Token) stärker verbreiten. Dabei ist aktuell schwierig abzuschätzen, ob sich Transaktionssignaturen langfristig durchsetzen können und welche Rolle neuere Trends in den Bereichen Trusted-Computing-Plattformen, Zertifikate für Endkunden (Bezug von Zertifikaten am Postschalter), Netzwerk-Security und spezialisierte E-Banking-Hardware spielen werden.

Sicher ist, dass wir in Bezug auf die Sicherheit im E-Business in den kommenden Jahren mit immer komplexeren Bedrohungen konfrontiert sein werden, die neue und flexiblere Lösungsansätze verlangen. Quantitative Risikoanalysen können hier eine grosse Hilfe sein. Sie unterstützen die effiziente Identifizierung von Schwachstellen trotz wachsender Komplexität und bringen einen interdisziplinären Dialog in Gang, der es erlaubt, die Schwachstellen auch richtig zu gewichten. ■

## Transaktionssignaturen

Transaktionssignaturen gelten heute als eine der sichersten Varianten zur Authentisierung von Bankzahlungen.

Der Kunde signiert seine gesamten Transaktionsdaten (Zielkontonummern, Währung, Betrag usw. oder einen sicheren Hash davon) mit einem nur ihm (und unter Umständen der Bank) bekannten Geheimcode. Die Signatur erfolgt auf einem sicheren Gerät, das nicht an den PC angebunden wird, damit es nicht von Schädlingen attackiert werden kann.

Ein Angreifer kann solche mit einer Transaktionssignatur versehenen Daten nicht zu seinen Gunsten nutzen, da die Signatur eindeutig mit den Transaktionsdaten verknüpft ist und jede Veränderung daran festgestellt werden kann.

« Die Bedrohungen im Bereich E-Business werden immer komplexer und verlangen neue, flexiblere Lösungen. »

# Experimentalanalyse in Projektreviews

In technischen Projektreviews gewinnen experimentell-analytische Ansätze als Ergänzung zu Verfahren wie Sourcecode- oder Dokumentationsstudium zunehmend an Bedeutung.

Von Thomas Klemm und Tom Sprenger

Technische Projektreviews werden aufgrund technologischer, organisatorischer oder personeller Umstände oder bei stark wechselnden Anforderungen an ein Projekt initiiert. Dabei verfolgt man folgende Ziele:

- Prävention

  Standortbestimmung und Risikoabschätzung (z.B. bei personellen Wechseln oder verändertem Verwendungszweck des Systems)
- Verifikation

  Sicherstellen, dass Vorgehen und Lieferobjekte den vorgegebenen Standards und Best Practices genügen (Qualitätssicherung)
- Problemanalyse und -behebung

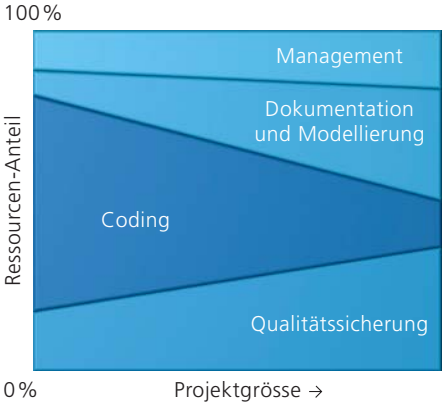
  Analyse und Behebung bekannter Probleme in den Bereichen funktionale Korrektheit, Performance/Skalierbarkeit und Stabilität/Robustheit/Zuverlässigkeit (Betreibbarkeit)

Unabhängig von der Motivation geht es letztlich darum, ein Informationsdefizit zu beheben. Die Informationslücken und die damit verbundene Unsicherheit sollen mittels einer Review identifiziert und durch erarbeitete Fakten gefüllt resp. behoben werden.

## Informationslücken als gängige Praxis

In der Softwareentwicklung werden heute gewisse Informationsdefizite bewusst in Kauf genommen. Anstelle streng formaler Verfahren – die aus Sicht der Qualitätssicherung zu bevorzugen sind – haben sich semiformale Verfahren wie z.B. objektorientierte Ansätze in Kombination mit einem reifen Software-Engineering-Prozess etabliert. Eine bezüglich Komplexität und Aufwand praktikable Lösung, aber auch mit beschränkter Präzision.

Damit daraus dennoch funktionierende Lösungen entstehen, müssen insbesondere in grösseren Softwareprojekten in den Bereichen Dokumentation und Modellierung sowie Qualitätsmanagement und -sicherung verhältnismässig mehr Ressourcen eingesetzt werden (siehe Grafik). In der Realität wird dies jedoch oft nicht oder ungenügend berücksichtigt: Grössere Softwareprojekte sind häufig unterdokumentiert und aus QS-Sicht nur lückenhaft verifiziert.




Erschwerend kommt oft ein Verlust von Information an organisatorischen, technologischen und zeitlichen Grenzen hinzu. Dies tritt häufig auf bei umfangreichen Projekten in grossen Organisationen mit vielen verschiedenen involvierten Parteien, die mit ihrem Spezialwissen für abgegrenzte Bereiche zuständig sind (stark partitionierte Wissensverteilung), und verstärkt bei langfristigen Projekten, wenn die involvierten Parteien über die Zeit wechseln (vgl. Artikel «Information im Griff» von Tobias Murer in Notitia Nr. 6/2004).

Viele der Informationen über ein Projekt sind zudem nur persönlich gefiltert und interpretiert erhältlich: Je länger eine Person in ein Projekt involviert ist, desto schwieriger ist es für sie, eine neutrale Sicht zu wahren. Feststellungen und Aussagen von Personen aus einem Projekt sind typischerweise mit der Projektgeschichte sowie der Rolle und den damit verbundenen Interessen der aussagenden Person eingefärbt.

## Neutrale Position entscheidend

Für die Qualität einer Review ist es entscheidend, dass sie aus möglichst neutraler Position durchgeführt wird.

Zwar könnte auch eine ins Projekt involvierte Person eine Review durchführen, doch kann eine aussenstehende Instanz die Rolle des Reviewers oft besser wahrnehmen, da sie eine neutralere und objektivere Sicht auf das Projekt hat und sich idealerweise erlaubt, auch etablierte Sachverhalte in Frage zu stellen – unbelastet und unabhängig von Rolle, Rang und Vorgeschichte.

## Ganzheitliche Sicht gefragt

Oft werden für eine Review Spezialisten der diversen beteiligten Komponenten einberufen. Jeder analysiert dann in erster Linie seinen Aspekt. Die Probleme zeigen sich jedoch oft erst im Zusammenspiel der Komponenten. Zudem bauen sich heutige Softwarelösungen typischerweise aus mehreren komplexeren Technologie-Layers auf und entstehen verteilt als Resultat einer Kooperation verschiedener

## Technische Projektreviews

Eine technische Projektreview beinhaltet die Analyse und Beurteilung eines Softwareprojekts bezüglich:

- Organisation und Prozessen
- Tools, Technik und Methodik
- Dokumentation
- Architektur, Design, Sourcecode-Qualität
- Verifikations- und Validierungsplan
- Releasemanagement
- Fehlerreporting und Korrekturmassnahmen

Je nach Ausrichtung der Review wird nur ein Teil der aufgelisteten Bereiche abgedeckt. Zunehmend ist eine Überprüfung von Qualitätsattributen auf der Basis der laufenden Software ebenfalls Bestandteil der Review:

- funktionale Korrektheit
- Performance, Skalierbarkeit
- Stabilität, Robustheit, Zuverlässigkeit

Die benötigten Informationen werden durch Interviews, Workshops, Dokument- und Sourcecodestudium sowie das Ausführen und Auswerten von Softwaretests gewonnen. Als Resultat wird typischerweise ein Bericht geliefert, der die einzelnen Befunde auflistet, klassifiziert und bewertet und einen Massnahmenkatalog enthält, wo notwendig mit konkreten Verbesserungsvorschlägen.

Organisationseinheiten. Die die Review ausführenden Instanzen müssen also ein entsprechend ganzheitliches Wissen nachweisen und das Projekt in seiner ganzen Breite und der geforderten Tiefe erfassen und verstehen können. Andernfalls ist das Risiko gross, dass das Projekt in einem lokalen Qualitätsoptimum stecken bleibt.

Die Eigenschaften und das Verhalten solcher komplexen, verteilten Systeme sind mittels formaler Analysemethoden wie Interviews, Workshops, Dokumentations- und Sourcecodestudium nur noch sehr schwer zu bestimmen. Beispielsweise ist eine sinnvolle Systemarchitektur zwar eine notwendige, aber keineswegs hinreichende Vorraussetzung für ein stabiles, performantes Systemverhalten. Informationen aus der Analyse des laufenden Systems werden immer wichtiger. Zu deren Gewinnung benötigt man experimentellanalytische Methoden, d.h. Vorgehen ähnlich der experimentellen Physik mit Experimenten und Tests.

*Thomas Klemm und Tom Sprenger bauen die hauseigenen Test- und Analyseinstrumente der QA-Infrastruktur.*

## Integriertes Messsystem

Die AdNovum hat schon früh unter dem Label des Quality Assurance Engineering (QAE) und im Wesentlichen aus praktischer Notwendigkeit begonnen, entsprechendes Know-how, Vorgehensweisen und ein effektives Tooling im Bereich der experimentell-analytischen Methoden aufzubauen.

Bei experimentell-analytischen Methoden wird der Code eines Projekts zwecks Analyse ausgeführt und tatsächlich durchlaufen. Dies kann im Rahmen von Tests (z.B. Unit-, Integrations-, Last- oder Stresstests) in einem Laborumfeld oder auch als Teil des produktiven Betriebs geschehen. Wichtig ist, dass während der Codeausführung die entscheidenden Messgrössen als Ausgangspunkt für die nachfolgende Analyse mitprotokolliert werden.

Während der Entwicklung stehen in der Regel leistungsfähige Analysetools zur Verfügung. In der Produktion dagegen sind solche Tools oft aus Gründen der Sicherheit oder Performance nicht zugelassen. Während isolierte Aspekte und das einfache Zusammenspiel von Komponenten eines verteilten Systems in dedizierten Testumgebungen getestet werden können, machen sich gewisse Effekte jedoch erst unter produktiven Bedingungen bemerkbar. Gefragt sind somit Werkzeuge, die in der Produktion legal und performanceneutral eingesetzt werden können. Damit qualitätsrelevante Resultate möglichst früh berücksichtigt werden können, sollten diese Werkzeuge zudem bereits in der Entwicklungs- und der Testumgebung eingesetzt werden.

Eine weitere Herausforderung besteht in der weiter oben postulierten ganzheitlichen Betrachtung des Systems: Wie sollen Ereignisse, die ihre Spur in verschiedenen Messgrössen und über mehrere Komponenten eines verteilten Systems hinweg hinterlassen haben, korreliert werden? Die grosse Mehrheit der auf dem Markt verfügbaren Werkzeuge beschränkt sich darauf, Messwerte für einen lokalen Bereich (z.B. einen Service) zu messen. Die Korrelation erfolgt über die Zeitmarke, die zu jedem Messpunkt notiert wurde – bei einem grösseren verteilten System und vielen Messpunkten ein denkbar fragiler Ansatz.

Derartige Probleme haben sich schon früh beim Entwickeln von verteilten CORBA-Systemen gezeigt. Man hat deshalb begonnen, ein Messsystem nach einem Embedded-Ansatz zu implementieren, wie man dies auch aus dem Bereich der Mikroprozessoren kennt (Analyse-Circuits on Chip). Dabei wird das Messsystem bei der Entwicklung einer Lösung als integraler Bestandteil in die Software eingebettet. Dieser Ansatz hat drei entscheidende Vorteile:

1. Zur Messwerterfassung werden keine zusätzlichen, externen Tools benötigt.
2. Das Messsystem ist Teil der Software und somit auch im Betrieb verfügbar.
3. Weil das Messsystem Teil der Software ist, können applikatorische Kontextinformationen berücksichtigt bzw. mitgemessen werden.

Da AdNovum im Hause eigene Middleware (CORBA, J2EE) entwickelt, bot sich die einmalige Gelegenheit, eine Lösung in dieser Infrastrukturkomponente selber einzubauen. So profitieren heute Projekte direkt davon, ohne dafür einen übermässigen Aufwand betreiben zu müssen. Damit ist die konsistente Anwendung der Mechanismen über alle Projekte und Komponenten hinweg gewährleistet.

Der implementierte Ansatz ist bestechend einfach: Jedem Aufruf einer Remote-Service-Funktion wird eine eindeutigen Transfer-ID beigefügt, die bei einem Folgeaufruf erweitert wird. Die Transfer-ID wird zusammen mit Laufzeitinformationen wie Antwortzeiten oder Memory-Verbrauch in das Logfile der jeweils betroffenen Komponenten geschrieben. Damit lässt sich ein Aufruf über mehrere Komponenten hinweg verfolgen. Ausserdem erhält man so detaillierte Angaben darüber, wie viel Zeit wo verbraucht wurde.

Was sich im Einzelfall als nützlich erweist, lässt sich auch zu einer Statistik mehrerer Auf-

> Die Analysetools für die Produktion sollten bereits in der Entwicklungs- und Testumgebung eingesetzt werden.

rufe aufbereiten. Diese erlaubt Aussagen über das zeitliche Verhalten des Gesamtsystems. Bei Performanceproblemen kann damit in der Regel die betroffene Komponente bis hin zum Methodenaufruf lokalisiert werden. Aber auch bei Stabilitätsproblemen ist es in der Regel äusserst hilfreich, wenn man Auskunft darüber erhält, was in den letzten Minuten vor einem Crash auf dem betroffenen System passiert ist.

Dank einer hochoptimierten Implementation ist der zeitliche Mehraufwand für das Schreiben der Logeinträge selbst in der Produktion absolut vertretbar. Somit hat man ein leistungsfähiges Mittel zur Hand, um weit verteilte und ansonsten unzugängliche Information sichtbar zu machen.

## Anwendung Performanceanalyse

Die Vorteile eines integrierten Messsystems lassen sich anschaulich am Beispiel einer grossen verteilten J2EE-Applikation zeigen:

Für den Zugriff der Applikation auf die Datenbank entwickelte AdNovum einen Datenbankserver auf dem Mainframe, der für jede mögliche Abfrage eine Methode zur Verfügung stellt. Im Rahmen der Performanceoptimierung ging es darum, die hohen Antwortzeiten mit den ausgeführten Datenbankabfragen in Verbindung zu bringen.

Mit dem bei der Entwicklung des Systems integrierten Messsystem liessen sich über das verteilte System sehr rasch jene Benutzeraktionen (EJB-Calls) identifizieren, welche auf der Datenbank Abfragen mit langen Antwortzeiten auslösten. Dies erlaubte bereits eine erste Priorisierung des Datenbank-Tunings. Da die Transfer-ID sowohl vom EJB-Tier als auch auf dem Datenbankserver aufgezeichnet wird, sind zu jedem EJB-Call allein aus den Logfiles alle zugehörigen Abfragen auf den Datenbankserver ersichtlich: Unnötig mehrfach ausgeführte Abfragen konnten damit beispielsweise sehr einfach detektiert und eliminiert werden. Redundante Abfragen könnten theoretisch auch mittels reiner Codeanalyse eruiert werden, dies ist bei einem so umfangreichen Projekt jedoch aus Zeitgründen nicht praktikabel. Zusätzlich erlaubte das Vorgehen die Verwendung von Logfiles eines Applikationstests, der in der Regel einen grösseren Teil der Funktionen abdeckt als ein isolierter Test.

> Ein Messsystem als Teil der Software kann den applikatorischen Kontext berücksichtigen und ist im Betrieb verfügbar.

## Fazit

Technische Projektreviews haben aufgrund der Komplexität, der technologischen Heterogenität und des organisatorischen und personellen Setup bei heutigen Projekten an Bedeutung gewonnen. Trotz aller Anstrengungen in Richtung standardisierte Prozesse und formaleren Methoden des SW-Engineerings lassen sich die Eigenschaften eines komplexen, verteilten Systems jedoch rein auf dem Papier nicht mehr abschliessend bestimmen. Technische Projektreviews erfordern deshalb – neben einer ganzheitlichen, neutralen Betrachtungsweise – zunehmend experimentell-analytische Methoden als Ergänzung zu den statisch informationsgewinnenden Verfahren wie beispielsweise Sourcecode- oder Dokumentationsstudium. Die praktische Erfahrung zeigt, dass es heute aus technischer wie wirtschaftlicher Sicht sinnvoll ist, in komplexere Software bei deren Entwicklung ein Analysesubsystem einzubetten. Dieses erlaubt die Erfassung und Analyse von Informationen mit denselben Mechanismen vom Beginn der Entwicklung bis in die produktive Umgebung. Diese Kontinuität erweist sich als lohnender Know-how- und Investitionsschutz über den ganzen Lifecycle einer Software hinweg.


### Thomas Klemm

*Thomas Klemm, Mathematiker mit Nachdiplom Informatik ETH Zürich, sammelte bei AdNovum seit 1998 Erfahrung mit CORBA Middleware. Er entwickelte einen Datenbank-Server auf einem Mainframe mit und treibt aktuell den Auf- und Ausbau der AdNovum-eigenen QA-Infrastruktur voran. Zur Abwechslung kurvt er gerne auf einem oder zwei Rädern durch die Gegend.*

### Tom Sprenger

*Tom Sprenger, Informatikingenieur, befasste sich im Doktorat an der ETH Zürich mit Informationsvisualisierung. 2002–2004 leitete er das AdNovum Office in San Mateo (USA). Zurück in der Schweiz, ist er für den strategischen Bereich Quality Assurance Engineering (QAE) der AdNovum verantwortlich. In der Freizeit stürzt er sich gerne auf dem Bike zu Tal.*

# Recht und IT im Zusammenspiel

Rechtliche Aspekte gewinnen in der IT zunehmend an Bedeutung. Die Forschungsstelle für Informationsrecht an der Universität St. Gallen (FIR-HSG) geht diese an und arbeitet dabei auch mit der AdNovum zusammen.

Von Prof. Urs Gasser, Geschäftsführer FIR-HSG

Welche Rolle spielen künftig digitale Beweise in Gerichtsfällen? Welche datenschutzrechtlichen Vorgaben müssen bei der elektronischen Archivierung berücksichtigt werden? Wie lassen sich Risiken an der Schnittstelle von IT und Recht etwa im Bereich E-Banking messen? Wieso verhalten sich Menschen online anders als offline? – Mit solchen und ähnlichen Fragen befasst sich die Forschungsstelle für Informationsrecht an der Universität St. Gallen (FIR-HSG).

Die Forschungs-, Lehr- und Beratungstätigkeit des FIR-Teams weist viele Schnittstellen mit den Tätigkeitsbereichen der AdNovum auf. Entsprechend hat sich zwischen der AdNovum und der FIR ein permanenter Austausch etabliert, in welchem aktuelles Theorie- und Praxiswissen aus den jeweils komplementären Bereichen IT, Management und Recht transferiert wird. Im Rahmen dieses Erfahrungsaustausches ist unlängst auch ein ganzseitiger NZZ-Artikel entstanden, in welchem Michael Müller (AdNovum), Daniel Häusermann und Urs Gasser (beide HSG) die technischen und rechtlichen Fragen rund um den E-Mail-Gebrauch im Unternehmen beleuchten und mögliche integrale Lösungsansätze skizzieren. Namentlich die Aufbewahrung von E-Mails ist eine grosse Herausforderung insbesondere für schweizerische Konzerne, die international tätig sind und sich mit unterschiedlichen Rechtsordnungen mit divergierenden Aufbewahrungsvorschriften konfrontiert sehen. Der amerikanische Sarbanes-Oxley Act ist in diesem Kontext für viele zum Reizwort geworden.

Im NZZ-Artikel zu rechtlichen und technischen Fragen der E-Mail-Nutzung zeigt sich aber nur die Spitze des Eisbergs. AdNovum und die FIR-HSG arbeiten derzeit intensiv an einem Projekt, welches die vielfältigen Risiken analysiert und bewertet, die mit der Einführung neuer elektronischer Geschäftsprozesse in Unternehmen unter Einhaltung gesetzlicher Vorschriften verbunden sind. Die systematische Erhebung und Bewertung dieser Risiken erfordert sehr viel Know-how aus den Bereichen IT, Recht und Organisationswesen. AdNovum und die FIR arbeiten aber nicht nur an einer anwendungsorientierten und integralen Methodik zur Risikoanalyse, sondern schlagen auch geeignete Massnahmen vor, die Risiken an der Schnittstelle von IT und Recht im Sinne des Kunden zu vermindern. Besonderes Augenmerk kommt derzeit dem Bereich Digital Records and Information Management zu.

Im Unternehmensalltag spielt die IT bekanntlich eine immer wichtigere Rolle, und dies zunehmend unabhängig von der jeweiligen Branche, in der sich ein Unternehmen bewegt. Die steigende Komplexität von IT-Systemen ist dabei nicht nur durch Marktbedürfnisse und technischen Fortschritt getrieben, sondern basiert in jüngerer Zeit auch (und gerade) auf erhöhten rechtlichen Anforderungen. Das Zusammenspiel dieser beiden Komponenten ist bisher – auch von Beratern – allerdings noch nicht «ganzheitlich» verstanden worden. AdNovum und die Forschungsstelle für Informationsrecht an der HSG machen hier einen wichtigen Schritt vorwärts, zugunsten der Kunden.

> FIR-HSG und AdNovum: Risikomanagement an der Schnittstelle von IT und Recht.

### FIR-HSG

*Die FIR-HSG wurde im Jahre 2000 gegründet und steht heute unter der Leitung von Urs Gasser, welcher nach mehreren Jahren in den USA nach St. Gallen zurückgekehrt ist und dort eine Professur für Informationsrecht innehat. Die FIR setzt sich zum Ziel, die vielfältigen Fragen an der Schnittstelle von Informations- und Kommunikationstechnologie, Ökonomie, Gesellschaft und Recht aus theoretischer und praktischer Sicht zu erforschen und zu bearbeiten.*
*In enger Zusammenarbeit mit ausländischen Partnern, insbesondere mit dem Berkman Center for Internet & Society an der Harvard Law School, beschäftigen sich Urs Gasser und sein Team derzeit mit einer Reihe von interessanten Problemen im Zusammenhang mit digitalem Urheberrecht (z.B. Haftung von Softwareentwicklern bei Peer-to-Peer-Anwendungen), Online Privacy, digitaler Identität oder elektronischem Beweisrecht. Auf der Agenda stehen aber auch breitere Fragestellungen wie etwa die Regulierung von virtuellen Welten (z.B. SecondLife), die Rolle und Verantwortung von Suchmaschinen-Anbietern oder die Frage der Interoperabilität von Produkten und Services im Internet.*
*www.fir.unisg.ch*


### Impressum

**Herausgeber:**
AdNovum Informatik AG
Corporate Marketing
Röntgenstrasse 22
CH-8005 Zürich
Telefon 044 272 61 11
Telefax 044 272 63 12
E-Mail info@adnovum.ch
www.adnovum.ch
**Verantwortlich und Redaktion:**
Manuel Ott
**Gestaltung und Realisation:**
Rüegg Werbung, Zürich
**Fotografie:**
Gerry Nitsch, Zürich