

# Enterprise Content Management sicher gemacht

In der Informationsgesellschaft ist die Verfügbarkeit von Daten und Dokumenten ein entscheidender Wettbewerbsfaktor. Die Einführung eines Enterprise Content Managements geniesst deshalb Priorität. Die gewonnene Transparenz birgt indes auch Risiken. *Bruno Kaiser, Manuel Ott*



**Bruno Kaiser**

lic. oec. publ., ist Chief Product Officer (CPO) und Geschäftsleitungsmitglied des Zürcher Softwarehauses AdNovum Informatik AG  
[Bruno.Kaiser@AdNovum.ch](mailto:Bruno.Kaiser@AdNovum.ch)



**Manuel Ott**

lic. phil. II, ist als technischer Redaktor verantwortlich für die Kundenzeitschrift Notitia von AdNovum  
[Manuel.Ott@AdNovum.ch](mailto:Manuel.Ott@AdNovum.ch)

Die Aufgabenerfüllung von Managern und Mitarbeitenden gestaltet sich zunehmend interaktiver. Sie erfordert Werkzeuge, die einen gezielten Umgang mit Daten, Informationen und Wissen erlauben und Inhalte möglichst zeitnah, vernetzt und in adäquater Form bereitstellen. Bei vielen Unternehmen und Organisationen sind heute Systeme im Einsatz, die spezifische Anforderungen in diesem Bereich abdecken, wie Document-, Content- und Web-Content-Management-Systeme (DMS, CMS, WCMS).

Enterprise Content Management (ECM) als Strategie beabsichtigt demgegenüber, die Funktionalität all dieser Systeme zu vereinen und zu erweitern, unter anderem mit der Einbindung von Systemen wie Business-Process-, Customer-Relationship- und Supply-Chain-Management (BPM, CRM, SCM).

## Industrialisierung der Wissensarbeit

Ziel ist es, sämtliche strukturierten und unstrukturierten Informationen im Unternehmen zu erschliessen und sie auf einer einheitlichen Plattform zur internen und teilweise externen Nutzung zur Verfügung zu stellen. Die Information soll über einen Single-Point-of-Access und ein einheitliches Repository ohne Daten- und Dokumentenredundanz unabhängig von Quelle und Nutzung allen Anwendungen zur Verfügung stehen und so ohne Medienbrüche prozessorientiert und abteilungsübergreifend genutzt werden können. ECM leistet damit einen Beitrag zur Industrialisierung der Wissensarbeit.

So weit die hehren Wünsche. Die Umsetzung der Forderungen des Enterprise Content Managements geht vor allem wegen der tiefgreifenden organisatorischen und unternehmenskulturellen Implikationen langsamer vor sich, als man aufgrund der ökonomischen Attraktivität der Idee erwarten könnte. Trotzdem scheint die Entwicklungsrichtung grundsätzlich klar zu sein.

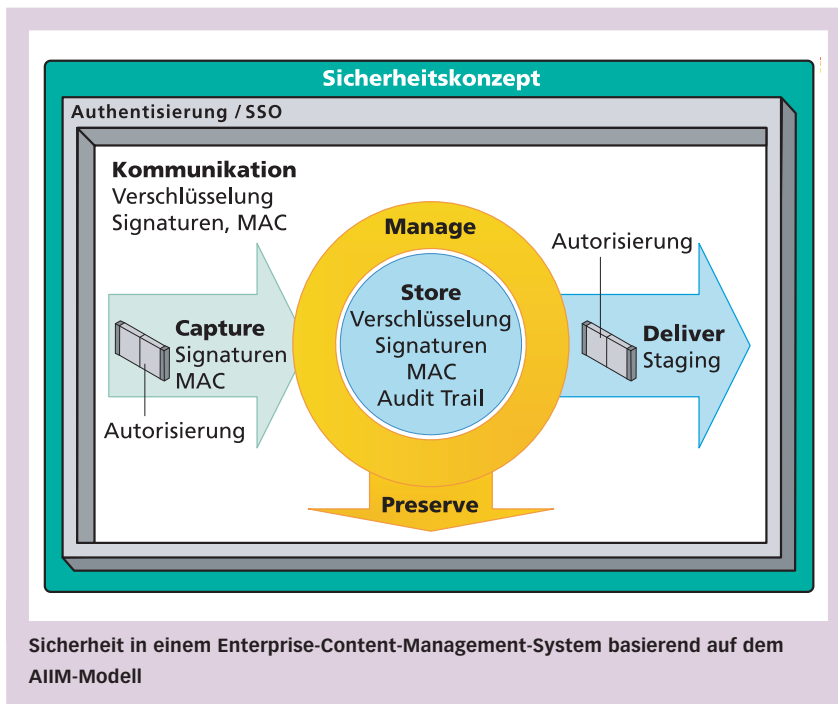
## Das gläserne Unternehmen

Der umfassende Anspruch des ECM auf Informationszugriff bedeutet für Unternehmen eine noch nie dagewesene Transparenz. Dies ist ein bedeutendes Sicherheitsrisiko in einer Welt, in der im Zuge der Globalisierung mit ihrem verbreiteten Sourcing und Shoring Spionage von Staaten wie auch von Firmen im grossen Stil betrieben wird. Auch für das Einschleusen falscher Informationen werden Unternehmen und Organisationen mit ECM exponierter, wenn sie sich nicht gut dagegen schützen.

Zwar zielt ECM bisher hauptsächlich auf die Kooperation mit Mitarbeitern (B2E) und Geschäftspartnern (B2B). Die Welten «in-house» (Intranet), «konzernweit» (Extranet) und «extern» (Internet) nähern sich jedoch immer mehr an, hinsichtlich Produkten, technischer Plattformen und Nutzungsmodellen, aber auch bezüglich Sicherheitslevel. Mit der zunehmenden Öffnung und Internationalisierung der Mitarbeiterschaft (Praktikanten, Externe, Partner, Captive Sourcing) ist das Intranet nicht mehr prinzipiell sicherer als das Internet. Ein Grossteil aller Attacken erfolgt heute von intern. Der gezielte Schutz von immateriellen Ressourcen im weltweit vernetzten Unternehmensverbund ist für die Verantwortlichen von ECM-Systemen und -Strategien somit eine der grössten Herausforderungen.

## Spezifische Sicherheitsmassnahmen

Voraussetzung für die abgestimmte und durchgehende Implementierung von Sicherheit in einem ECM-System (ECMS) und einen effizienten Einsatz entsprechender Mechanismen ist ein unternehmensweites Sicherheitskonzept. Dieses muss die allgemeinen und bereichsspezifischen Security Policies mit den erforderlichen Sicherheitsmassnahmen, Authentisierungsstärken und Audit Levels festlegen, vor allem aber auch die Klassifizierung von Dokumenten und



Inhalten und den Schutzbedarf der einzelnen Klassen.

Um spezifische Sicherheitsmassnahmen für ein ECMS festzulegen, benötigt man einen Überblick über dessen Funktionen. Hierzu eignet sich das Modell von AIIM (siehe Abbildung, [www.aiim.org](http://www.aiim.org)). ECM umfasst demnach die Erfassung (Capture), Verwaltung (Manage), Speicherung (Store), Bereitstellung (Deliver) und Bewahrung (Preserve) von Inhalten.

#### Authentischer Zugriff

Eine grundlegende Sicherheitsanforderung an ein ECMS besteht im Zugriffsschutz.

Will man sicherstellen, dass die Autorisierungskonzepte greifen und Inhalte tatsächlich nur entlang der Berechtigungen eingespeist, eingesehen, verwendet und verändert werden können, muss jeglicher unauthentische Systemzugriff unterbunden werden. Hierzu empfiehlt es sich, den Einstieg über eine zentrale Access-Infrastruktur zu bündeln, die über einen leistungsfähigen Authentisierungsservice mit diversen Authentisierungsverfahren und -stärken verfügt. Die Verwaltung der Benutzeridentitäten sollte dabei ebenfalls zentral erfolgen, idealerweise durch Anbindung eines Identity Managements. So kann der Einstieg in die angebotenen Systeme mit Single Sign-on erfolgen und ist damit nicht nur sicherer, sondern zugleich auch komfortabler.

Die Vertraulichkeit, das heisst der Schutz von Informationen vor unberechtigtem Zu-

griff, lässt sich weiter erhöhen durch verschlüsselte Kommunikation, eventuell sogar durch die Verschlüsselung von Inhalten auf den Datenspeichern.

Die Authentizität von Daten – die gesicherte Herkunft vom Absender – sowie ihre Integrität, das heisst ihre Unverändertheit und Vollständigkeit, können mit folgenden Mitteln gewährleistet werden:

- Elektronische Signaturen und Message Authentication Code (MAC) können bei der Übermittlung von Daten und Dokumenten, aber auch bei der Erfassung (Vollständigkeit) und Datenspeicherung eingesetzt werden, gegebenenfalls unterstützt

**«ECM unterstützt die Industrialisierung der Wissensarbeit.»**

durch eine PKI (Private Key Infrastructure) für die Verwaltung der Schlüssel und Zertifikate und die Authentizitätsprüfung von Signaturen.

- Für den Informations-Input (Capture) kann eine Autorisierung verlangt werden.
- Inhalte können mit der Information über den Herausgeber (Publisher) versehen werden, der sie im ECMS verfügbar gemacht hat.

Je diverser, komplexer und weitverzweigter die eingebundenen Systeme und je grösser zugleich das Potenzial gleichzeitiger Benut-

zer, desto mehr muss auch die Verfügbarkeit eines ECMS mit spezifischen Massnahmen gewährleistet werden:

- Mit Autorisierung und einer geschickten Definition von Rollen und Gruppen kann das Auslösen performanceintensiver Prozesse wie Informationsaufbereitung und -ausgabe (Deliver) kontrolliert werden.
- Staging: Um die Quelldatenbanken von Bereinigungs- und Transformationsprozessen zu entlasten, werden die Daten in einem Datenbereich (Staging Area) temporär zwischengespeichert, bevor sie in die Zieldatenbank geladen werden. Die Staging Area bietet zudem eine mögliche Plattform für Kontrollprozesse.
- Backup/Restore für Verfügbarkeit bei Ausfall eines Speichermediums.

Als Überwachungsfunktion empfiehlt sich weiter, einen Audit Trail zu führen, das sind Protokolle und Journale über Zugriffe und die Nutzung und Veränderung der Information.

#### Interdisziplinäre Projekte

Die Technologien und Mechanismen, die man für die Abdeckung dieser Sicherheitsanforderungen benötigt, sind grundsätzlich vorhanden und haben sich in anderen Anwendungsgebieten im praktischen Einsatz als tauglich erwiesen. Die konkreten Implementationen im spezifischen Kontext des Enterprise Content Managements hingegen müssen erst noch gebaut werden. Aber auch wenn dies dereinst erreicht sein wird, bleibt der angemessene Schutz der Information in einem ECMS eine Herausforderung. Die Schwierigkeit besteht insbesondere darin, den Inhalt der erfassten Dokumente genügend effizient – also möglichst automatisiert – und in der erforderlichen Granularität zu klassifizieren, zumal es schon manuell oft nicht einfach ist, den Schutzbedarf von Inhalten und Inhaltsfragmenten festzulegen.

Enterprise Content Management bringt, richtig eingeführt und angewendet, für ein Unternehmen zweifellos grosse Einsparungen und Wettbewerbsvorteile. Allein schon wegen seiner bedeutenden Implikationen nicht nur technischer Art, sondern auch in Organisation und persönlichen Arbeitsmethoden und Prozessen ist die Einführung von ECM jedoch ein komplexes und interdisziplinäres Projekt und erfordert ein entsprechend abgestimmtes und professionelles Vorgehen. Dies gilt auch für die Sicherheit: Gesamtstrategie, umsichtige Planung, Vorarbeiten und begleitende Massnahmen sind notwendig, um die damit verbundenen Risiken im Griff zu behalten. ■