



DOK.

Technologien, Strategien & Services für das digitale Dokument

Microblogging goes Business
Wissensnetze als Basis für Enterprise 2.0
Datenschutz für Kollaborationsprozesse



Enterprise Search: Der Schlüssel zum Wissen

Special: DMS EXPO

Ordnung vs. Chaos: Rollen und Rechte im Enterprise 2.0

Enterprise 2.0, Social Media, Rechteverwaltung, LDAP, Active Directory,
Freigabe-Workflows, Benutzerverwaltung

Enterprise 2.0 bezeichnet den Einsatz von Social Software, die aus dem Netz unter dem Begriff Web 2.0 bekannt ist, in professionellem Rahmen innerhalb von Unternehmen. Projektkoordination, Wissensmanagement sowie die Innen- und Außenkommunikation können damit verbessert werden. Die Kunst, diese Werkzeuge effizient einzusetzen, besteht darin, die Balance zwischen dem Mitmachchaos, bei dem „alle alles dürfen“, und einem restriktiven Informationsbunker herzustellen. Rollen, Rechte und Regeln – kurz R^3 – wohl bedacht vergeben, lautet dazu die Erfolgsformel.

Zwischen freiem Fluss des Wissens und dessen Austausch auf der einen und striktem Management auf der anderen Seite gilt es, eine Balance zu finden. Dazu gehört, den Dreisprung von Rollen, Rechten und Regeln – R^3 – zu beherrschen. Warum das so nötig ist, darauf weist die Definition von Enterprise 2.0 selbst hin: „Enterprise 2.0 bezeichnet den Einsatz von Sozialer Software zur Projektkoordination, zum Wissensmanagement und zur Innen- und Außenkommunikation in Unternehmen. Diese Werkzeuge fördern den freien Wissensaustausch unter den Mitarbeitern, sie erfordern ihn aber auch, um sinnvoll zu funktionieren. Der Begriff umfasst daher nicht nur die Tools selbst, sondern auch eine Tendenz der Unternehmenskultur – weg von der hierarchischen, zentralen Steuerung und hin zur autonomen Selbststeuerung von Teams, die von Managern eher moderiert als geführt werden.“ So steht es bei Wikipedia.

Moderierte Autonomie

Doch wie weit geht Autonomie und wie stringent ist die Moderation? Wann entsteht Chaos und wann würgen rigide Einschränkungen den freien Wissensaustausch ab? Darf ein Ergebnis aus einem internen Forschungsprojekt im Intranet veröffentlicht – neudeutsch gepostet – werden? Wohl kaum. Wer also darf was? Lesen, ändern, schreiben und löschen. Hier greift R^3 .

www.adenin.de

Martin Amm ist Vorstand der **Adenin Technologies AG**. Das Unternehmen mit Sitz in Nürnberg ist Anbieter von Intranet-Portal-Lösungen und vertreibt seine Technologiebasis weltweit. Über 100 Module der Suite IntelliEnterprise bilden im Intranet Organisations- und Informationsstrukturen ab.

In Rollen sind typische Funktionen im Unternehmen beschrieben, etwa Mitarbeiter im Vertrieb, in der Personalabteilung, Marketing, Controller oder Content-Verantwortlicher. Darüber hinaus können auch Benutzergruppen in Rollen definiert werden, die nicht zur ständigen festen Belegschaft einer Firma gehören: freier Mitarbeiter, Aushilfskräfte, Kunden oder Entwicklungspartner sind typische Beispiele. Im einfachen Fall hat ein Mitarbeiter eine oder mehrere Rollen, etwa Manager Vertrieb und Verkaufsinendienst. Entscheidend ist, dass Zugriffsrechte auf Dokumente nicht per Mitarbeiter, sondern per Rolle vergeben werden, da diese die Pflege insbesondere bei Mitarbeiterwechseln einfacher macht.

Rechte wiederum legen fest, was eine Rolle mit Informationen machen darf. Entscheidend dabei ist, dass Merkmale wie „anlegen“, „ändern“, „löschen“ oder „lesen von Informationen“ nicht an eine Person vergeben werden, sondern an eine Gruppe von Benutzern, die in Rollen zusammengefasst sind. Kurz: Nicht Herr Meyer darf, sondern die Rolle Personalreferent darf.

Aus mehreren Kriterien oder Merkmalen setzen sich schließlich Regeln zusammen. So kann aufgrund bestimmter Ereignisse, oder spezifischer Inhalte, eine Information gepostet werden. Häufig ist über Regeln festgelegt, wer Dokumente sehen darf und wie eine Freigabeprozedur – der Workflow – aussieht. Kurz: Welche Rolle im Unternehmen muss einen Content gelesen und geprüft haben, bevor er anderen zur Verfügung gestellt werden darf?

Bloß nicht den „Motor Wissen“ abwürgen

Genau an diesem Punkt geht ein Aufschrei durch die Gemeinde der Enterprise-2.0-Protagonisten: Kontrolle, Einschränkung, freies Web, ade!, hört man sie klagen. Der Wissensmotor wird abgewürgt, bevor er richtig auf Drehzahl gekommen ist. Doch die Welt ist nicht 2.0. Und daher kommen Unternehmen um ein Mindestmaß an Rechten, Rollen und Regeln nicht herum. Enter-

prise 2.0, so frei wie das Internet und gleichzeitig so sicher wie die Unternehmens-IT, muss die Devise daher lauten. Besonders hohe Anforderungen kommen durch Compliance-Richtlinien wie den Sarbanes Oxley Act (SOX) hinzu.

In der Praxis finden sich zwei Extreme, wie Enterprise 2.0 umgesetzt wird. In einem Teil der Unternehmen ist eine Art Überanalyse festzustellen, mit dem Erfolg, dass am Ende mehr Rollen als Mitarbeiter vorhanden sind. Die Folge davon: 80 Prozent der Rollen werden überhaupt nicht verwendet. Der zweite Weg ist der typische Wiki-Ansatz: Jeder darf alles. Beide führen jedoch nicht zum Ziel.

Im Vorfeld sollten Unternehmen daher zunächst grobe Informationsklassen bilden: einmal ausgehend von der Zielgruppe, wer darf was lesen, ändern und ergänzen. Daneben gilt es, inhaltlich Verantwortliche zu identifizieren. Ferner ist zu klären, ob Rollen und Rechte zentral oder dezentral zu pflegen sind. Daraus ergibt sich eine überschaubare Matrix mit Zuordnungen. Grundsätzlich sollte bei der Vergabe von Erlaubnissen etwas freizügiger vorgegangen und bei Bedarf dann nachträglich restriktiver eingegrenzt werden.

Betrachtet man das Thema Rollen und Rechte, wird sehr schnell klar, dass Unternehmen ihren Mitarbeitern – den Benutzern – bereits Rollen und Rechte beispielsweise in Directory-Systemen wie LDAP oder Active Directory (AD) zugewiesen haben. Weitere Profile etwa in ERP- oder CRM-Anwendungen kommen hinzu. Nun folgt durch Enterprise 2.0 noch eine weitere Möglichkeit, Rollen und Rechte etwa für ein Enterprise-Wiki zu vergeben. Jetzt hängt es von der Unternehmensstrategie ab, wie diese Merkmale zu pflegen und managen sind.

Zentral UND dezentral

Ist es allein die IT-Abteilung, die alle Benutzerdaten verwaltet, ist es vorteilhaft, wenn sich das Enterprise-2.0-Werkzeug in die vor-

Informations-Typ	Publizieren & Aktualisieren	Zugriff
Unternehmensnachrichten	Beschränkt z.B. Corporate Communications	Frei
Arbeitsanweisungen	Beschränkt	Frei
Projekt Collaboration	Frei für Projektmitarbeiter	Beschränkt auf Projektmitarbeiter
Markt- & Mitbewerbbeobachtung	Frei	Frei
Markt- & Mitbewerbbeobachtung	Beschränkt	Frei
Produktentwicklung	Beschränkt	Beschränkt
Wissensdatenbanken	Frei	Frei

Wer was darf: der Schlüssel zum Enterprise 2.0

Ein Benutzer hat eine oder mehrere Rollen. Eine oder mehrere Rollen haben ein oder mehrere Rechte und ein Dokument kann ein oder mehrere Regeln zum Zugriff haben. Quelle: Adenin

handene Landschaft integrieren lässt, um Benutzerdaten etwa vom AD oder LDAP zu nutzen. Dazu muss ein Abgleich von Rollen und Rechten (Synchronisation) aus bestehenden Systemen und der eigenen Benutzer- und Rollenverwaltung möglich sein. Das Wiki-Werkzeug greift dann auf Vorgaben beispielsweise aus dem LDAP zurück. Der Vorteil: Doppeleingaben entfallen, der Administrationsaufwand ist deutlich reduziert.

Trotz der Vorteile einer zentralen Pflege erlauben rund 60 Prozent der Unternehmen im Enterprise 2.0 ein dezentrales Rollen- und Rechtemanagement. Sinnvolle Gründe dafür gibt es viele: So besteht in Fachabteilungen häufig die Notwendigkeit, ad hoc eine Arbeitsgruppe oder eine Community einzurichten. Daher sollten die Tools die Möglichkeit bieten, Benutzer und Rollen zusätzlich und unabhängig von AD zu verwalten zu können. Das geht überdies oft schneller, als darauf zu warten, bis die zentrale IT diese Gruppe angelegt hat. Zusätzlich spart man sich bei dezentralem Management Ausgaben für weitere AD-Lizenzen.

Der Vorwurf, eine verteilte Pflege fördere den Wildwuchs und damit erhöhte Verwaltungskosten und mehr Sicherheitslücken, lässt sich zwar nicht ganz entkräften. Jedoch gilt es, Nutzen und Risiken genau abzuwägen. Standardmäßig sollte ein Enterprise-2.0-Werkzeug nur lesend auf ein AD zugreifen dürfen, die IT behält also die Hoheit. Darüber hinaus sind Nutzer von Enterprise-2.0-Tools häufig keine „vollwertigen“ System-User: Sie haben keinen Account im AD und können lediglich via Browser an Dokumente und Collaboration-Bereiche gelangen und haben keinen Zugriff auf weitere Systemressourcen. Kurzum: Sie stellen keine Gefahr dar.

Rollenvielfalt ohne Rollenchaos

Bei Regeln unterscheidet man grundsätzlich zwei Arten: die optionalen „Freigaberegeln“, auch als Freigabe-Workflow bezeichnet, sowie „Zugriffsregeln“, die eine Kombination aus mehreren

Rollen darstellen. Letztere sind beispielsweise bei einer Matrix- oder Teamorganisation sinnvoll – etwa wenn ein Unternehmen unter verschiedenen Marken oder Business Units operiert. Damit nicht für jede denkbare Kombination eine Rolle verwaltet werden muss und insbesondere dann auch die richtige(n) Rolle(n) für die Zugriffsrechte auszuwählen sind, existieren Zugriffsregeln. Dort werden je Mitarbeiter nur „einfache“ Rollen verwaltet wie „Vertrieb A“ oder „Region B“. Das Zugriffsrecht ergibt sich dann aus einer Kombination von Rollen. Die Möglichkeit, Zugriffsregeln zu gestalten, sollten zeitgemäße Enterprise-2.0-Werkzeuge bieten.

Mithilfe von individuellen Freigaberegeln, die etwa in einer Workflow-Engine mit unterschiedlichen Eskalationsstufen zu pflegen sind, lässt sich ein Freigabeprozess von Dokumenten gefahrlos automatisieren. So kann es im Sinne der Compliance oder auch nach SOX zwingend notwendig sein, bestimmte Dokumente mit einem definiertem Workflow erst durch einen dezierten Freigabeprozess an die verantwortlichen Stellen zu schicken, bevor die Dokumente veröffentlicht werden. Im Regelwerk werden dazu Dokumente und Inhalte als sicherheitsrelevant eingestuft, sodass der Freigabeprozess automatisch ausgelöst werden kann.

Grundsätzlich sind Rollen, Rechte und Regeln mit Bedacht zu vergeben. Enterprise 2.0 erfordert eine bewusste Entscheidung des Unternehmens, offen zu sein, Querdenken zuzulassen, mit Kritik umgehen zu können, weniger zu managen, sondern stärker zu moderieren. Es ist eine Frage der Kultur, ob ich „open minded“ bin – Informationen gehören dem Unternehmen und damit allen im Unternehmen – oder an der althergebrachten „Silo-Denke“ festhalte. Gleichzeitig sollte klar sein, dass Offenheit in Teilbereichen nicht möglich ist. Informationen, die gesichert sein müssen, um nicht etwa gesetzliche Folgen nach sich zu ziehen, gilt es zu identifizieren. Die Herausforderung dabei ist, R³ sinnvoll auszubalancieren und zunächst das Interesse zum Mitmachen zu wecken. ■