AdNovum

NOTITIA

Bemerkenswertes von und über AdNovum

Frühling 2011, Heft Nr. 20

Enterprise-Portale

Inhalt

Liebe Leserin, Lieber Leser

Es freut mich, Sie zur 20. Ausgabe unserer Kundenzeitschrift begrüssen zu dürfen.

Kunden, Partner und Lieferanten greifen immer tiefer in die Prozesse von Unternehmen ein. Dies bringt mehr Effizienz, Kundennähe und passendere und konsistentere Angebote. Im Gegenzug erwarten und benötigen die externen Anspruchsgruppen wie die Mitarbeitenden einen einfachen und schnellen Zugriff auf personalisierte und konsolidierte Informationen und Anwendungen. Parallel dazu gewinnen Kommunikation und Zusammenarbeit an Bedeutung, und damit auch die Kollaborationstools und -plattformen des Web 2.0.

Für diese Bedürfnisse versprechen Enterprise-Portale eine umfassende Lösung und sind deshalb sehr gefragt. Portale bieten eine unglaubliche Vielfalt an Funktionen und Leistungen. Gemeinsam haben sie oft einzig den Aspekt der Integration.

Nun bilden die Applikationen und Dienste in den meisten Unternehmen jedoch historisch gewachsene und entsprechend heterogene Landschaften, die grosse Investitionen beinhalten und wesentliche Geschäftsprozesse gewährleisten. Damit bleibt die Integration die grösste Herausforderung, werden doch von einer modernen Portallösung Performanz, Verfügbarkeit, Verteilbarkeit, Sicherheit und Compliance erwartet.

Wie gelingt die Einführung eines Enterprise-Portals? Worauf ist zu achten? Welche Komponenten braucht es dafür? Lesen Sie dazu den einleitenden Artikel von Gábor Ginter und Pascal Buchbinder und das Interview mit Christof Dornbierer und Tom Sprenger.

Speziell gewinnbringend in verteilten Umgebungen, wie sie Enterprise-Portale typischerweise integrieren, ist auch die Umsetzung einer zentralen Autorisierung. Andreas Petralia und Moritz Kuhn berichten im Hintergrund-Artikel aus erster Hand über die Anwendung des XACML-Autorisierungsmodells in einem E-Health-Projekt im Kanton Genf.

Als Autor des Partner-Beitrags dürfen wir in dieser Ausgabe Herrn Jürg Truniger von der Firma qumram begrüssen. Er stellt eine Lösung vor, die erlaubt, über Webplattformen ausgetauschte Informationen und Transaktionen lückenlos nachvollziehbar – und damit revisionssicher – zu archivieren.

Nun wünsche ich Ihnen viel Lesevergnügen!

Ruedi Wipf

CEO AdNovum Informatik AG

Stein auf Stein zum Portal

Was ist ein Enterprise-Portal, wie realisiert man es und was braucht es dazu? AdNovum hat dazu einen eigenen, pragmatischen und deshalb flexiblen Ansatz entwickelt.

Von Gábor Ginter und Pascal Buchbinder

Ohne kontinuierliche Interaktion mit Kunden, Lieferanten und Partnern geht in Organisationen und Unternehmen in der heutigen Wirtschaftswelt gar nichts mehr. Dies hat einschneidende Implikationen für den Umgang mit Informationen und Prozessen und die Gestaltung von Softwaresystemen. Prozesse sollen einmal durch zentrale Services systemübergreifend integriert und optimiert werden, dann aber auch über die beteiligten Organisationen hinweg, indem man Teilprozesse vernetzt.

Die Anwender sollen Content und Services aggregiert, vernetzt und in personalisierter Form zur Verfügung haben und ohne Medienbrüche bearbeiten können. Mit der organisationsübergreifenden Zusammenarbeit und Prozessabwicklung gewinnen Sicherheit und Compliance weiter an Bedeutung und erfordern eine zentrale Verwaltung und Kontrolle von Zugriffen und Berechtigungen. Dies ermöglicht einen benutzerfreundlichen Single-Sign-on, und neue Applikationen lassen sich mit reduzierten Kosten und kürzerer Time-to-Market einführen.

Der Begriff Enterprise-Portal wird je nach Schwerpunkt und Marketingstrategie der Anbieter unterschiedlich definiert.

Vielfältiges Angebot

Unter dem Oberbegriff Enterprise-Portale ist in den vergangenen Jahren ein vielfältiges Angebot von Softwaresystemen entstanden, das diese Bedürfnisse aufnimmt. Je nach Schwerpunkt und Marketingstrategie der Anbieter wird der Begriff unterschiedlich definiert und mit Funktionen und Eigenschaften ausgefüllt. Enterprise-Portale bieten Collaboration-Management, Business-Process-Management, Enterprise-Resource-Planning, Customer-Relationship-Management, Supply-Chain-Management, Document-, Content- und Knowledge-Management und dergleichen mehr und reichen bis hin zu Expertensystemen auf Portalbasis.

An angebotener Funktionalität fehlt es also nicht. Will man diese aber nutzen und den in Aussicht gestellten Businessnutzen realisieren, kommt man nicht um die Frage herum, wie man eine solche Portalsoftware optimal einführt und parametriert. Sie muss so in die bestehende Applikationslandschaft integriert werden, dass sie die Geschäftsprozesse optimal unterstützt und dabei die Anforderungen hinsichtlich Verfügbarkeit, Performance, Verteilbarkeit, IT-Sicherheit und Compliance erfüllt.

Integration als gemeinsamer Nenner

Die Grundfunktion und der gemeinsame Nenner aller Portale ist die Integration von Informationen, Applikationen und Services. Es ist für ein Portalprojekt deshalb von zentraler Bedeutung, dass sie gelingt. Integration kann Folgendes beinhalten:

- Single-Sign-on und zentrales Identity- und Access-Management
- Eine einheitliche Benutzeroberfläche über alle Applikationen und Services hinweg
- Integrierte Basisfunktionen wie Indexierung und Suche
- Eine gemeinsame Datenbasis, damit Informationen über Applikationsgrenzen hinweg verknüpft werden können
- Eine Prozessplattform auf Basis einheitlicher Daten, was transparente und effizientere Prozesse ermöglicht

Neben der Verfügbarkeit und Performance verdient die Aktualität der Daten besondere Aufmerksamkeit. Sie ist umso wichtiger, je mehr Daten direkt in Echtzeit oder Quasi-Echtzeit geschrieben oder gelesen werden.

Das Gelingen der Integration ist für ein Portal zentral.

Ebenfalls zentral für die Akzeptanz durch die Anwender ist die Usability des Portals und der eingebundenen Applikationen. Die Benutzeroberfläche muss deshalb möglichst einheitlich, einfach und intuitiv bedienbar sein. Für unterschiedliche Anwender-

gruppen und deren divergierende Anforderungen können aber auch Konfigurationsmöglichkeiten gefragt sein. Dies kann bis zu einer individuellen Gestaltung der Benutzeroberfläche mit eigenem Logo und spezifischen Labels und Eingabefeldern reichen.

Der Bau von Enterprise-Portalen ist als dynamische Optimierungsaufgabe zu verstehen.

Pascal Buchbinder stellt Security-Komponenten für Portale bereit.

Bei dem beginnen, was ist

Dem verbreiteten Top-down-Ansatz, eine möglichst passende Portalsoftware einzukaufen und dann die benötigten Funktionen zu parametrieren oder zu implementieren und die benötigten Systeme zu integrieren, sei hier ein Bottom-up-Ansatz entgegengestellt: Auf Basis der aktuellen und der erwarteten Geschäftsanforderungen und der aktuellen Applikations- und Systemlandschaft soll entschieden werden, wie das Portal gebaut wird. Welche der bestehenden Komponenten sollen im Sinne des Investitionsschutzes weiterbetrieben und in die Portallösung integriert werden? Welche sind end-of-life und sollen durch neue Systeme ersetzt werden? Welche Module sollen für die Portalfunktionalität neu gewählt und in Betrieb genommen werden? Dies können dann durchaus Module einer Standard-Portalsoftware sein. Der Bau von Enterprise-Portalen ist dabei als dynamische Optimierungsaufgabe über die Zeit hinweg zu verstehen, die ein schrittweises und pragmatisches Vorgehen erfordert: Laufend sind neue Systeme und Anforderungen zu integrieren und alte abzulösen.

Orientierung an Portaltypen

Um so vorgehen zu können, muss man jedoch eine Vorstellung davon haben, wie eine geeignete und zugleich genug generische Portalarchitektur aussehen soll. Welche Funktionen muss sie anbieten, welche Komponenten soll sie umfassen, wie sollen diese zusammenwirken? Dabei ist es hilfreich, sich an grundlegenden funktionalen Portaltypen zu orientieren, wie Informations-, Transaktions- und Kollaborationsportal.

- Ein Informationsportal definiert den Zugriff auf aggregierte und allenfalls personalisierte Informationen.
- Ein Transaktionsportal erlaubt dem Benutzer, Transaktionen im Rahmen von Services auszulösen und damit Informationen an das Unternehmen zu übermitteln.
- Ein Kollaborationsportal ermöglicht es Benutzern, Aufgaben und Inhalte miteinander zu teilen und gemeinsam zu bearbeiten.

Meist umfasst das gewünschte Enterprise-Portal mehrere dieser Typen gleichzeitig. Die einzelnen Typen erfordern jedoch spezifische Komponenten und bringen Implikationen bezüglich Architektur, aber auch bezüglich Organisation, Marketing und Governance mit sich.

Ein Enterprise-Portal umfasst meist mehrere Portaltypen gleichzeitig.

Bausteine identifizieren

Anhand dieses Rasters lassen sich die benötigten Portalbausteine zuverlässig identifizieren und eine bedürfnisgerechte Architektur definieren. Portalbausteine können dabei nicht nur konkrete Systeme sein, sondern auch Konzepte oder Guidelines.

Typische Portalbausteine sind:

- Eine serviceorientierte Architektur (SOA) auf der Basis offener Standards und Schnittstellen für die nahtlose Integration des Portals in die IT-Landschaft und die einfache Einbindung weiterer Applikationen und Dienste
- Ein Sicherheitsframework mit einer zentralen Identity- und Access-Management-Infrastruktur, mit dem man Benutzer, Rollen und Berechtigungen effizient verwalten und das Portal einfach neuen Benutzergruppen zugänglich machen kann
- Eine einheitliche Benutzeroberfläche mit hoher Usability

Aus den Abhängigkeiten und der Priorisierung der Bausteine lässt sich eine Roadmap gewinnen.

Ermittelt man zusätzlich die Abhängigkeiten zwischen den Bausteinen und priorisiert die Bausteine entsprechend, gewinnt man eine Portal-Roadmap, entlang der sich das Portal Baustein um Baustein realisieren lässt. Dabei können gewisse Bausteine aus bestehenden Komponenten realisiert und die Basisinfrastruktur gezielt von Applikationsbausteinen getrennt und schon vorgängig umgesetzt werden.

In die Zukunft investieren

Um die heterogene Applikations- und Servicelandschaft von Organisationen und Unternehmen in einem Enterprise-Portal zu integrieren und die Anwender an Bord zu holen, sind ein flexibles Sicherheits- und Integrationsframework und viel technisches Knowhow gefragt. Vor allem aber braucht es Erfahrung und ein pragmatisches Vorgehen, um die Anforderungen ausgehend vom Bestehenden und unter Wahl der richtigen Komponenten entlang einer Roadmap Baustein um Baustein umzusetzen.

Pascal Buchbinder

Pascal Buchbinder, Elektroingenieur HTL, befasst sich seit langem mit Themen rund um die Sicherheit von Webapplikationen. Seit April 2010 betreut er als technischer Projektleiter die Weiterentwicklung des Security-Frameworks Nevis und bringt sein Fachwissen in vielfältige Portalprojekte ein. Seine sozialen, kulturellen und sportlichen Bedürfnisse stillt er mit Familie, Fotografie und Mountainbiking.

Gábor Ginter

Gábor Ginter hat 2004 sein Studium als Wirtschaftsinformatiker an der Universität Szeged in Ungarn abgeschlossen und ist seit 2005 bei der AdNovum Hungary Kft. in Budapest tätig. Er arbeitet in diversen Projekten für staatliche Stellen, Telekommunikationsfirmen und Banken mit. Als Ansprechperson im ungarischen Team für die Entwickler in der Schweiz übernimmt er dabei neu auch Führungsverantwortung. Unlängst hat er für ein Enterprise-Portal eine hoch komfortable, intuitiv bedienbare Benutzeroberfläche entwickelt. In seiner Freizeit tobt er sich gerne an Simulator- und Rollenspiel-Computergames aus.

Gábor Ginter entwickelt smarte Oberflächen für Portale.

Enterprise-Portal als Business Enabler

Ohne Portal macht heute kein Unternehmen mehr Business. Christof Dornbierer, CTO, und Tom Sprenger, CIO und Head of IT Consulting, über Stolpersteine und Potentiale bei der Umsetzung von Portalprojekten.

Was ist ein Enterprise-Portal?

Ch.D.: Der Begriff Enterprise-Portal ist überladen. Er wird für alles Mögliche von der Linksammlung bis hin zum umfassenden Unternehmensportal verwendet. Unternehmensportale werden je nach Ausprägung auch als Informations-, Transaktions- oder Kollaborationsportale bezeichnet. Informationsportale bieten einen einheitlichen Zugriff auf die Informationen und Dienstleistungen eines Unternehmens, Transaktionsportale bilden Businessprozesse ab und Kollaborationsportale dienen dem Wissensaustausch zwischen verschiedenen Anspruchsgruppen, typischerweise Mitarbeitenden, Kunden und Partnern. Aus unserer Sicht sind diese verschiedenen Portaltypen Teilaspekte eines übergreifenden Enterprise-Portals.

Kann ein Enterprise-Portal all diese Aspekte umfassen?

T.Sp.: Prinzipiell schon, allerdings ist das nicht in jedem Fall sinnvoll. Was genau über ein Enterprise-Portal angeboten wird, hängt letztlich vom Dienstleistungsangebot des Unternehmens ab. Portale können zudem auch firmenexterne Daten und Dienstleistungen integrieren. Ein Enterprise-Portal vereint alle Informationen und Dienstleistungen unter einem Dach, die ein Unternehmen internen und externen Nutzern zur Verfügung stellen möchte. Wichtig ist aus unserer Sicht vor allem, wie diese Elemente integriert werden, also Aspekte wie Portalarchitektur und Sicherheit.

> Am Beispiel E-Banking lässt sich die Entwicklung vom Service zum Portal schön aufzeigen.

Und was bringt ein Enterprise-Portal den Nutzern?

Ch.D.: Portale bieten heute wesentlich mehr Möglichkeiten als früher. Ein gutes Beispiel dafür sind Logistiklösungen, zum Beispiel bei der Post. Früher haben wir ein Paket zur Post gebracht und darauf vertraut, dass das Paket ankommt. Heute können wir den Weg des Pakets verfolgen, von der Aufgabe über die Sortieranlage bis hin zur Zustellung. Wir erhalten damit als Kunden über das Portal der Post gezielten Zugriff auf Informationen aus postinternen Prozessen.

> Compliance ist um Faktoren schwieriger zu gewährleisten, wenn Kunden direkt auf die Daten zugreifen.

Auch die Inhalte sind dynamischer geworden. Früher boten ein Portal oder eine Website lediglich Informationen an. Heute können wir dort dynamisch Informationen zusammenstellen und unter Umständen auch in die Prozesse eingreifen, zum Beispiel durch Umleiten von Paketen.

Ein weiterer Aspekt ist Personalisierung. Als Nutzer können wir heute Portale so einrichten, dass sie exakt unseren Bedürfnissen entsprechen, und Unternehmen stellen Informationen und Dienste verschiedenen Benutzergruppen in der jeweils passenden Form bereit.

T.Sp.: Am Beispiel E-Banking lässt sich die Entwicklung vom Service zum Portal schön aufzeigen. In den Anfangszeiten meinten wir mit E-Banking die E-Banking-Applikation. Wir konnten dort einfache Bankgeschäfte selbst tätigen. Heute meinen wir mit E-Banking das E-Banking-Portal, in dem wir aktuelle Kurs- und Analysteninformationen abrufen, mit Aktien handeln oder Konten eröffnen.

Als Kunden nehmen wir die Grenze zwischen Information und Service nicht mehr wahr. Wir sind Teil des Systems und partizipieren an der Weiterentwicklung von Systemen und Produkten. Einerseits aktiv, indem wir zum Beispiel Produkte bewerten, andererseits allein schon dadurch, dass wir die Systeme benutzen. Unser Klickverhalten wird laufend ausgewertet und die Systeme lernen daraus.

Damit verschieben sich ja eigentlich die Grenzen des Systems, das heisst, man kann nicht mehr einfach zwischen innerhalb und ausserhalb des Unternehmens unterscheiden. Was bedeutet das für Unternehmen?

Ch.D.: Ein Innen und ein Aussen gibt es nach wie vor, doch entscheidet darüber nicht mehr die Firmenzugehörigkeit, sondern die Rolle des Benutzers in Bezug auf den Geschäftsprozess. Dadurch steigt bei der Umsetzung von Portallösungen die Integrationstiefe. Unternehmen müssen den Zugriff auf Informationen und Dienstleistungen bis ins Detail sauber regeln. Dabei müssen in einem ersten Schritt Fragen geklärt werden wie «Wer darf was machen?», «Wer ist in welche Prozesse wie involviert?».

T.Sp.: Damit wären wir dann beim Thema Compliance, bei den regulatorischen Auflagen, die ein Unternehmen erfüllen muss. Es muss nachweisen können, wer zu welchem Zeitpunkt auf welche Informationen Zugriff hatte. In gewachsenen Systemlandschaften ist dies meist schwierig. Und wenn Kunden direkt auf die Daten zugreifen können, wird es noch um Faktoren komplexer, als wenn Daten nur intern verwaltet werden.

Gibt es Qualitätskriterien für Portallösungen? Was macht ein gutes Portal aus?

T.Sp.: Aus funktionaler Sicht stehen Business Alignment und Business Enabling im Vordergrund. Je besser ein Portal die unternehmensspezifischen Geschäftsprozesse unterstützt und bündelt, desto mehr bringt es dem Unternehmen. Deshalb ermutigen wir als IT-Berater den Kunden dazu, zuerst eine Portalvision zu entwickeln. Das Vorgehen ist immer gleich. Wir klären mit dem Business die Zielsetzungen und schauen, wo die Prioritäten liegen. Danach schauen wir uns das technische Umfeld an und zeigen im Dialog mit Business und IT Umsetzungsvarianten auf.

Klingt eigentlich recht simpel. Und doch scheitern Portalprojekte oft. Weshalb?

T.Sp.: Ich sehe im Wesentlichen zwei Gründe. Zum einen scheitern Portalprojekte, weil vorausgehend nicht hinreichend geklärt wird, welche geschäftlichen Ziele mit der Lösung erreicht werden sollen. Business Alignment und Business Enabling sind dadurch ungenügend. Zum anderen können technologische Gründe ein Portalprojekt zu Fall bringen. So kann es passieren, dass ein Unternehmen ein Portalprodukt einführt und nach der Einführung merkt, dass sich die Servicelandschaft hinter dem Portal anders entwickelt hat, als zum Zeitpunkt der Evaluation angenommen wurde. Als Resultat ist dann unter Umständen die Produktlösung technologisch nicht kompatibel mit den Applikationen, die sie integrieren soll.

Ch.D.: Ein weiterer Stolperstein ist die Benutzerakzeptanz. Portalprojekte verändern typischerweise die Art und Weise, in der Menschen zusammenarbeiten. Sie bringen eine Standardisierung von Abläufen. Und Menschen mögen es nicht, wenn ein Projekt oder eine Software sie zwingt, ihre Arbeitsabläufe zu ändern. Darum müssen wir uns bei der Einführung einer Portallösung genau überlegen, was es für die Benutzer bedeutet. Das Portal muss allen einen spürbaren Mehrwert bringen, sonst wird es sabotiert und umgangen. Hier sind wir wieder beim Fokus auf den echten Nutzen. Es ist nicht unbedingt sinnvoll, coole Features einzuführen, die niemandem etwas bringen.

> Als IT-Berater ermutigen wir den Kunden dazu, zuerst eine Portalvision zu entwickeln.

> Menschen mögen es nicht, wenn eine Software sie zwingt, ihre Arbeitsabläufe zu ändern.

Die wichtigste Voraussetzung ist also, dass Ziele und Nutzen geklärt sind. Und dann? Wie geht ihr bei der architektonischen Ausgestaltung vor?

Ch.D.: Das kommt auf die Situation an. Hat das Unternehmen bis jetzt nur auf einer Website Informationen online geschaltet und kommt zu uns, weil es eine Portallösung einführen möchte? Oder hat es bereits versucht, eine Portallösung einzuführen, und ist mit der Lösung nicht zufrieden? Oder hat es bereits diverse kleine Portale oder Systeme im Internet stehen, die es miteinander verbinden will?

T.Sp.: Letzteres ist eigentlich der Normalfall. Meistens liegen die Informationen in verschiedenen, nicht miteinander verbundenen Systemen. Der Datenabgleich erfolgt über organisatorische Prozesse. Ab einem gewissen Umfang funktioniert das dann so nicht mehr. Es impliziert, dass gewisse Informationen redundant vorhanden sind, was Mehraufwand bedeutet und die Datenintegrität gefährdet. Ein weiteres Thema ist hier die Sicherheit. Werden verschiedene Services separat ins Internet geschaltet, besteht die Gefahr, dass niemand mehr die Übersicht hat. Damit werden unter Umständen kritische Informationen für Benutzer sichtbar, für die sie nicht bestimmt sind.

Also doch nicht so simpel. Wie gelingt es euch, in einem solchen Fall den Überblick zu gewinnen?

T.Sp.: Wir teilen das Projekt in kleinere, überschaubare Pakete auf und setzen diese dann eines nach dem anderen in der geeigneten Reihenfolge um. Wichtig dabei ist, bei der architektonischen Ausgestaltung die Ziele im Auge zu behalten und sich bei jeder

Geballte Erfahrung: Christof Dornbierer (links) und Tom Sprenger haben in Portalprojekten schon alles Mögliche integriert.

Entscheidung an diesen Zielen zu orientieren. Hier hilft uns unsere langjährige Erfahrung im Umgang mit grossen Projekten.

Ch.D.: Ja, die Erfahrung ist sicher ein wichtiger Faktor. Sie sagt uns auch, dass Portallösungen langfristig ausgerichtet sein und Raum für Innovation und Ausbau bieten sollten. Es ist weder interessant noch sinnvoll, immer wieder von vorn zu beginnen. Deshalb haben wir einen Technologiebaukasten mit bewährten Komponenten zusammengestellt. Er enthält sowohl bewährte Open-Source-Komponenten wie auch kommerzielle Produkte und wird mit jedem Projekt reicher. Falls notwendig bauen wir auch proprietäre Komponenten, zum Beispiel um vorhandene Systeme effizient integrieren zu können. Wir schauen einfach möglichst genau, wohin der Kunde will und was er bereits hat – und nehmen dann das, was am besten passt.

Wie muss ich mir diesen Technologiebaukasten vorstellen?

Ch.D.: Der Technologiebaukasten enthält einerseits Softwarekomponenten wie etwa Komponenten für die Verwaltung von Zugriffsrechten, Credentials und Applikationen. Andererseits enthält er auch konzeptionelle Komponenten wie etwa einen Bauplan, eine typische Portalarchitektur. Die Architektur dient als Leitplanke, sie soll aufzeigen, was wir berücksichtigen müssen.

Mit einer guten Roadmap zahlen sich Investitionen selbst dann aus, wenn sich die Ziele verändern.

Weiter enthält der Baukasten Best Practices zum Vorgehen beim Aufbau eines Portals. Wie fange ich an? Welche Basisinfrastruktur brauche ich? Welche Abhängigkeiten gibt es? Was muss ich zuerst machen? Wie gehe ich bei der Umsetzung vor? Entscheidend ist hier nicht nur die Architektur, also der Bauplan, sondern auch der zeitliche Aspekt, die Planung.

T.Sp.: Ja, das ist ein wichtiger Punkt. Die Umsetzung erfordert bei grossen Projekten zwingend eine evolutionäre Roadmap. Sie muss gestaffelt entlang von klar formulierten Meilensteinen erfolgen. Und wir müssen bei der Planung berücksichtigen, dass sich die Ziele während der Umsetzung verändern können, zum Beispiel wegen Entwicklungen am Markt oder technologischer Neuerungen. Eine gute Roadmap sorgt dafür, dass sich bereits getätigte Investitionen in solchen Fällen trotzdem auszahlen.

Christof Dornbierer

Christof Dornbierer, dipl. Informatikingenieur ETH und seit 2004 bei AdNovum, spielte eine tragende Rolle bei der Entwicklung des AdNovum-eigenen Sicherheitsframeworks Nevis, das in Portalprojekten seit vielen Jahren erfolgreich eingesetzt wird. Seit August 2008 ist er CTO und Mitglied der Geschäftsleitung von AdNovum und heute für die Bereiche Application Engineering, Product Engineering und Quality Management verantwortlich. In seiner Freizeit ist er öfter draussen anzutreffen, sei es zu Fuss oder auf dem Velo.

Dr. Tom Sprenger

Dr. Tom Sprenger, dipl. Informatikingenieur ETH und seit 2001 bei AdNovum, leitete von 2002 bis 2004 die AdNovum-Niederlassung in San Mateo (USA). Nach seiner Rückkehr nach Zürich engagierte er sich in der Qualitätssicherung und baute den Bereich Quality Management auf. Seit 2007 ist Tom Sprenger CIO und Mitglied der Geschäftsleitung und heute für den Ausbau der Dienstleistungsbereiche IT Consulting und Application Management von AdNovum verantwortlich. Privat stürzt er sich gerne in Vollmontur auf seinem Mountainbike die Singletrails hinunter.

Autorisierung zentral steuern

AdNovum hatte jüngst Gelegenheit, ein Autorisierungs-Management-System für ein Gesundheits-Enterprise-Portal zu bauen. Welche Form der Autorisierung soll auf welcher Stufe erfolgen? Wo werden die Regeln definiert, wo durchgesetzt?

Von Moritz Kuhn und Andreas Petralia

Enterprise-Portale ermöglichen Mitarbeitern, Kunden und Lieferanten den Zugang in die Informationswelt des Unternehmens und gegebenenfalls auch das Mitwirken an dessen Prozessen. Sie sind dynamische Gebilde und deshalb mit Vorteil modular aufgebaut. Ein wichtiger Baustein neben Personalisierung, Service, Integration und Content ist dabei die Security. Der Baustein Security beinhaltet Authentisierung, Autorisierung, Access Control und Auditing. Bei grösseren Systemen wie Enterprise-Portalen gibt es unterschiedliche Ansätze, wie solche Basisfunktionalitäten integriert werden. Dabei stellen sich folgende Fragen:

- Wo wird der Benutzer authentifiziert, der Zugriff autorisiert und diese Entscheidung durchgesetzt (Authentisierung – Autorisierung – Access Control)?
- Wo fallen die Auditdaten an und wo werden sie abgespeichert (Auditing)?

Im Folgenden werden diese Fragen sowohl aus einer theoretischen als auch aus einer praktischen Sicht anhand eines konkreten Beispiels beleuchtet. Wir fokussieren dabei auf die Basisfunktionalitäten Autorisierung und Access Control.

> Enterprise-Portale sind dynamische Gebilde und deshalb mit Vorteil modular aufgebaut.

Praxisbeispiel e-toile

e-toile ist ein Informatik-Grossprojekt im Gesundheitswesen, das sich zurzeit im Kanton Genf in Vorbereitung befindet. Ziel des Projekts ist es, den Zugriff auf medizinische Daten über organisatorische Grenzen hinweg kontrollierbar zu machen. Nur so lässt sich die Einhaltung gesetzlicher Vorgaben (Compliance) gewährleisten. Um dies zu erreichen, sollen Authentisierung, Autorisierung und Auditing zentralisiert werden, während Access Control verteilt direkt in den teilnehmenden Organisationen stattfindet. Für das Projekt hat der Kanton Genf die Schweizerische Post als Generalunternehmer beauftragt, die ihrerseits in Sicherheitsfragen mit AdNovum zusammenarbeitet. Doch zunächst zur Theorie.

Formen der Autorisierung

Wir unterscheiden verschiedene Formen der Autorisierung:

- *Grobautorisierung findet auf der Ebene von Applikationen statt. Sie regelt zum Beispiel, ob ein Benutzer berechtigt ist, eine Applikation oder einen Teil einer Applikation zu verwenden.*
- *Funktionale Autorisierung regelt Zugriffe auf der Ebene von Operationen und wird häufig als Role Based Access Control umgesetzt (Beispiel: Nur Benutzer, die der Gruppe Supervisor angehören, dürfen die Operation «Daten löschen» durchführen).*
- *Kontextbezogene Feinautorisierung bezieht neben Informationen über die Operation beliebige Kontextmerkmale in die Autorisierungsentscheidungen mit ein. Diese Merkmale beschreiben meist das Subject, das die Operation ausführt, und die Daten, auf denen die Operation ausgeführt werden soll.*

> Das Ziel ist der kontrollierte Zugriff auf medizinische Daten über organisatorische Grenzen hinweg.

Die theoretische Sicht: Authentisierung ...

Für die Authentisierung wird meist ein zentraler Service verwendet. Dieser integriert verschiedenste Verfahren, um Benutzer sicher zu authentifizieren und ihnen ein Token (digitale Identität) auszustellen, etwa in Form einer SAML Assertion. Die digitale Identität können alle in das Portal integrierten Applikationen verwenden, womit eine separate Authentisierung pro Applikation entfällt. So wird die Komplexität der Applikationen reduziert und gleichzeitig deren Sicherheit erhöht. Soll ein neues Authentisierungsverfahren eingeführt werden, muss dies nur vom zentralen Authentisierungsdienst unterstützt werden.

... versus Autorisierung und Access Control

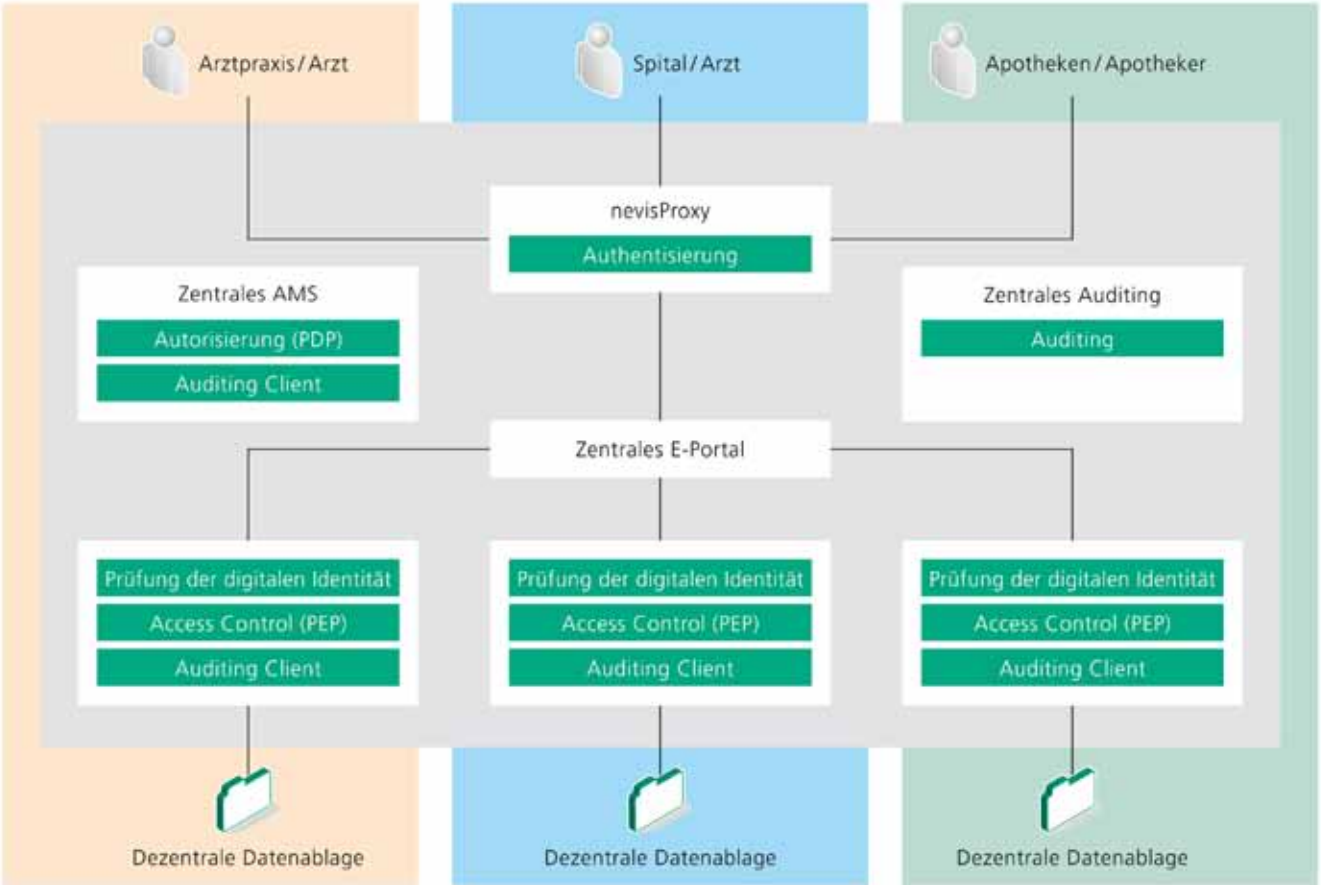
Demgegenüber wird bei der Autorisierung maximal die Grobautorisierung (s. auch Kasten) zentral gesteuert. Die Feinautorisierung bleibt Aufgabe der Applikationen. Zwar bieten viele Frameworks Unterstützung für Verfahren wie Role Based Access Control (RBAC), doch sind diese auf funktionale Autorisierung beschränkt und werden in der Applikation implementiert. Die enge Verknüpfung von Autorisierungslogik mit Applikationscode, etwa bei der Zuordnung von Rollen zu Berechtigungen, hat aber gerade für Enterprise-Portale Nachteile.

Sie ist der Grund für die aktuell verbreitete Praxis, dass jede Applikation die Autorisierung selber managt, indem sie eine implizite Security Policy implementiert. Änderungen an dieser Policy

> Gemäss verbreiteter Praxis implementiert jede Applikation implizit eine eigene Security Policy.

– zum Beispiel eine neue Zuordnung von Rollen zu Berechtigungen – sind somit aufwändig, teuer und fehleranfällig. Ausserdem ist es fast unmöglich, eine konsolidierte, unternehmensweite Sicht der effektiven Sicherheitsregeln und damit der Security Policy zu erhalten.

Bei Autorisierung und Access Control stellen sich also Herausforderungen, für die bei der Benutzerauthentifizierung bereits generische Lösungen bestehen: die Entflechtung von Business- und Autorisierungslogik, eine zentrale Verwaltung der Autorisierungs-Policy und ein generischer Mechanismus für die kontextbezogene Feinautorisierung.



Zentrale und dezentrale Komponenten des Autorisierungs-Management-Systems bei e-toile.

Vielversprechender Ansatz XACML

Genau diese Ziele verfolgt der OASIS-Standard XACML, die «eXtensible Access Control Markup Language». Er definiert eine deklarative Access-Control-Policy-Sprache, ein Entscheidungsmodell für diese Policies sowie eine verteilte Autorisierungs- und Access-Control-Architektur.

Die zentrale Komponente der XACML-Architektur ist der Policy Decision Point (PDP). Der PDP wertet Autorisierungsanfragen (XACML Requests) basierend auf ihren Attributen und einer XACML Security Policy aus. Ein XACML-Autorisierungs-Request enthält Informationen über das Subject, die Action, die Resource(s) und das Environment:

- Das Subject beschreibt die Identität des Aufrufers. Es beinhaltet typischerweise Attribute für die User-ID, Benutzergruppen oder User-Session.
- Die Action entspricht der Operation, die das Subject ausführen möchte.
- Die Resource ist das Objekt, auf dem das Subject die Action durchführen will.
- Das Environment enthält beispielsweise Attribute zu Ort oder Zeit des XACML Request.

Neben einer Resource-ID können Resources, wie auch Subject, Action und Environment, mit beliebigen weiteren applikationsspezifischen Attributen beschrieben werden, etwa einem Confidentiality Code.

Der OASIS-Standard XACML definiert eine Sprache und ein Entscheidungsmodell für die Access Control Policies.

XACML-Autorisierungs-Requests werden durch Policy Enforcement Points (PEP) gestellt. PEPs sind verteilte Access-Control-Komponenten, die Autorisierungsentscheidungen eines PDP durchsetzen. Sie lassen sich in alle Schichten einer Applikation integrieren und über grosse IT-Systeme verteilen. Dazu können PEPs die unterschiedlichsten Formen annehmen, sie können zum Beispiel ein Teil einer Web Service Handler Chain, ein JSF Action Listener oder ein Reverse Proxy sein.

Wenn aus Theorie Praxis wird

Im Projekt e-toile lag es nahe, Autorisierung und Access Control auf dem XACML-Standard aufzubauen. In e-toile werden primär die Zugriffe auf die elektronischen Patientendokumente autorisiert. Diese Dokumente sind dezentral in Repositories verschiedener Organisationen gespeichert. Zusätzlich besteht eine Registry über die Dokumenten-Metadaten. Das zentrale Autorisierungs-Management-System (AMS) implementiert einen PDP auf Basis XACML. Die PEPs – ebenfalls Teil der Autorisierungs-Management-Lösung – wurden als leichtgewichtige Reverse Proxies entwickelt und direkt vor den Dokumenten-Repositories und der Registry positioniert. Alle Zugriffe müssen einen PEP passieren. Die PEPs filtern die Abfrageergebnisse gemäss den Autorisierungsentscheidungen des AMS.

Mit zentraler Autorisierung stellt e-toile sicher, dass in allen Organisationen dieselbe Security Policy gilt.

Die drei besonderen Herausforderungen bei Autorisierung und Access Control hat AdNovum in der AMS-Lösung für e-toile erfolgreich adressiert:

Entflechtung von Business- und Autorisierungslogik

Vergleichbar mit zentralen Authentisierungsdiensten bietet das AMS zentrale Autorisierung als Basisfunktionalität für beliebige Applikationen. Dies erlaubte es uns, die Autorisierungslogik komplett von der Businesslogik zu trennen. Zusätzlich konnten wir in e-toile die Access-Control-Logik von den Businessapplikationen entkoppeln. Der Vorteil: Änderungen bei Autorisierung und Access Control betreffen die Businessapplikationen nicht direkt und umgekehrt. Das vereinfacht und vergünstigt die (Weiter-) Entwicklung und Wartung der Komponenten.

Zentrale Verwaltung der Autorisierungs-Policy

Dank der zentralisierten Autorisierung konnten wir sicherstellen, dass in allen Organisationen stets dieselbe Security Policy für Dokumentenzugriffe gilt. Die Security Policy wird nicht implizit durch die Implementierung im Applikationscode verteilt, sondern liegt als explizite Policy an zentraler Stelle. Dies ermöglicht ein vereinfachtes Auditing und Testing. In Verbindung mit einem zentralen Audit-Log werden Autorisierungsentscheidungen so besser nachvollziehbar. Durch die Zentralisierung lässt sich die Policy zudem einfach an neue Anforderungen anpassen. So kann zum Beispiel die Zuordnung von Rollen zu Berechtigungen während der Laufzeit geändert werden. Solche Änderungen werden sofort in allen Policy Enforcement Points wirksam.

Kontextbezogene Feinautorisierung

Das XACML-Autorisierungsmodell, wie AdNovum es in Zusammenarbeit mit der Schweizerischen Post im Projekt e-toile umgesetzt hat, ist ausgesprochen vielseitig und geht weit über Role Based Access Control und funktionale Autorisierung hinaus. Die e-toile Security Policy regelt detailliert, unter welchen Bedingungen und in welchen Situationen ein Arzt auf ein Patientendokument zugreifen darf. In jede Autorisierungsentscheidung fliessen neben Informationen über die Action rund 15 kontextabhängige

Andreas Petralia (links) und Moritz Kuhn haben für ein Gesundheits-Enterprise-Portal ein Autorisierungs-Management-System gebaut.

Kriterien ein. Darunter befinden sich Informationen über das Patienten-Arzt-Verhältnis (Arzt des Vertrauens, Blacklisting usw.), das Dokument (Autor, Empfänger, Confidentiality Code usw.) und die Behandlungssituation (z.B. Notfall). In XACML Policies können beliebige kontextbasierte Merkmale und generische Claims verwendet und flexibel verknüpft werden.

Die e-toile Security Policy regelt im Detail, in welchen Situationen ein Arzt auf ein Patientendokument zugreifen darf.

Der Ansatz eines portalweiten Autorisierungs-Management-Systems mit zentralen und verteilten Komponenten hat sich in der Praxis bestens bewährt. Den Kunden von AdNovum empfehlen wir deshalb, eine solche Lösung in Architekturentscheidungen mit einzubeziehen.

Moritz Kuhn

Moritz Kuhn betreut das Projekt e-toile als technischer Projektleiter. Er ist Master of Science in Computer Science ETH und arbeitet seit drei Jahren bei der AdNovum. Zunächst begann er als Entwickler in Middleware- und IT-Security-Projekten. Heute ist er als Consultant und technischer Projektleiter tätig. Seine Freizeit verbringt Moritz Kuhn am liebsten mit seiner Familie. Zudem engagiert er sich als Kirchenpfleger.

Andreas Petralia

Andreas Petralia betreut das Projekt e-toile als Business-Projektleiter. Er ist dipl. Elektroingenieur ETH und arbeitet seit acht Jahren bei der AdNovum. Sein IT-Security-Knowhow festigte er als Entwickler von Middleware und bei Security-Projekten. Heute arbeitet Andreas Petralia als Senior Consultant in der Businessunit IT Consulting. Privat verbringt er viel Zeit mit seinen beiden Töchtern und lässt beim Squashen überschüssige Energie ab.

Web-Informationsflüsse nachvollziehbar machen

Moderne Portale bieten eine personalisierte Kombination von Informationen und Bedienmöglichkeiten. Nachvollziehbarkeit und Archivierung der Informationsflüsse sind aber noch praktisch nirgends geregelt. Dafür sind neue Lösungen gefragt.

Von Jürg Truniger, qumram gmbh

In den 20 Jahren seines Bestehens haben sich das Internet und die verschiedenen Webtechnologien enorm verbreitet. Informationen und Transaktionen zwischen Firmen, Kunden und Geschäftspartnern, zwischen staatlichen Institutionen und Bürgern, aber auch innerhalb von Organisationen werden grossteils online ausgetauscht und abgewickelt. Ein Ende dieses Trends ist nicht abzusehen.

Herausforderung Nachvollziehbarkeit

Immer relevantere und kritischere Geschäftsprozesse laufen über den Online-Kanal. Damit steigen die Anforderungen hinsichtlich Vollständigkeit und Nachvollziehbarkeit der Informationsflüsse. Die heutigen Informationssysteme stellt dies vor erhebliche Herausforderungen, hauptsächlich aus zwei Gründen:

Zum einen ist ein Grossteil der von den Webplattformen ausgelieferten Webpages dynamisch und entsteht erst durch die Interaktion mit dem Benutzer oder Kunden. Enterprise-Portale

Dynamische Webpages entstehen erst durch die Interaktion mit dem Benutzer.

stellen den Benutzern in ihren Webbrowsern Informationen und Applikationen zur Verfügung, die gezielt auf ihre individuellen Bedürfnisse oder die Gegebenheiten eines bestimmten Geschäftsprozesses optimiert sind. Die Inhalte werden in gewünschter Kombination direkt im Browser der Benutzer aggregiert und aufbereitet, immer häufiger in Echtzeit. Eine vollständige Sicht der relevanten Informationen wird dabei also einzig in den Webbrowsern erzeugt. Zweitens stammen die dargestellten Informationen und Transaktionen aus den unterschiedlichsten Quellsystemen. Diese bilden in der Regel eine heterogene Applikations- und Systemlandschaft und oft wird ein Teil davon durch externe Outsourcer oder in der Cloud betrieben.

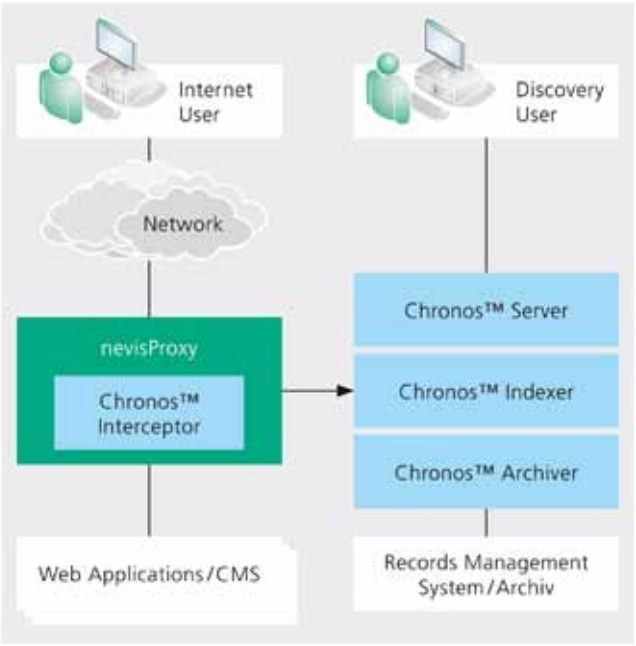
Die geforderte userspezifische Aggregation der Informationen lässt sich somit auf Ebene der Backends nicht bewerkstelligen. Dort lässt es sich schlicht nicht im Detail nachvollziehen, welche Informationen und Transaktionen in ihrer Kombination dem Kunden angezeigt werden.

Richtlinien einhalten auf allen Kanälen

Wird eine Information aufgrund ihrer Verbindlichkeit als aufbewahrungspflichtig klassifiziert, ist sie entsprechend zu behandeln, egal ob sie in einem Bundesordner abgelegt oder beispielsweise auf einem Intranet-Portal veröffentlicht ist. Im Online-Kanal werden die Aufbewahrungsvorschriften jedoch noch kaum umgesetzt, unter anderem aus dem praktischen Grund, dass es bis anhin keine entsprechenden Lösungen gab.

Über qumram GmbH

qumram ist ein junges Unternehmen, das sich auf die Archivierung von Webcontent spezialisiert. Webcontent wird immer wichtiger und unterliegt denselben Anforderungen bezüglich Aufbewahrung und Archivierung wie Dokumente oder E-Mails. qumram stellt sicher, dass Websites und Webapplikationen auch nach Jahren noch in Originalform reproduziert werden können. Ähnlich einer Time Machine ermöglichen es die qumram-Produkte dem Benutzer, sich die ganze Website zu einem beliebigen Zeitpunkt in der Vergangenheit anzusehen – und das inklusive personalisierter Inhalte und Webapplikationen.
www.qumram.ch



Archivierung von Web-Informationsflüssen mittels Nevis und der Chronos-Suite.

Besonders grosser Handlungsbedarf besteht bei Unternehmen und Organisationen, die mit einer hohen Regulierungsdichte bzw. mit einer Vielzahl von Compliance-Anforderungen konfrontiert sind, wie Finanz- und Pharmaunternehmen oder behördliche Institutionen.

Den Datenstrom aufzeichnen

Um Nachvollziehbarkeit und damit Informationssicherheit zu gewährleisten, sind Webinhalte exakt so aufzubewahren, wie sie dem Endnutzer präsentiert werden. Erreicht wird dies durch die lückenlose Aufzeichnung des Datenstroms zwischen dem ausliefernden Webserver und dem Webbrowser des Endusers.

WEBINHALTE SIND SO AUFZUBEWAHREN, WIE DER ENDNUTZER SIE SIEHT.

Dafür bietet das Security-Framework Nevis von AdNovum eine ideale Plattform. Für die gezielte Aufzeichnung und Analyse der Daten hat qumram (s. Kasten S. 15) den Chronos Interceptor entwickelt. Der Chronos Interceptor wird von qumram zusammen mit ergänzenden Modulen in einer Softwaresuite angeboten und ist auch in Nevis integriert.

Intelligent und parametrierbar

Die Chronos-Suite bietet neben der Erfassung des Datenstroms umfassende Möglichkeiten, die aufgezeichneten Informationen auf intelligente Art weiterzuverarbeiten. Der vollständig parametrierbare Indizierungsservice (Chronos Indexer) bezieht die aufgezeichneten Daten auf asynchrone Weise und prüft auf Basis des Modifikationsdatums bzw. mittels Prüfsummenchecks, ob eine Webseite – der gesamte HTML-Code inkl. Bildern usw. – bereits archiviert ist. Er fügt nur dann eine neue Version hinzu, wenn er eine inhaltliche Änderung feststellt. Das System speichert dann nur die Änderungen und braucht damit wenig Speicherplatz. Der Chronos Indexer übernimmt bei Bedarf auch die Erstellung zusätzlicher Repräsentationen der Seiten, beispielsweise im PDF/A-Format. Er ist zudem in der Lage, vorab definierte Bereiche einer Website bzw. eines Portals gezielt von einer Archivierung auszuschliessen.

Vor der Übergabe an ein Repository oder elektronisches Archiv reichert der Chronos Indexer die zu archivierenden Webseiten mit frei definierbaren Metadaten an. Die Seiten lassen sich damit automatisch klassifizieren, was wiederum die Zuordnung zu einem Geschäftsdossier oder Ordnungssystem gewährleistet.

Bereit für den globalen Einsatz

Mit der kombinierten Nutzung von Nevis und Chronos können Unternehmen die Verbindlichkeit und Nachvollziehbarkeit der Online-Informationsflüsse mit geringstmöglicher Anpassung an den bestehenden IT-Systemen realisieren. Die Lösung speichert die Daten in Originalform und somit technologieunabhängig. Sie kann heterogene und historisch gewachsene Systemlandschaften unabhängig von Laufzeitumgebungen und Plattformstrategien vollständig abdecken und eignet sich damit ideal für den globalen Einsatz.

Impressum

Herausgeber:
AdNovum Informatik AG
Corporate Communication
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:
Patrick Rohner, Zürich (Titel); Gerry Nitsch, Zürich (Porträts); Márton Magócsi, Budapest (Portrait Gábor Ginter)
Gedruckt auf Balance Pure FSC