

NOTITIA

ADNOVUM

BEMERKENSWERTES VON UND ÜBER ADNOVUM

Window of Opportunity

Effizienzsteigerung in der Software-Entwicklung als Chance

Application-Management

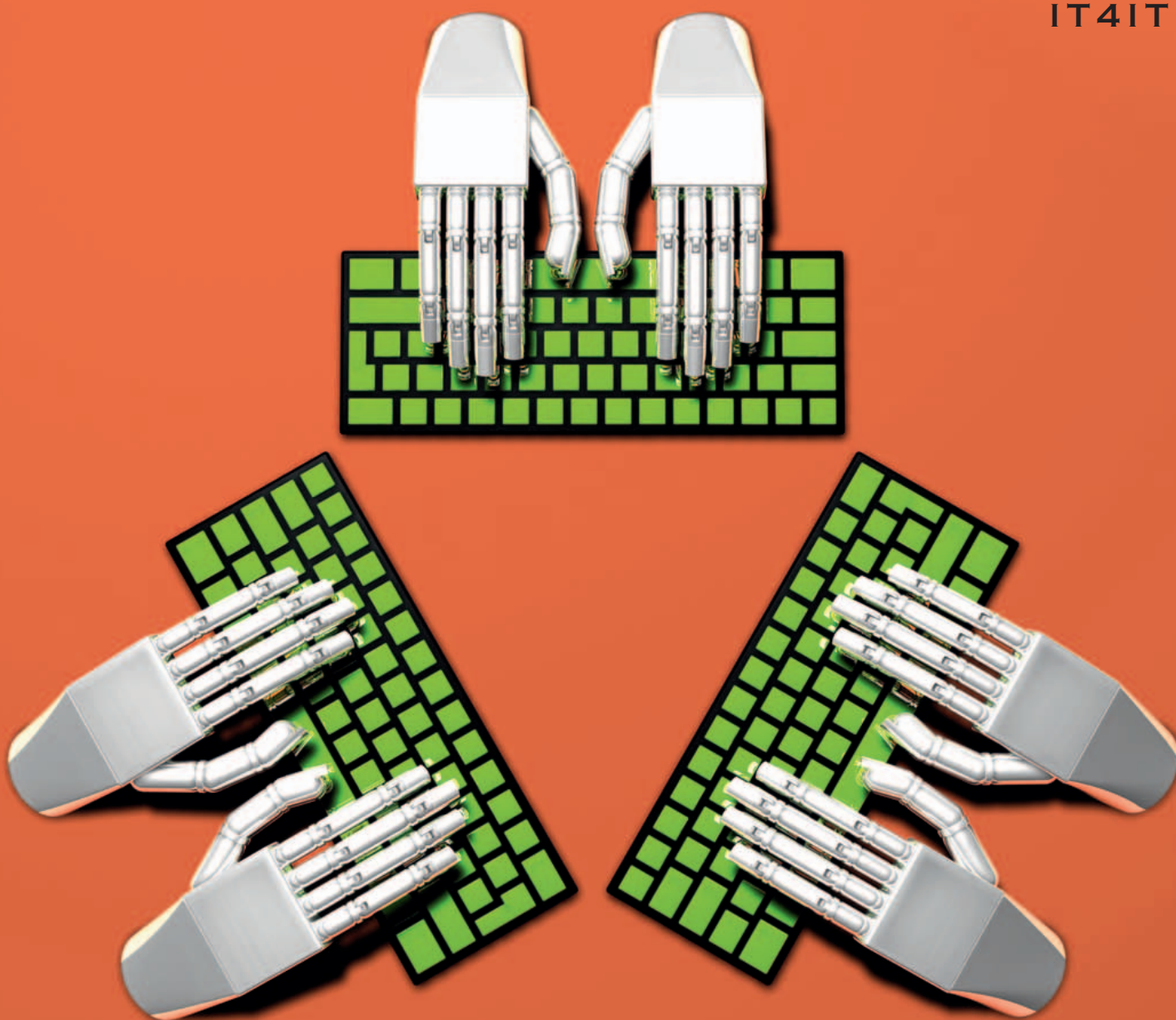
Kundennähe, Flexibilität und individueller Dienstleistungsmix

Sichere Transaktionen

Neue Massnahmen für neue Bedrohungen

FRÜHLING 2009, NR. 16

IT4IT





Liebe Leserin, lieber Leser

Zuverlässig funktionierende Applikationen, die die Geschäftsprozesse proaktiv unterstützen, sind heute mehr denn je ein kritischer Erfolgsfaktor. Sie müssen sich mit dem dynamischen Umfeld stetig bewegen und mit dem Geschäftsgang skalieren. Die Herausforderungen der Applikationsbereitstellung lassen sich ganz verschieden angehen. In der vorliegenden Notitia zeigen wir drei Ansätze. Man kann die Applikationen selbst entwickeln und kontinuierlich in effizienzsteigernde Massnahmen investieren. Wie diese aussehen

Window of Opportunity

GERADE IN WIRTSCHAFTLICH SCHWIERIGEN ZEITEN LOHNT ES SICH, IN DIE ZUKUNFT ZU INVESTIEREN UND DIE EIGENE IT-ORGANISATION MIT GEZIELTEN MASSNAHMEN FÜR DEN VERSCHÄRFTEN WETTBEWERB FIT ZU MACHEN.

VON BETTINA POLASEK UND TOM SPRENGER

Die globale Finanzkrise hat sich auf weitere Bereiche ausgedehnt. Ihre Effekte machen sich zyklusbedingt in den verschiedenen Branchen unterschiedlich stark bemerkbar. Unternehmen sind in jedem Fall gut beraten, Massnahmen zu ergreifen, um den Abschwung möglichst aufzufangen bzw. dessen Folgen abzufedern. Wie sollen IT-Organisationen und -Abteilungen in der gegenwärtigen Situation agieren? Wie können sie den aktuellen wirtschaftlichen Umschwung als Chance nutzen?

Neben dem naheliegenden – eindimensionalen – Anziehen der Sparschraube bietet die IT kreativere Handlungsoptionen. Anstatt mit der Reduktion von IT-Budgets eine für alle Parteien unter Umständen sehr unbefriedigende Situation zu schaffen, kann man rasch handeln und mit breit abgestützten Programmen die operative Flexibilität erhöhen, die Fixkosten senken und insbesondere die Effizienz steigern, auch unter Einbezug von Sourcing-

Strategien (vgl. dazu das Interview in dieser Notitia). Damit können grössere Vorhaben auch in Zeiten knapper Budgets termingerecht und in der geforderten Qualität realisiert werden. Frühzeitig ausgelöst, bringen Effizienzsteigerungsprogramme einen nachhaltigen Nutzen und sogar einen Wettbewerbsvorteil – auch in der Zeit nach der Krise.

WIR HABEN EIN EFFIZIENZSTEIGERUNGSPROGRAMM INS LEBEN GERUFEN, DAS PARALLEL ZUM TAGESGESCHÄFT MITLÄUFT.

Aus eigener Erfahrung

IT und im Besonderen Software-Engineering ist unser Kerngeschäft. AdNovum hat schon nach dem Platzen der Dotcom-Blase effizienzsteigernde Massnahmen eingeleitet. Solche Schritte wurden damals unumgänglich, um weiterhin wettbewerbsfähig zu blei-

ben. Motiviert durch diese initiale Situation haben wir ein Effizienzsteigerungsprogramm ins Leben gerufen, das parallel zum Tagesgeschäft mitläuft. Damit überprüfen wir auch heute kontinuierlich die definierten Massnahmen auf ihre Wirksamkeit und passen sie bei Bedarf an, erweitern oder verwerfen sie.

Unser Know-how und unsere Erfahrung mit den erforderlichen Massnahmen und den Schlüsselfaktoren ihrer Umsetzung teilen wir im Rahmen unseres Consultingangebots im Sinne von IT4IT mit unseren Kunden und Partnern.

Theorie

Im Sinne eines Leitbilds kann Effizienzsteigerung mit Industrialisierung in Zusammenhang gebracht werden. Die IT-Branche bezeichnet sich selber gerne als Industrie. Bei genauerer Betrachtung wird aber deutlich, dass sich der Grad der Industrialisierung bei

der Herstellung von Softwarelösungen in den meisten Fällen auf bescheidenem Level bewegt. Hier schlummert ein entscheidendes unausgeschöpftes Potential.

Industrialisierung heisst unter anderem, auf definierten und gemanagten Prozessen aufzubauen und jederzeit strukturierte Infor-

können und was bei ihrer Umsetzung zusätzlich zu beachten ist, erfahren Sie im einleitenden Artikel von Bettina Polasek und Tom Sprenger.

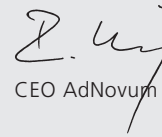
Eine Applikation in Eigenregie zu entwickeln, zu integrieren, zu pflegen und weiterzuentwickeln ist jedoch nicht in jedem Fall die ideale Lösung. Ein Ansatz ist es, die Applikation für solche Leistungen einem spezialisierten Partner anzuvertrauen. Im Interview berichten Nina Laschet und Stephen Jones über das Application-Management der AdNovum.

Effizienz und Effektivität sind nicht nur bei der Entwicklung und Bereitstellung von Fachapplikationen gefragt, sondern ebenso bei Sicherheitssystemen. Denn auch die Gegenseite agiert zunehmend organisierter und professioneller. Attacken auf Webapplikationen werden immer raffinierter und können auf ein Arsenal vorgefertigter Bauteile zurückgreifen. Manuel Hilty beleuchtet in seinem Artikel die Welt der klassischen und der neuen Angriffsformen und stellt Gegenmassnahmen vor, im Besonderen Anomalieerkennung und

Transaktionssignaturen. Auf der Hefrückseite zeigt unsere Partnerin T-Systems die Vorteile ihrer ASP-Banking-Solution für kleine und mittlere Banken auf.

Ich wünsche Ihnen bei der Lektüre viel Vergnügen!

Ruedi Wipf



CEO AdNovum Informatik AG

mationen über den aktuellen Zustand der Fertigung zugreifbar zu haben (Stichwort CMMI-Levels). Vergleichbar mit den Testreihen und den Montagestrassen der Automobilindustrie sollen jede Einzelkomponente und jeder Schritt von der Entstehung bis hin zum Endprodukt mit Messpunkten für Qualität und Fortschritt versehen sein. Eine solche Umgebung erlaubt es, laufend ein aktuelles Bild der Situation in den Projekten zu haben, und hilft beim Controlling derselben. Mit dieser Basis wechselt man in ein kontinuierliches Modell, in dem man jederzeit handlungsbereit ist und Abweichungen vom Soll sofort erkennen und darauf reagieren kann. So können bereits in frühen Stadien Probleme erkannt und adressiert und damit Leerläufe, Verzögerungen, Ressourcenengpässe und Mehrkosten minimiert werden.

Pfeiler der Industrialisierung

Die Industrialisierung des Software-Engineerings beruht auf fünf tragenden Säulen.

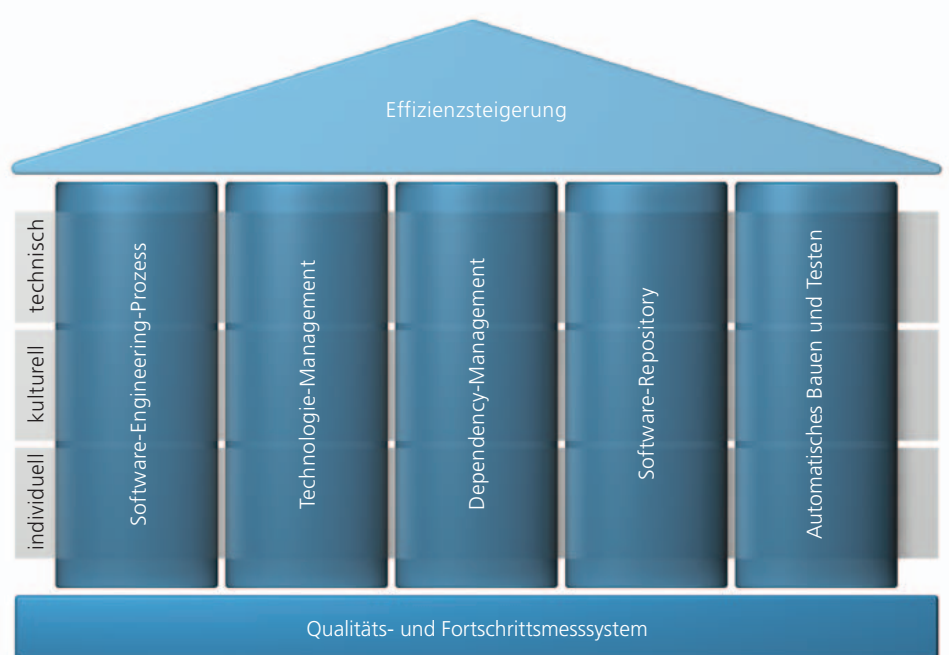
Erstens gilt es, einen wohldefinierten Entwicklungsprozess inkl. Configuration- und Change-Management zu etablieren, der insbesondere auch in der Praxis gelebt werden muss.

Dann ein firmenweites und konsequentes Technologie-Management auf strategischer, taktischer und operativer Stufe, dieses ist ein Schlüsselfaktor zur Vermeidung unnötiger und unerwünschter Aufwände (z.B. im Know-how-Management) und damit zur Effizienzsteigerung im Gesamtkontext.

Weiter braucht es ein starkes Dependency-Management, das das Beherrschen von Abhängigkeiten in Softwareprojekten ermöglicht. Ein Faktor, dem insbesondere in der heutigen Welt von SOA und anderen modularen Architekturen und global verteilter Entwicklung zentrale Bedeutung zukommt. Mit dem Wissen über Abhängigkeiten von Softwarekomponenten kann das Technologie-Management operativ verankert sowie schnell auf das Verwenden problematischer Komponenten reagiert werden – z.B. solcher mit einem bekannten Bug oder Security-Flaw.

Viertens sind vollversionierte Software-Repositories zu nennen. Sie bilden die Basis für das Dependency-Management. Sämtliche Software und deren Komponenten werden versioniert abgelegt und auf diese Art von Drittprojekten referenziert. Werden zusätzlich auch die Werkzeuge versioniert abgelegt, können damit neue Softwarekomponenten im Sinne des industriellen Leitbilds zuverlässig reproduzierbar gebaut werden.

Damit kommen wir zum fünften Element. Es ist die Anforderung, dass Softwareprojekte nach einer initialen Konfiguration ohne



Grundpfeiler der IT-Industrialisierung.

weitere menschliche Interaktion automatisiert durchgebaut und getestet werden können. Dies erhöht zum einen wiederum den Grad der zuverlässigen Reproduzierbarkeit, ist andererseits aber auch Grundvoraussetzung für das Etablieren eines automatischen Qualitätsmesssystems, z.B. eines NightlyBuilds. Dieses liefert die regelmässigen Messpunkte aus dem Projekt, wie Kompilierbarkeit, Technologie- und Sourcecode-Metriken, Testabdeckung etc., die die gewünschte strukturierte Aussage über Projektfortschritt und -qualität ergeben.

teil, das Bestreben zur Effizienzsteigerung muss inhärent tool- und produktunabhängig positioniert sein.

Umsetzung: Kultur als Herausforderung

Die Umsetzung der effizienzsteigernden Massnahmen ist ein zentraler und vielschichtiger Punkt. Sie sollte sorgfältig geplant und den jeweiligen Bedürfnissen der Firma und deren Mitarbeiter angepasst sein. Solche Eingriffe sind nicht nur technisch eine Herausforderung, sondern auch aus kultureller und

Betroffenen klar und nach kurzer Zeit auch positiv spürbar sein, um die gewünschte Akzeptanz und Nachhaltigkeit zu erreichen. Die Hürden, welche für die erfolgreiche Umsetzung einer Massnahme bei einzelnen Beteiligten oder auch bei der gesamten Firmenkultur genommen werden müssen, sind nicht zu unterschätzen.

Die Umsetzung sollte man entlang eines mehrstufigen Plans angehen. Als Erstes ist ein Assessment der aktuellen Situation angesagt. Dieses adressiert auch Fragen zur Standortbestimmung und unterstützt grundsätzliche Entscheidungen, z.B. welche Projekte intern und welche extern durchgeführt werden sollen.

Als zweite Stufe kann eine Potentialanalyse folgen. Darin sollte festgehalten werden, wo die bestehenden Stärken, aber auch Schwächen liegen (SWOT-Analyse). Dies dient dann als weitere Grundlage, um die eigentlichen Massnahmen zu definieren. Die beschlossenen Massnahmen sollten anschliessend priorisiert werden. Flankierend dazu ist auch zu definieren, wie ihre Umsetzung im Sinne eines Controllings überprüft werden kann.

Die Massnahmen werden vorzugsweise zusammengefasst in einem Effizienzsteige-

EIN AUTOMATISCHES QUALITÄTSMESSSYSTEM ERMÖGLICHT STRUKTURIERTE AUSSAGEN ÜBER DEN PROJEKTFORTSCHRITT.

Damit sind auch die Tools angesprochen, mit denen sich die Effizienzbestrebungen unterstützen lassen. Insbesondere ein Thema ist hier die medienbruchfreie Weitergabe von Informationen über die Phasen hinweg – Spezifikation, Implementation, Testing, Betrieb und Wartung. Ein verbreiteter Trugschluss ist jedoch, dass allein mit der Einführung eines Tools die Probleme gelöst werden. Im Gegen-

individueller Sicht. Oft werden effizienzsteigernde Massnahmen von den Betroffenen a priori negativ aufgenommen. Es ist deshalb wichtig, dass das Management geschlossen hinter den Massnahmen steht und die Mitarbeiter bei der Definition und der Umsetzung frühzeitig integriert und auch auf Ängste und Unsicherheiten eingeht. Die Vorteile und Ziele der definierten Regelungen müssen für die

Tom Sprenger

Dr. Tom Sprenger, dipl. Informatik-Ingenieur ETH, ist seit 2001 bei der AdNovum im Einsatz. 2002–2004 leitete er die AdNovum Niederlassung in San Mateo (USA). Seit seiner Rückkehr in die Schweiz ist er für den Bereich Quality Assurance Engineering (QAE) verantwortlich und befasst sich dabei unter anderem mit der Einführung von Massnahmen zur Steigerung der Wirtschaftlichkeit in der Software-Entwicklung und der Vorbereitung von Projekten für die Offshore-Produktion. Seit 2007 ist er CIO und Geschäftsleitungsmitglied der AdNovum Informatik AG. In der Freizeit stürzt er sich gerne in Vollmontur auf seinem Mountain-Bike talwärts.



rungsprogramm, analog einem Security-Programm, umgesetzt. Ein solches Programm soll klare und einfache Schritte enthalten,

Akzeptanz dafür müssen zuerst wachsen und sich im Alltag etablieren. Die Umsetzung von effizienzsteigernden Massnahmen erstreckt

in Angriff zu nehmen. Der Blick ist dabei vom Endprodukt auf den eigentlichen Prozess zu lenken: Dieser ist inklusive der nötigen Einrastpunkte für Zulieferer zu optimieren und mit messbaren Kontrollpunkten auszustatten. Die Neuerungen müssen bewusst motivierend begleitet und kontrolliert umgesetzt werden. So besitzt jede IT-Organisation eine reelle Chance, auch in einer wirtschaftlich ungünstigen Situation kompetitiv zu agieren. ■

DER GANZE PROZESS DER UMSETZUNG IST KONTINUIERLICH ALS AKTIVES VEHIKEL VORANZUTREIBEN.

wie man an das gewünschte Ziel kommt. Es verfolgt einen umfassenden Ansatz, indem es die zentralen Aspekte abdeckt und alle Strukturen durchdringt. So müssen beispielsweise organisatorische Faktoren adressiert werden. Neue Rollen und Verantwortlichkeiten sind zu skizzieren und festzulegen, neue Prozessschritte müssen definiert und im bestehenden Ablauf verankert werden. Eventuell müssen neue Kompetenzbereiche ausgeschrieben und besetzt werden. Diese organisatorischen Punkte greifen oft breit in die Firma ein und betreffen nicht nur die IT, sondern auch andere Organisationseinheiten. Auch diesen sind die Ziele und Massnahmen darum klar und motivierend zu kommunizieren, um Missverständnissen vorzubeugen.

Die Umstellung kann nicht von heute auf morgen geschehen, das Verständnis und die

sich deshalb oft über eine längere Zeitspanne, typischerweise ein bis zwei Jahre. Wichtig ist es, auf dem Weg zum Ziel klar definierte Meilensteine und auch Lieferobjekte festzulegen, damit der Fortschritt überprüft werden kann. Der ganze Prozess ist kontinuierlich als aktives Vehikel voranzutreiben, welches bei ständiger kritischer Betrachtung immer wieder Verbesserungsmöglichkeiten aufnimmt und zur Umsetzung bringt.

Fazit

Um auch bei reduzierten Budgets handlungsfähig zu bleiben, macht sich heute jede IT-Organisation Gedanken zur Industrialisierung ihrer Softwareherstellung, z. B. indem die Fertigungstiefe durch Sourcing-Strategien gesenkt wird. Dieser Ansatz entbindet jedoch nicht davon, effizienzsteigernde Massnahmen

Bettina Polasek

Bettina Polasek, dipl. Informatik-ingenieurin ETH, ist seit 2006 bei der AdNovum als Software-Entwicklerin tätig. Seit gut einem Jahr ist sie als Peer für die Quality-Assurance-Engineering-Gruppe in der AdNovum Ungarn verantwortlich für Qualitätssicherungsaspekte im Software-Entwicklungs-Prozess. In der Freizeit kurvt sie gerne mit ihrem Partner auf dem Tandem durch die Landschaft.



Application-Management

NINA LASCHET UND STEPHEN JONES IM INTERVIEW MIT NOTITIA.

NOTITIA: AdNovum hat vor kurzem eine Business-Applikation aus der Automobilbranche im Application-Management übernommen. Was beinhaltet dies?

N.L.: Wir haben die Wartung der Software übernommen und gleich einen Release mit ein paar Change-Requests implementiert, getestet und beim Kunden produktiv eingeführt. Dazu haben wir den Code zu uns ins Haus geholt und bei uns eine Testumgebung aufgebaut.

Weshalb wurde das Management der Applikation zu AdNovum ausgelagert?

N.L.: Die Changes waren dringend nötig. Die Applikation war verwaist und das Know-how dazu in der Firma nicht mehr vorhanden.

Niemand hatte Zeit, neben dem Alltagsgeschäft noch Know-how aufzubauen und Änderungen an die Hand zu nehmen.

Wie ist AdNovum dazu gekommen, Application-Management anzubieten?

S.J.: Aufgrund unserer Engineering-Kompetenz hat sich eine Nachfrage dafür ergeben, aus Wartungsvereinbarungen von Software, die wir entwickelt haben, aber auch für Software, die von Kunden oder Drittanbietern entwickelt wurde.

« CHANGE-REQUESTS ZWINGEN EINEN, DEN SOURCECODE KENNENZULERNEN. »

Für den Kunden kann externes Application-Management aus verschiedenen Gründen interessant sein: Die Leistung kann intern nicht kostengünstig und effizient erbracht werden, oder das Unternehmen findet keine Mitarbeiter mit dem nötigen Know-how, insbesondere wenn es um ältere Technologien geht. Oder man möchte sich von der Applikation lösen, weil sie nicht in der Kernkompetenz liegt oder nach einer strategischen Neuausrichtung nicht mehr ins Portfolio passt. Oft genügt es schon, dass die Zukunft einer Applikation ungewiss ist. Die Mitarbeiter des Unternehmens sind dann gegebenenfalls nicht motiviert, Zeit in sie zu investieren, man gibt die Applikation lieber extern zur Pflege.

Machen Sie da auch Vorschläge, was man weiter mit der Applikation tun könnte?

S.J.: Ja, machen wir gerne, falls gewünscht; es gibt aber auch den Fall, wo es wirklich nur darum geht, das Management der Applikation auszulagern.

N.L.: Im vorliegenden Fall haben wir beispielsweise auch die Codequalität untersucht und eine entsprechende Review abgegeben. Auf dieser Basis konnten wir unsere Ideen einbringen; wir haben dann einen Vorschlag für einen Neubau der Applikation eingebracht.

Welche besonderen Herausforderungen bot diese Auslagerung?

N.L.: Dokumentation war kaum vorhanden, wir haben praktisch nur den Sourcecode erhalten. Dieser war zudem nicht ganz pflegeleicht, er enthielt einen bunten Mix von Technologien. Für den Neubau haben wir deshalb vorgeschlagen, deren Anzahl zu reduzieren, damit man nicht so viel verschiedenes Know-how unterhalten muss. Zudem war die Testumgebung beim Kunden nicht mehr einsatzfähig, wir mussten sie völlig neu aufbauen.

Welches sind die Erfolgsvoraussetzungen von Kundenseite für die Auslagerung des Managements einer Applikation?

S.J.: Erstens der politische Konsens. Es müssen sich wirklich alle Beteiligten beim Kunden einig sein, dass die Applikation extern weitergepflegt werden soll. Nur so können wir als

externer Partner die Unterstützung bekommen, die wir brauchen, um das Know-how aufzubauen.

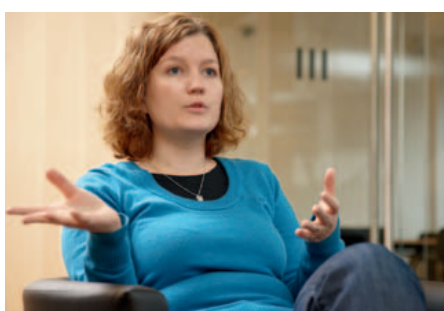
Zweitens braucht es Change-Requests, quasi ein «Meisterstück»: Dies zwingt einen als Entwickler, den Sourcecode kennenzulernen und man gewinnt Hands-on Experience. Damit ist man nachher wirklich in der Lage, Support zu leisten und gegebenenfalls Weiterentwicklungen durchzuführen.

N.L.: Drittens: Die Übergabe muss beim Kunden als Projekt angesehen und von einem internen Projektleiter begleitet werden, der als zentrale Ansprechperson fungiert, Fragen und Informationen weiterleitet, Release-Termine arrangiert.

Welche Vorteile hat externes Application-Management gegenüber anderen Optionen?

S.J.: Gegenüber der Variante, die Applikation selber zu betreiben und weiterzuentwickeln, bietet Application-Management durch einen Anbieter wie uns erhöhte Flexibilität bezüglich Ressourcen und damit eine Kosteneinsparung. Der Kunde muss Fachleute nicht selber anstellen und beschäftigen, sondern kann sie dann beanspruchen, wenn er sie braucht.

N.L.: Und er erhält jeweils genau die richtigen Spezialisten für sein Vorhaben.





Nun, der Kunde könnte doch auch Mitarbeiter im Bodyleasing anstellen?

S.J.: Diese lassen sich jedoch zeitlich wohl nicht derart flexibel einsetzen wie ein externes Application-Management-Team, und der Kunde trägt die Verantwortung für die Applikation immer noch selbst. Ein Service Level Agreement (SLA) mit uns dagegen beinhaltet eine Verpflichtung unsererseits, es ist wie eine

kennenlernen und seine spezifischen Bedürfnisse in ihrer Terminologie ausdrücken können, bevor er sie nutzen kann.

N.L.: Eventuell muss er sie sogar anpassen.

S.J.: Bei einer Übergabe der Applikation an uns kann der Kunde seine bewährte Software weiter nutzen. Empfiehlt sich später ein Neubau mit Verwendung von Standardsoftware, stehen wir als Implementationspartner zur Verfügung. Wir passen uns in jedem Fall dem Vokabular, den Prozessen und den Organisationsstrukturen des Kunden an. Der Kunde erhält bei uns einen Service, der für ihn aussieht, als wäre er intern.

Und Application-Outsourcing?

S.J.: Der Vorteil beim Application-Management ist, die gesamte Infrastruktur ist beim Kunden immer noch intern. In zwei Minuten ist er beim Server, und der Server bleibt innerhalb seines eigenen Sicherheitsdispositivs.

Das heisst natürlich auch, die entsprechende Sicherheitsverantwortung bleibt beim Kunden?

S.J.: Je nach Grösse des Unternehmens kann das ein Vorteil oder ein Nachteil sein. Der Kunde hat genau die Security, die er braucht. Und er muss keine netzwerkbedingten Verzögerungen gewärtigen. Bei performancekritischen Anwendungen kann das relevant sein. Je nach Anbindung des Rechenzentrums des Kunden zum Outsourcing-Provider stellt sich auch die Frage, ob es sich lohnt, zwei Standorte zu betreiben.

Welches sind AdNovums spezifische Stärken im Application-Management?

N.L.: Wir haben einen etablierten Software-Engineering-Prozess und ein ausgebautes Quality-Engineering.

«SERVICE, DER AUSSIEHT, ALS WÄRE ER INTERN.»

Versicherung. Der Kunde erhält Unterstützung in allen Belangen, er kann die Verantwortung für die Software und den Betrieb vollständig übergeben. Variable, unberechenbare Kosten lassen sich mit einem SLA in fixe Aufwandsposten umwandeln.

Oder einfach auf eine Standardsoftware wechseln?

S.J.: Auch wenn eine Standardsoftware im Wesentlichen dasselbe Business-Thema abdeckt, muss der Kunde sie erst mal vertieft

S.J.: Dank unserer langjährigen Erfahrung im Software-Engineering und im Applikationsbau, die gepaart ist mit branchenspezifischem Business-Know-how, können wir uns im gesamten Lebenszyklus einer Applikation bewegen. Wir können eine Applikation bzw. ihre Komponenten weiterentwickeln, modernisieren, renovieren oder ersetzen. Wir können die Applikation z.B. technologisch auf eine neue Basis stellen: sie im fachlichen Bereich belassen, aber unten eine neue Technologie hineinschieben.

Und wenn der Kunde keine Weiterentwicklung, sondern «nur» Wartung wünscht?

S.J.: Bei der Übernahme einer Applikation analysieren wir die Software und integrieren sie in unseren Software-Entwicklungs-Prozess mit reproduzierbaren Builds, Continuous Integration und deterministischem Technologie- und Versions-Management. So sind wir bei dringenden Korrekturen und Anforderungen jederzeit in der Lage, innert Stunden bis Tagen einen Release zu liefern. Falls nötig optimieren wir auch das Tracing und Logging, damit wir im Fehlerfall die wichtigen Informationen schnell finden.

N.L.: Mit unseren individuellen SLAs erhält der Kunde zudem genau das Paket von Support- und Wartungsdienstleistungen, das er wünscht.



Wie positionieren Sie sich gegenüber IT-Generalisten, die europaweit oder weltweit anbieten und auch Applikationen übernehmen?

N.L.: Ganz klar mit unserem individuellen Service. Wir können den Kundenwünschen genau entsprechen und sind falls erforderlich

schnell vor Ort, z. B. um mit dem Kunden auf der Testumgebung zu testen und ein Problem zu analysieren. Wir können auf jede Technologie eingehen und damit verbundene Probleme lösen, wir können auch neue Technologien aufnehmen.

S.J.: Da wir nicht bestimmten Technologien und Produkten verpflichtet sind, können wir den Kunden dabei entsprechend unabhängig beraten.

Wie gewährleisten Sie dem Kunden Unabhängigkeit von AdNovum, also die Option zum Wechsel des Anbieters oder zur Rückübernahme?

N.L.: Mit unserem Application-Management behält der Kunde alle Rechte an der Applikation und dem Sourcecode. Wenn er sie



zurückhaben bzw. weitervergeben möchte, stellen wir den Know-how-Rückfluss sicher.

S.J.: Mitarbeiter des Kunden arbeiten z. B. bei uns inhouse bei der Entwicklung der Applikation mit und erarbeiten sich so die Erfahrung und das Know-how, um sie danach in eigener Verantwortung weiterzupflegen. Für die Übergabe passen wir die Software falls nötig auch an das spezifische Build- und Development-Environment des Kunden an.

N.L.: Ob nun der Kunde auf Windows arbeitet, mit IBM RAD oder mit einem anderen System, wir stellen uns darauf ein und passen alles so an, dass es bei ihm läuft.

Der Kunde ist also nicht fixiert auf das System oder die Architektur, die AdNovum vertritt?

N.L.: Die AdNovum vertritt nicht eine Architektur, sondern die AdNovum ist eben multiplattformfähig.

S.J.: Unseren Security-Stack beispielsweise haben wir auf x verschiedene Plattformen portiert. Wir können bezüglich Sourcecode-Struktur, Compiler, Betriebssystem und Build-Tool (z. B. Ant oder Maven) auf jegliche Kundenwünsche eingehen.

Bietet AdNovum mit ihrem Application-Management auch Industrialisierung und Neugestaltung der Prozesse?

N.L.: Bei unserer Business-Applikation haben wir für den Software-Engineering-Prozess beim Kunden Vorschläge eingebracht, die

« DER KUNDE BEHÄLT ALLE RECHTE AN DER APPLIKATION UND DEM SOURCECODE. »

dann auch umgesetzt wurden: Installationsprozess, Testing-Ablauf und Testumgebung beim Kunden sind nun stetig optimiert worden.

Und bezüglich Geschäftsprozessen?

S.J.: Wenn wir das Management einer Applikation übernehmen, bauen wir mit dem Know-how über die Applikation zugleich kundenspezifisches fachliches Know-how in diesem Bereich auf. Damit können wir den Kunden nicht nur in technologischen, sondern auch in organisatorischen und strategischen Fragen unterstützen. Application-Management bietet also eine gute Ausgangslage für ein Consulting im fachlichen Bereich.

Wie setzt sich ein AdNovum-Team für ein Application-Management-Projekt zusammen?

N.L.: Ein Business-Projektleiter und ein technischer Projektleiter, dazu ein paar weitere Teammitglieder, die je mit einem Teilpensum im Team mitarbeiten. Damit haben wir eine genügend breite Basis von Know-how-Trägern, die sich im Supportfall gegenseitig vertreten können.

Beziehen Sie beim Application-Management auch mal Leistungen aus anderen Locations mit ein?

N.L.: Wir haben Mitarbeiter in Ungarn, die bei der Entwicklung und Weiterentwicklung zum Zug kommen. Unser zentrales Angebot an den Kunden ist jedoch, dass er immer eine Ansprechperson in der Nähe hat, die für Supporteinsätze und Meetings kurzfristig vor Ort sein kann. Jedes unserer Application-Management-Teams besteht im Kern aus Leuten in der Schweiz.

Weshalb ist die räumliche Nähe so bedeutend?

S.J.: Bei den Lösungen, die wir managen, sind in der Regel die Applikation und auch das

Umfeld individuell. Wir benötigen deshalb viel spezifisches Wissen, das jedoch unter Umständen beim Kunden nicht mehr vorhanden ist. Application-Management funktioniert dann nur, wenn wir selber hingehen und die nötigen Informationen vor Ort beschaffen

können. Unsere Kunden legen zudem Wert darauf, einen Ansprechpartner zu haben, der in der Nähe ist ...

N.L.: ... und der die gleiche Sprache spricht, z. B. Deutsch.

Vor allem aber muss er das Projekt gut kennen. Die Applikationen sind zum Teil sehr komplex. Wenn der Ansprechpartner beispielsweise weiss, dass kürzlich schon ein ähnlicher Fall aufgetreten ist, kann er eine Problemursache unter Umständen um Faktoren schneller eruieren. Die persönliche Entgegennahme der Supportcalls durch eine kompetente Ansprechperson, die sie eventuell sogar kennen, wird von unseren Kunden sehr geschätzt.

Nina Laschet

Nina Laschet, Master of Computer Science ETH, arbeitet seit 2007 bei der AdNovum. Sie hat als Technische Projektleiterin die Entwicklung verschiedenster Fachapplikationen koordiniert. In ihrer Freizeit erkundet sie gerne mit ihrem Partner die Nationalparks und Downtowns von Kalifornien.

Stephen Jones

Stephen Jones, dipl. Informatik-Ing. ETH, ist seit 2003 bei AdNovum tätig. Als Business-Projektleiter begleitet er Software über den ganzen Lebenszyklus, von der Ausarbeitung einer Vision über die Optimierung im Betrieb bis zur Ablösung. In der Freizeit macht er zu Fuss oder auf dem Snowboard die Berge unsicher.

Sichere Transaktionen

DIE BEDROHUNGEN FÜR WEBAPPLIKATIONEN ZIELEN ZUNEHMEND AUF DIE BENUTZERPLATTFORM UND ERFORDERN DAMIT NEUE SICHERHEITSMASSNAHMEN, BEISPIELSWEISE TRANSAKTIONSSIGNATUREN.

VON MANUEL HILTY

Sicherheit ist bei Webapplikationen schon seit Anbeginn ein Thema. Früher gingen die Attacken vorwiegend von zwei Gruppen aus: von Hackern, nicht immer mit kriminellen Absichten, teilweise auch nur als sportlicher Wettbewerb, und von Script-Kiddies, welche von Hackern implementierte Attacken ausführten, ohne über grosse Fachkenntnisse zu verfügen. In den letzten Jahren ist die Internetkriminalität jedoch stetig organisierter, systematischer und professioneller geworden. Angreifer sind vermehrt im organisierten Verbrechen und in Geheimdiensten angesiedelt und agieren nicht mehr nur als Einzelpersonen, sondern auch in Gruppen. Damit

gabesvalidierung gegen bösartigen Input (SQL-Injection, Command-Injection etc.), Authentifizierung und Autorisierung gegen unautorisierten Zugriff, Firewalls und OS-Maintenance gegen Korruption des Host-Systems sowie Verschlüsselung (SSL) gegen das Abhören der Kommunikation (Einsehen und Stehlen von Kundendaten, Kreditkartennummern, Passwörtern etc.).

Neue Bedrohungen

In den vergangenen Jahren haben sich die Angriffe zunehmend auf die Benutzerplattformen (PCs) verlagert. Ein Grund dafür ist, dass die oben erwähnten Sicherheitsmassnahmen

Oft wird Malware bei sogenannten Drive-by Infections während dem Surfen im Web eingefangen, leider oft auch bei seriösen Anbietern. Eine Google-Studie von Ende 2007 ergab beispielsweise, dass 10 % aller Internetseiten Malware enthalten. Es gibt mittlerweile eine Malware-Industrie, welche Entwicklungs-Kits für Malware inklusive Support verkauft. Damit lassen sich massgeschneiderte Angriffe einfach entwickeln. Zudem ist inzwischen auch Betriebssystem-unabhängige Malware entstanden, welche direkt die Webbrowser angreift.

Durch die zunehmende Infizierung von Client-Software werden sogenannte Man-in-the-Browser-Attacken immer weiter verbreitet. Bei einer solchen Attacke manipuliert Malware die Kommunikation innerhalb des Webbrowsers, was es ihr erlaubt, andere Daten weiterzureichen, als der Benutzer eingibt, und ihm andere Informationen anzuzeigen, als die Webapplikation gesendet hat. Dabei wird der Client-Server-Kanal nicht attackiert und die Attacke wird weder vom Benutzer noch vom Server erkannt.

Bei Man-in-the-Browser-Angriffen auf E-Banking-Applikationen verändert die Malware das Zielkonto und/oder den Betrag einer Transaktion, um das Geld auf Konten von Mittelsleuten umzuleiten und von dort ins Ausland zu verschieben. Diese Mittelsleute – sog. Money-Mules – werden von den Betrügern unter Vorwänden wie z.B. karitativen Zwecken dazu gebracht, ihre Konten für Geldtransfers zur Verfügung zu stellen.

Gegenmassnahmen

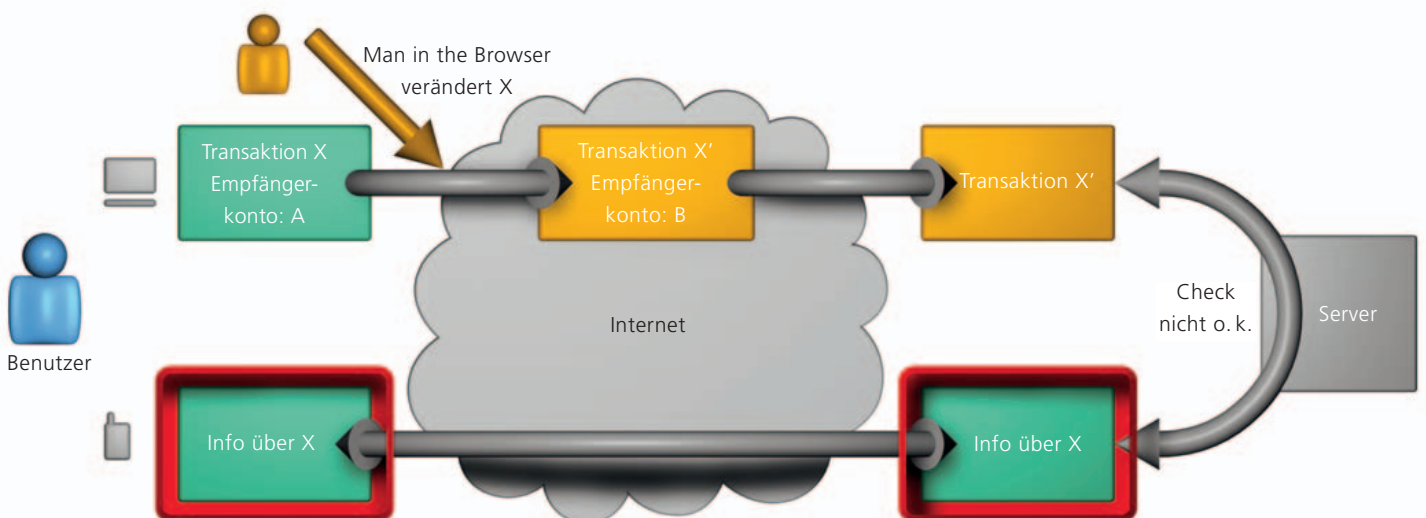
Die Gegenmassnahmen gegen die klassischen Angriffe auf Webapplikationen sind

BETRIEBSSYSTEM-UNABHÄNGIGE MALWARE GREIFT HEUTE DIREKT DIE WEBBROWSER AN.

steigt nicht nur der Umfang der Internetkriminalität, sondern auch die Qualität der Angriffe, und es stehen konkrete wirtschaftliche und politische Interessen im Vordergrund.

Auch die Art der Bedrohungen ist im Wandel. Lange Zeit zielten die Angriffe auf die Webapplikation, den Webserver oder den Kommunikationskanal, worauf entsprechende Gegenmassnahmen entwickelt wurden: Ein-

mittlerweile zu etablierten Best Practices geworden sind und die «klassischen» Angriffsformen signifikant erschwert haben. Die Sicherheit der Client-Plattformen hat sich hingegen nicht erhöht, im Gegenteil. Malware ist allgegenwärtig und findet durch die schnellen Veränderungen und die hohe Komplexität der auf Client-Computern verwendeten Software immer neue Angriffspunkte.



Transaktionssignaturen.

nicht dazu geeignet, solche Man-in-the-Browser-Attacken zu verhindern. Deshalb sind neue Gegenmassnahmen nötig. Zurzeit werden die folgenden drei Ansätze am meisten verfolgt:

- Signieren oder Bestätigen von Transaktionen durch den Benutzer
- Fraud-Detection
- Einsatz sicherer Client-Plattformen

Letzteres wird z. B. umgesetzt, indem die Benutzer einen «gehärteten» Webbrowser auf einem nicht veränderbaren USB-Stick erhalten und für ihr E-Banking verwenden sollen. Dies schützt gegen klassische Man-in-the-Browser-Attacken, nicht jedoch gegen all-fällige modifizierte Varianten, welche anstatt den Browser die Benutzeroberfläche des Betriebssystems manipulieren. Die Massnahme hat dafür den Vorteil, dass sie für den Benutzer nur einen minimalen Mehraufwand bedeutet und auch die Komplexität kaum erhöht.

Fraud-Detection hat zum Ziel, manipulierte Transaktionen aufgrund statischer Regeln oder der Detektion von Anomalien zu erkennen. Diese Massnahme wird in der Kreditkartenindustrie und in Zusammenhang mit dem Geldwäschereigesetz schon seit Jahren angewendet. So wird beispielsweise Verdacht geschöpft, wenn der Betrag einer Transaktion ungewöhnlich hoch ist oder wenn eine Kreditkarte innerhalb kurzer Zeit an zwei weit auseinanderliegenden Orten verwendet wird.

Wenn die Fraud-Detection-Software eine Transaktion als verdächtig taxiert, darf diese nicht ausgeführt werden oder ihre Legitimität muss zuerst auf anderem Wege verifiziert werden, z. B. durch manuelle Bearbeitung oder Rückfragen. Der Einsatz von Fraud-Detection bringt für die Benutzer keine erhöhte Komplexität, für die Bank jedoch unter Umständen grosse Backoffice-Aufwände.

Solche Komponenten sind typischerweise als dedizierte Hardware-Geräte realisiert (z. B. separate Karten oder USB-Sticks). Diese Geräte können viel besser geschützt werden als Softwarekomponenten, welche auf einer verwundbaren Plattform laufen. Auf dem Display des Gerätes werden die Eckdaten der Transaktion angezeigt. Je nach System kann der Benutzer die Transaktion dann direkt auf

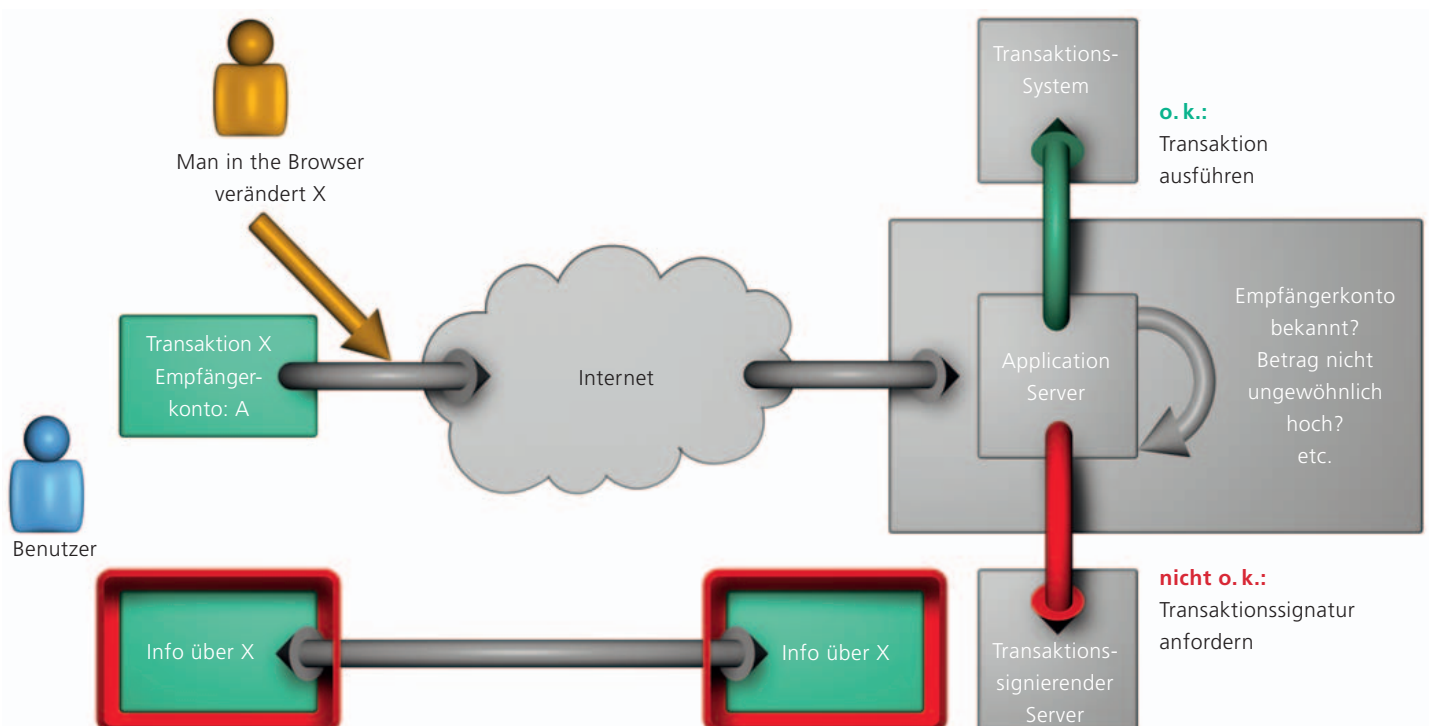
VERBREITET SIND HEUTE TRANSAKTIONSBESTÄTIGUNGEN VIA SMS. BEI SMARTPHONES EINE HEIKLE SACHE.

Transaktionssignaturen

Transaktionssignaturen oder -bestätigungen – hier beide als Transaktionssignaturen bezeichnet – ermöglichen es den Benutzern, den Inhalt einer Transaktion vor der Ausführung auf eine sichere Art und Weise zu verifizieren. Dabei wird dem Benutzer der Inhalt der Transaktion über einen zusätzlichen Kanal nochmals angezeigt. Der Benutzer kann diesen Inhalt überprüfen und, falls alles korrekt ist, bestätigen. Der zusätzliche Kanal kann entweder komplett separiert sein vom Kanal, über welchen die Transaktion in Auftrag gegeben wurde, oder auch denselben Übertragungsweg haben und auf einer vertrauenswürdigen, d. h. hochsicheren Komponente enden.

dem Gerät bestätigen, evtl. mit einer digitalen Signatur, oder auf dem Gerät wird ein Bestätigungscode angegeben, den der Benutzer in der Webapplikation eingeben kann.

Ein weit verbreitetes Beispiel für die Verwendung von separaten Kanälen sind Transaktionsbestätigungen via SMS. Dabei wird dem Benutzer ein SMS mit den Eckdaten der Transaktion und einem Bestätigungscode geschickt, der Rest funktioniert analog zum obigen Beispiel. Diese Variante ist einfach zu realisieren, jedoch nicht mehr sicher, falls dasselbe Gerät nicht nur zum Empfangen von SMS, sondern auch für die Benutzung der Webapplikation verwendet wird. Dies muss bei der Verwendung von Smartphones beachtet werden.



Kombination von Transaktionssignaturen und Fraud-Detection.

Der grosse Vorteil von Transaktionssignaturen ist ihre hohe Sicherheit, welche aus der Robustheit gegenüber Angriffen auf die Client-Plattformen resultiert. Auch wenn ein Angreifer die Client-Plattform eines Benutzers kontrolliert, kann er die Display-Ausgabe des zweiten Kanals nicht manipulieren. Damit kann man zwar nicht verhindern, dass ein Angreifer Transaktionsdetails verändert, aber die Benutzer können solche Änderungen detektieren und die entsprechenden Transaktionen verweigern. Der hauptsächliche Nachteil von Transaktionssignaturen ist, dass sie die Usability der Webapplikationen verringern. Benutzer, welche ständig dazu aufgefordert werden, Transaktionen zu bestätigen, könnten unaufmerksam werden und so Änderungen an Transaktionen nicht mehr detektieren. Zudem befürchten die Betreiber von Websites, dass die Supportaufwände durch die Einführung einer solchen Technologie signifikant steigen würden.

Die Nachteile von Transaktionssignaturen lassen sich durch geschicktes Kombinieren mit anderen Mechanismen – im Speziellen Fraud-Detection – kompensieren: Transaktionssignaturen werden nur noch dann verlangt, wenn die Fraud-Detection eine verdächtige Transaktion detektiert hat. Damit wird der Benutzeraufwand signifikant reduziert, aber trotzdem ein hoher Sicherheitslevel beibehalten.

Transaktionssignaturen in Nevis

Das Nevis-Framework von AdNovum unterstützt die Einbindung verschiedener Trans-

aktionssignatur-Verfahren. So sind z. B. SMS-Bestätigungen und die Verwendung von AXSionics-Tokens implementiert. Andere Verfahren können einfach eingebunden werden. Bei Nevis verfolgen wir den Ansatz von nichtinvasiven Transaktionssignaturen: Die Nevis-Komponenten verarbeiten die Transaktionssignaturen selbstständig, sodass die Applikationen nicht umgebaut werden müssen, was den Implementationsaufwand deutlich reduziert. Zudem erlaubt nevisProxy die Einbindung von Fraud-Detection-Komponenten. Die Fraud-Detection kann nevisProxy in diesem Fall mitteilen, bei welchen Transaktionen eine Transaktionssignatur verlangt wird.

Fazit

Der Schutz gegen «klassische» Attacken auf Webapplikationen kann mit bewährten Mechanismen zu einem sehr hohen Grad sichergestellt werden. Angesichts der neuen Bedrohungsformen sind diese Massnahmen jedoch nicht ausreichend. Obwohl dafür noch keine ultimative Lösung in Sicht ist und alle Ansätze ihre Stärken und Schwächen aufweisen, bietet eine sinnvolle Kombination von Massnahmen wie Transaktionssignaturen und Fraud-Detection einen hohen Schutz, kombiniert mit akzeptabler Benutzbarkeit. Mit Nevis lassen sich solche Verfahren nichtinvasiv in bestehende Webapplikationen einbinden. ■

Manuel Hilty

Manuel Hilty befasste sich in seinem Doktorat an der ETH mit der technischen Umsetzung von Datenschutzanforderungen. Bei einer Privatbank hat er Erfahrung als Sicherheitsspezialist gesammelt. Seit Anfang 2008 bringt er sein Wissen bei der AdNovum als Technischer Projektleiter und Architekt in diverse Kundenvorhaben ein. Den Winter verbrachte er neben dem Arbeiten vor allem damit, sich auf verschiedenste Arten über oder durch den Schnee zu bewegen.



Manuel Hilty setzt sich als Technischer Projektleiter für die IT-Sicherheit ein.

ASP für Banken

MIT EINER UNIVERSALBANKPLATTFORM VIA APPLICATION SERVICE PROVIDING DIE EIGENE WETTBEWERBSPOSITION STÄRKEN.

VON THOMAS KEEL, HEAD OF SALES & MARKETING, T-SYSTEMS BANKING SERVICES

Kleine und mittelgrosse Banken der Schweiz erkennen zunehmend, dass sie nicht zwingend eine eigene kostspielige IT-Infrastruktur aufbauen und unterhalten müssen. Tatsächlich erfüllt eine Universalbankplattform auch im ASP-Modell (Application Service Providing) alle Anforderungen an eine Banklösung.

Der Weg zu einer modernen Vertriebsbank, die den gestiegenen Kundenanforderungen entspricht, führt über eine verstärkte Standardisierung und Industrialisierung der Bank-IT-Prozesse. Die Migration auf Universalbankplattformen wie Avaloq oder Finnova

die Auslagerung von Wartung und Betrieb der Applikationen und der IT-Infrastruktur sprechen gewichtige Gründe wie die Reduktion des Betriebsrisikos oder der Zugriff auf aktuelle Technologien und Know-how. Das ASP-Modell erlaubt der Bank und ihrem Management, sich ganz auf die Betreuung ihrer Kunden zu konzentrieren.

USP durch individuelle Anpassungen

Bis vor kurzem mussten die Banken ihre Plattform häufig in Eigenregie betreiben. Das ASP-Modell befreit sie nun auch davon, sich

DIE T-SYSTEMS ASP-BANKING-SOLUTION POWERED BY AVALOQ UNTERSTÜTZT BANKEN BEIM AUSLAGERN VON IT-PROZESSEN.

und die Auslagerung von Wartung und Betrieb dieser Applikationen an externe Dienstleister bieten den Banken substanzielle Vorteile.

Für viele kleinere bis mittlere Institute kommt ein Eigenbetrieb strategisch und kapazitätsmässig je länger, je weniger in Frage. Für

um Lizenzen, die IT-Architektur und Festlegung von Hard- und Softwarekomponenten zu kümmern. Aus Sicht der Bank gibt es nur einen zentralen Ansprechpartner. Er übernimmt die Verantwortung für die Lizenzierung, Implementierung, Integration und Migration der Banking-Solution und garantiert den IT-Betrieb und das Application-Management auf Basis von Service Level Agreements (SLA).

Im ASP-Modell kommen – wie auch beim klassischen Outsourcing – Vorteile wie Skaleneffekte oder Professionalisierung der IT bei gleichzeitiger Effizienzsteigerung zum Tragen. Zudem können durch die Wahl einer Standardplattform die Implementations- und Migrationszeiten verkürzt und die Qualität beim IT-Betrieb weiter gesteigert werden. Dank Abrechnung gemäss «pay per use» passen sich die Kosten dem Geschäftsgang an.

Doch auch Standardpakete erfordern eine aktive Mitwirkung der Bankfachleute. Zwar ist ein beträchtlicher Teil der Bankanwendungen standardisiert und letztlich für alle Banken gleich, beispielsweise die Abwicklung von Zahlungen. Doch die individuell angepassten Teile der Lösung machen die USPs der Bank

T-Systems

T-Systems ist in der Schweiz mit über 900 Mitarbeitenden an verschiedenen Standorten vertreten. Rund 120 davon stehen im Bereich Banking Services für schweizerische Retail- und Privatbanken im Einsatz. Das Banken-Kompetenzzentrum von T-Systems verknüpft Outsourcing mit Standardisierung und Individualisierung und schafft so mehr Beweglichkeit und eine nachhaltige Kostensenkung.
www.t-systems.ch

aus. Hier muss sich die Bank darüber im Klaren sein, wie sie sich von ihren Wettbewerbern differenzieren will: durch ihre Produkte oder durch spezifische Prozesse.

Gerade kleinere und mittlere Banken, die besonders von Standardpaketen profitieren, müssen hier ihre Chance zur Profilierung nutzen. Und dies geht eben nur durch eine aktive Mitarbeit bei der Gestaltung der Gesamtlösung. Die Erfahrung des Anbieters mag auch in dieser Phase einfließen, aber für ihr Geschäftsmodell ist letztlich die Bank selbst zuständig.

Alle Finma-Vorschriften erfüllt

Die T-Systems ASP-Banking-Solution powered by Avaloq ist auf die Bedürfnisse von Retailbanken und Privatbanken mit bis zu 200 Usern ausgerichtet. Das standardisierte Basispaket, das bereits alle Vorschriften der Finma erfüllt, kann aber jederzeit ganz nach Bedarf erweitert werden: sei es mit der Anbindung von Finanzservices wie SWX, Reuters und Bloomberg, mit dem Aufbau und Betrieb von weiteren Umsystemen oder mit Druck- und Versandservices.

Fazit: Insbesondere kleinere bis mittlere Banken können sich sehr wohl im Wettbewerb behaupten, wenn sie ihre IT-Prozesse standardisieren und den Betrieb der ausgewählten Lösung einem spezialisierten Bank-IT-Services-Anbieter überlassen. IT ist notwendig für den erfolgreichen Betrieb einer Bank, gehört aber nicht zu den Kernkompetenzen. Das ASP-Modell gibt Banken die Chance, technisch auf der Höhe der Zeit zu sein, ohne in eigenes Know-how investieren zu müssen. ■

Impressum

Herausgeber:

AdNovum Informatik AG
Corporate Marketing
Röntgenstrasse 22
CH-8005 Zürich
Telefon 044 272 61 11
E-Mail info@adnovum.ch
www.adnovum.ch

Verantwortung und Redaktion:

Manuel Ott
Feedback: notitia@adnovum.ch

Gestaltung und Realisation:

Rüegg Werbung, Zürich

Fotografie:

Gerry Nitsch, Zürich