

ECM muss ins Sicherheitsdispositiv integriert werden

Die allgegenwärtigen Sicherheitsrisiken betreffen auch das Enterprise Content Management (ECM), umso mehr als dieses alle Bereiche und Schnittstellen des Unternehmens verbindet. Entsprechend ist es in die Systeme und Konzepte des Unternehmens einzubinden. *Bruno Kaiser, Manuel Ott*

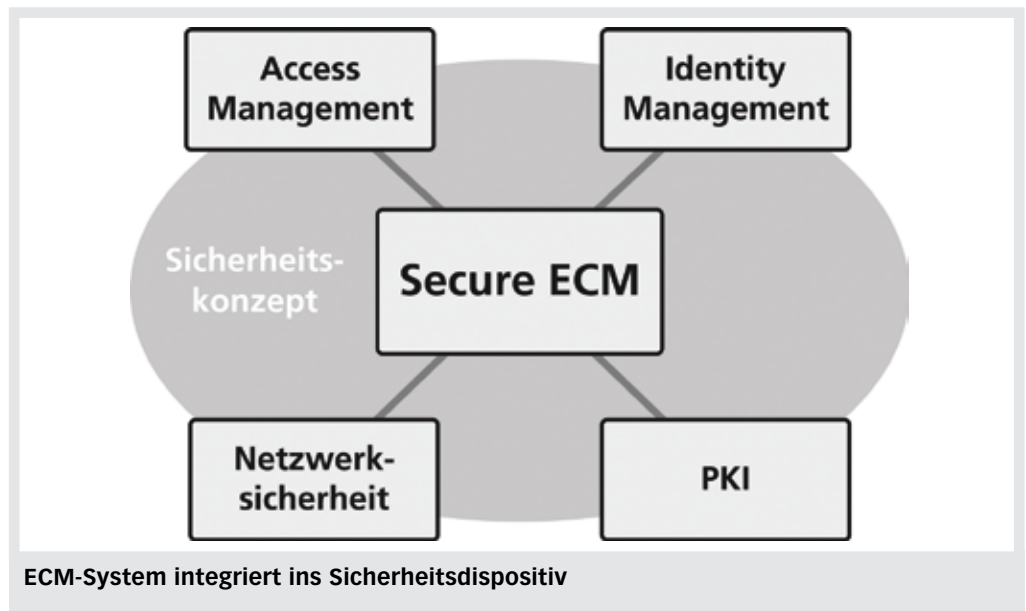
Mit der Globalisierung haben sich neue Strukturen und Timings von Unternehmensorganisation und Geschäftsprozessen ergeben. Produktion und Absatz erfolgen an entfernten, oft risikoreichen Standorten, die über grosse Distanz geführt und kontrolliert werden müssen. Dadurch ergeben sich neue Angriffspunkte, beispielsweise für Industriespionage. Die Absicherung von immateriellen Unternehmensressourcen gewinnt damit an Bedeutung.

Die Sicherheitsrisiken sind allgemein komplexer geworden, und die einzelnen Bedrohungen sind oft miteinander vernetzt und damit schwerer zu managen. Aktuell sind immer neue und noch raffiniertere Attacken aus dem Web zu beobachten, der Spam-Level ist wieder angestiegen, Missbräuche in Social Networks nehmen weiter zu, die globale Wirtschaftskrise wird für betrügerische Aktivitäten genutzt. Vermehrt treten auch gefälschte und irreführende Anwendungen auf. Gemäss Melani, der Melde- und Analysestelle Informationssicherung, verlagern sich die Angriffe von E-Mails mit Anhang oder Links hin zu Drive-by-Infektionen via vertrauenswürdig scheinende Webseiten.

Innen nicht sicherer als aussen

Die Attacken erfolgen dabei immer professioneller, gezielter und organisierter und wie die Leistungserstellung zunehmend zeit- und ortsungebunden. Das Intranet ist dabei nicht mehr prinzipiell sicherer als das Internet. Zum einen durch die zunehmende Öffnung und Internationalisierung der Mitarbeiterschaft und der Stakeholder, aber auch weil die Unterschiede zwischen «inhouse» (Intranet), «konzernweit» (Extranet) und «extern» (Internet) hinsichtlich technischer Plattformen und Nutzungsmodelle zusehends schwinden.

Das Verfügbarmachen von modernen Kommunikationsformen des Web 2.0 am Arbeitsplatz ist gemäss Gartner 2010 denn auch einer der strategisch wichtigsten Technologietrends. Bei Enterprise-Content-Management-Systemen äussert sich dies zum



Beispiel darin, dass nicht mehr nur einzelne Administratoren und Editoren, sondern zunehmend die ganze Benutzerschaft – interne wie externe – Schreibberechtigung auf das System erhält. Es genügt somit nicht, nur die «Grenzen» der Netzwerke und die darin befindlichen Geräte zu verteidigen, sondern man muss auch die Aktivitäten innerhalb der geschützten Netzwerke im Griff haben.

Der Schutz von Daten und Informationen geht jedoch weit über den Zugriffsschutz (Vertraulichkeit) und damit zusammenhängend den Datenschutz hinaus. Es geht auch um Integrität (den Schutz vor unbemerkter und unautorisierter Veränderung), um Authentizität (die Sicherstellung des richtigen Ursprungs beziehungsweise Absenders einer Meldung), um Non-Repudiation (die elektronische Nachvollziehbarkeit und Beweisbarkeit von Aktionen) sowie um Verfügbarkeit der Informationen, was bedeutet, dass die Systeme beispielsweise nicht durch DOS-Attacken ausser Gefecht gesetzt werden können.

Regulierungen und Compliance als Treiber

Die schnelle Verfügbarkeit von Informationen im Unternehmen ist mittlerweile ein bedeutender Wettbewerbsfaktor. Gleichzeitig

nehmen die Regulierungen und die Anforderungen an Compliance, Transparenz und Nachvollziehbarkeit von Seiten der Corporate Governance und diverser Stakeholder laufend zu. Dies sind zentrale Treiber für die Einführung eines Enterprise-Content-Management-Systems.

Sämtliche Informationen im Unternehmen sollen erschlossen werden. Ein ECM-System soll Inhalte vernetzt und in adäquater



Bruno Kaiser,
Lic. Oec. Publ.,
MBL HSG, ist
Chief Product
Officer (CPO)
und Geschäfts-

leitungsmitglied des Zürcher Software-

hauses Adnovum Informatik AG.

Bruno.Kaiser@Adnovum.ch



Manuel Ott,
Lic. phil. II, ist
als technischer
Redaktor verant-

wortlich für die

Kundenzeitschrift

Notitia der Adnovum Informatik AG.

Manuel.Ott@Adnovum.ch

Form über einen Single-Point-of-Access auf einer einheitlichen Plattform zur internen und teilweise externen Nutzung bereitstellen. Geschäftsrelevante Figures wie Quartalszahlen des Unternehmens müssen punktgenau zeitgesteuert publiziert werden können. ECM vereint dazu Systeme für Dokumentenmanagement (DMS), Content-Management (CMS), Web Content Management (WCMS) und Records Management und erweitert sie mit der Einbindung von Business-Systemen sowie spezieller Informationssysteme, zum Beispiel Marktdatensysteme für Aktienkurse. Zunehmend werden auch Collaboration- und Community-Funktionen («Social Computing») in die ECM-Systeme integriert, wie Ideenmanagement, Blogs, Wikis und Foren.

Ambivalente Transparenz

Zentral ist das Management der neuen Transparenz. Die Gefahr besteht dabei nicht nur in der Visibilität nach aussen («gläsernes Unternehmen»), sondern auch bezüglich gezieltem Einschleusen von Falschinformationen. Mit der zentralen Verwaltung der Daten beinhaltet ECM jedoch auch eine grosse Chance für die Informationssicherheit. Nur damit lassen sich feingranulare Sicherheits-Policies pro Datenfeld effizient und effektiv anwenden, durchsetzen und überwachen.

Unternehmensweites Sicherheitskonzept

Für die genannten Sicherheitsherausforderungen sind heute Ansätze und Systeme verfügbar, mit denen die entsprechenden Risiken unter Kontrolle gehalten werden können, wenn sie umfassend und mit der nötigen Professionalität eingesetzt werden: Digital Rights Management (DRM), Identity and Access Management (IAM), Intrusion Prevention and Detection, Security Activity Monitoring und andere mehr.

Wie können die Sicherheitsanforderungen in einem ECM-System umgesetzt werden? Grundlage ist ein unternehmensweites Sicherheitskonzept, in dem die alle-

gemeinen und bereichsspezifischen Security Policies mit den erforderlichen Massnahmen, Authentisierungsstärken und Audit Levels festgelegt sind. Ebenso müssen darin in einem Autorisierungskonzept die Klassen von Dokumenten und Inhalten und deren Schutzbedarf definiert sein.

Vertraulichkeit dank Zugriffsschutz

Inhalte sollen nur entlang der Autorisierungskonzepte und Berechtigungen eingespeist, eingesehen, verwendet und verändert werden können. Dazu muss jeglicher unauthentische Systemzugriff unterbunden werden. Dies erreicht man zum Beispiel dadurch, dass man den Einstieg über eine zentrale Access-Infrastruktur bündelt, die über einen leistungsfähigen Service mit diversen Authentisierungsverfahren und -stärken verfügt und die Funktion einer Web Application Firewall wahrnimmt. Das ECM-System wird deshalb vorzugsweise ins Access Management des Unternehmens integriert.

Auch die Benutzeridentitäten sollten zentral verwaltet werden, idealerweise durch Anbindung eines Identity Managements. Dies erlaubt einen Single-Sign-on für die angebotenen Systeme, der Einstieg wird damit sicherer und zugleich komfortabler. Zudem ist das ECM-System in die Netzwerksicherheit im Unternehmen zu integrieren, das heisst mit dem Zonenkonzept, den Firewalls etc., sodass es auch von dieser Seite vor internen und externen Attacken geschützt ist.

Durch verschlüsselte Kommunikation, eventuell sogar durch die Verschlüsselung von Inhalten auf den Datenspeichern, lässt sich die Vertraulichkeit weiter erhöhen. Voraussetzung für Verschlüsselung ist die Verteilung der benötigten Schlüssel, etwa durch Anbindung an eine Public-Key-Infrastruktur (PKI).

Integrität und Authentizität

Die Integrität und die Authentizität von Daten – die gesicherte Herkunft vom Absender – können mit elektronischen Signaturen und

Message Integrity Codes (MIC) oder Message Authentication Codes (MAC) gewährleistet werden. Diese können bei der Übermittlung von Daten und Dokumenten, aber auch bei der Erfassung (Vollständigkeit) und Datenspeicherung eingesetzt werden, gegebenenfalls unterstützt durch eine PKI für die Verwaltung der Schlüssel und Zertifikate und die Authentizitätsprüfung von Signaturen. Im ECM-Umfeld kann zudem für Informations-Input eine Autorisierung verlangt und Inhalte können mit der Information über den Herausgeber (Publisher) versehen werden.

Non-Repudiation und Verfügbarkeit

Für die Nachvollziehbarkeit von Aktivitäten im ECM-System empfiehlt es sich, elektronische Protokolle und Journale über Zugriffe und die Nutzung und Veränderung der Informationen zu führen, das heisst einen sogenannten Audit Trail. Dieser ermöglicht zusammen mit anderen Technologien das Security Activity Monitoring, die Überwachung und Speicherung der Aktivitäten von internen als auch externen Usern im Netzwerk. Security Activity Monitoring erlaubt einerseits Vorschriften zur Nachverfolgung von Geschäftsprozessen einzuhalten, dient aber auch dazu, verdächtige Aktivitäten – zum Beispiel Betrugsversuche im E-Banking oder Datenklau durch Angestellte – zu eruieren.

Die Verfügbarkeit von Informationen und Daten im ECM-System bei Ausfall eines Speichermediums kann mittels Back-up- und Restore-Routinen und -Prozeduren gewährleistet werden. Das System ist aber auch vor Überlastung zu schützen: Um die Quelldatenbanken von Bereinigungs- und Transformationsprozessen zu entlasten, kann man die Daten, bevor sie in die Zieldatenbank geladen werden, in einem speziellen Datenbereich temporär zwischenspeichern (Staging). Diese sogenannte Staging Area eignet sich auch als Plattform für Kontrollprozesse. Performanceintensive Prozesse wie Informationsaufbereitung und -ausgabe lassen sich mittels Autorisierung und geschickt definierten Rollen und Gruppen kontrollieren und begrenzen.

Kein Stand-alone-System

ECM darf kein Stand-alone-System sein, sondern muss ins Sicherheitskonzept des Unternehmens integriert und an die entsprechenden Systeme angebunden werden, also das Identity- und Access Management, die Netzwerksicherheit, die PKI etc. Die Sicherheitsfunktionen können dabei je nach Situation und Strategie des Unternehmens optimal kombiniert und abgestimmt werden.

Charakteristiken eines Secure ECM

- **Unternehmensweites Sicherheitskonzept:** Security Policies & -Massnahmen, Authentisierungsstärken, Audit Levels, Autorisierungskonzept
- **Identity- & Access Management:** Authentisierung, WAF, Benutzerverwaltung, SSO, Access Control
- **Netzwerksicherheit:** Zonenkonzept, Firewalls
- **Verschlüsselung, evtl. PKI**
- **Integrität & Authentizität:** elektronische Signaturen, MIC, MAC
- **Non-Repudiation:** Audit Trail, Security Activity Monitoring
- **Verfügbarkeit:** Back-up/Restore, Staging

Digitale Nachhaltigkeit – ein Konzept mit Zukunft

Der nachhaltige Umgang ist nicht nur bei natürlichen Ressourcen notwendig, sondern wird künftig auch bei digitalen Gütern immer wichtiger. Doch welche Auswirkungen und Potenziale hat diese Entwicklung für Produzenten und Konsumenten insbesondere von Software? *Matthias Stürmer*

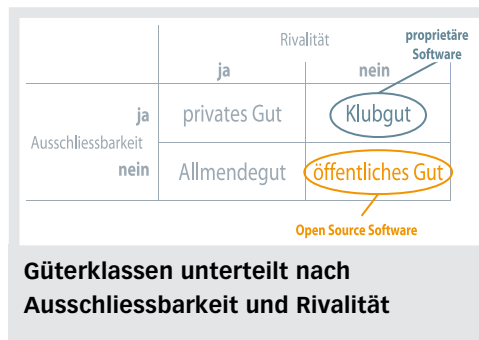
Nachhaltigkeit ist ein Trendbegriff, der heute vorwiegend im Zusammenhang mit ökologischen Themen wie Umweltschutz, Klimawandel und alternativen Energiequellen verwendet wird. Weshalb sollte Nachhaltigkeit nun auch bei immateriellen Gütern relevant sein, die nicht wie natürliche Ressourcen begrenzt verfügbar sind und aufgebraucht werden können? Und welchen Zusammenhang hat dieser Nachhaltigkeitsaspekt mit erfolgreichen Geschäftsmodellen von Softwareunternehmen?

Der Begriff der Nachhaltigkeit

Wer das Konzept der Digitalen Nachhaltigkeit verstehen will, muss sich erst mal mit der Definition von «Nachhaltigkeit» auseinandersetzen. Dieser Begriff wurde bereits im Jahre 1713 durch Hans Carl von Carlowitz im Zusammenhang mit der Forstwirtschaft verwendet. Damals wie auch heute beschreibt das Konzept der Nachhaltigkeit die Nutzung eines regenerierbaren Systems, sodass dieses in seinen wesentlichen Eigenschaften erhalten bleibt und sein Bestand auf natürliche Weise nachwachsen kann. Die begrenzte Verfügbarkeit von Ressourcen der Natur stellt somit die entscheidende Eigenschaft dar, dass ein behutsames Aufbrauchen überhaupt erst notwendig ist. Auch die mit dem Begriff der ökologischen Nachhaltigkeit verwandten Konzepte wie soziale oder ökonomische Nachhaltigkeit gehen von sogenannter Rivalität der Ressourcen aus, also dass diese nicht beliebig oft verwendet werden können.

Herausforderungen unserer Wissensgesellschaft

Demgegenüber behandelt die Digitale Nachhaltigkeit ausschliesslich immaterielle Güter, genauer noch Wissensgüter. Dies ausgehend von der Idee, dass wir heute in einer Wissensgesellschaft leben, in der die Verfügbarkeit von Wissen ein entscheidender Überlebensfaktor sowohl für Menschen wie auch für Organisationen darstellt. Für ein kleines, rohstoffarmes Binnenland wie die Schweiz ist Wissen von besonders grosser volkswirtschaftlicher



Bedeutung: Die Bildung der Bevölkerung, Innovationskraft der Unternehmen, Effizienz in der öffentlichen Verwaltung, Exzellenz in der Wissenschaft – fast alle Gesellschaftsbereiche setzen die langfristige und offene Verfügbarkeit von Wissensgütern voraus. Im Informationszeitalter eröffnet die fortschreitende Digitalisierung für unser Land grosse Potenziale, die zur Herstellung und Verbreitung von Wissensgütern erschlossen werden können und so dem Nutzen der gesamten Volkswirtschaft dienen können.

Doch neue Technologien schaffen auch neue Herausforderungen, beispielsweise in der langfristigen Weiterentwicklung von Software unabhängig von einzelnen Konzernen oder in der sicheren Archivierung digitaler Daten. Nachhaltige Lösungen wären gefragt, aktuelle Beispiele zeigen jedoch, dass diese alles andere als selbstverständlich sind. Softwareentwicklungen bleiben verschlossen und bewusst inkompatibel, mächtige Firmenmonopole werden durch Investitionen von öffentlichen Institutionen weiter gestärkt und mit öffentlichen Geldern erstellte Inhalte und Forschungsergebnisse sind nur gegen erneute Bezahlung verfügbar.

Das Konzept der Digitalen Nachhaltigkeit

In diesem Spannungsfeld von gesellschaftlichen und unternehmerischen Interessen setzt das Konzept der Digitalen Nachhaltigkeit an. Obwohl heute noch keine breit abgestützte Definition dieses Begriffs existiert und er – wenn überhaupt – bloss im Zusammenhang mit Datenspeicherungen in Archiven

verwendet wird, zeigen die zuvor beschriebenen Beispiele die Notwendigkeit der Benennung dieser Thematik.

Digitale Güter können anders als natürliche Ressourcen beliebig oft verwendet und vervielfältigt werden, ohne dass sie an Wert verlieren, das heisst sie sind nicht-rivalisierend. Jedoch zeigt die klassische Unterscheidung (siehe Abbildung), dass digitale Güter ohne Weiteres ausschliessbar sein können. Währenddem sich Klubgüter in der digitalen Welt als proprietäre Software oder mittels Digital Rights Management (DRM) geschützte Medien manifestieren, sind Open-Source-Software oder unter Creative Commons veröffentlichte Musik Beispiele von öffentlichen Gütern. Die freie Verwendung von digitalen Gütern stellt somit ein entscheidender Faktor dar, der die nachhaltige Nutzung von Wissensgütern beeinflusst.

Eine weitere Eigenschaft stellt die freie Veränderung oder Weiterentwicklung von digitalen Gütern dar. Erst wenn der Quellcode einer Software für alle frei verfügbar und veränderbar ist, kann dieses digitale Gut auch von Externen verbessert werden. Bildet sich wie beispielsweise beim Linux Kernel eine aktive und heterogene Community von Freiwilligen und Unternehmen, die die Software kontinuierlich weiterentwickeln, ist der nachhaltige Nutzen für Leistungserbringer und Leistungsbezüger gewährleistet.

Open Source allein reicht nicht aus

Es gilt zu beachten, dass die freie Lizenz eine notwendige aber nicht hinreichende Bedingung für die nachhaltige Entwicklung eines digitalen Gutes ist. So stellen besonders die vielseitige und gesunde Entwicklergemeinschaft und die intelligente Koordination des



Dr. **Matthias Stürmer** arbeitet als Projektleiter beim Internetdienstleister Liip AG.

Open-Source-Projekts – sei es durch Einzelpersonen oder Firmen – entscheidende Faktoren für die langfristige Weiterentwicklung der Software dar. Ähnliches ist bei Portalen von freien Inhalten beobachtbar. Die Beiträge auf Wikipedia stehen zwar unter einer freien Lizenz, der Erfolg von Wikipedia begründet sich aber vor allem auf der aktiven Autorenschaft, die auf einfache Weise Inhalte erstellen und verändern kann. Das geschickte Community-Management von derartigen Projekten bildet somit eine wichtige Grundlage für deren Erfolg.

Nutzen der Digitalen Nachhaltigkeit für Konsumierende

Die Vorteile für die Empfänger digital nachhaltiger Produkte sind offensichtlich. Einerseits können langfristig Kosten gespart werden durch Wegfall von Lizenzgebühren, andererseits sinkt die Abhängigkeit von Dienstleistern und steigt somit die Verhandlungsposition bei der Beschaffung, was wiederum die Preise senkt. Die Volkswirtschaften profitieren von einem intensiveren Wettbewerb durch niedrigere Markteintrittsbarrieren für Unternehmen, Monopolstellungen werden aufgeweicht. Daraus folgt, dass sich Firmen durch tatsächliche qualitative Unterschiede ihrer Leistungen differenzieren müssen, anstelle die Abhängigkeit ihrer Kunden auszunutzen.

Für die Gesellschaft bedeutet dies, dass sie im ökonomischen Sinne von den positiven volkswirtschaftlichen Auswirkungen profitiert, wenn Marktverzerrungen verringert und die angebotenen Produkte und Dienstleistungen qualitativ verbessert werden. Des Weiteren entstehen wie oben beschrieben neue, öffentliche Güter, von denen alle Menschen Nutzen ziehen können. Öffentliche Gelder werden künftig verstärkt in die Herstellung von öffentlichen Gütern investiert. Dadurch verkleinert sich der sogenannte Digital Divide, und alte und junge, sozial hoch und niedrig gestellte sowie Menschen in industrialisierten und nicht-industrialisierten Regionen der Welt erhalten gleichermassen freien Zugang zu Wissen und Bildung – beides Menschenrechte laut Artikeln 19 und 26 der Allgemeinen Erklärung der Menschenrechte.

Diese schöne, neue Welt entsteht nicht einfach so. Heutige Strukturen, besonders im öffentlichen Bereich, verhindern noch zu oft die Nutzung dieses Potenzials. Aus diesem Grund wurde in der Schweiz Anfang des Jahres auch die Parlamentarische Gruppe Digitale Nachhaltigkeit von Politikern aus allen Parteien gegründet. Mit 25 National- und Ständeräten ist bereits jeder zehnte Parla-

mentarier Mitglied der Gruppe, die sich für die Förderung von digital nachhaltigen Technologien einsetzt.

Auswirkungen für Hersteller digitaler Güter

Wo aber im Konzept der Digitalen Nachhaltigkeit bleibt Wertschöpfungspotenzial für die Produzenten von digitalen Gütern? Wird dadurch nicht die Konkurrenz zunehmen und die Umsätze und Margen drücken? Ja, das ist die eine Seite der Münze. Aber diese und andere Veränderungen im Bereich der digitalen Güter sind unaufhaltsam. Technologische Entwicklungen wie das Internet haben die Musikindustrie umgekrempelt und neue Gewinner und Verlierer geschaffen. Wer also Marktentwicklungen ignoriert und nicht nach alternativen Geschäftsmodellen Ausschau hält, kann rasch von Branchenveränderungen überrumpelt werden. Und wenn selbst das traditionelle Marktforschungsunternehmen Gartner einen weiteren Anstieg von Open-Source-Software prophezeit, dann sind grössere Veränderungen in der Softwareindustrie absehbar.

Das Dienstleistungsmodell für Open-Source-Software

Open-Source-Modelle für das Business gibt es viele, grundsätzlich lassen sich aber zwei Arten unterscheiden, das Dienstleistungsmodell und das Hybrid-Modell. Beim ersten Modell erbringen Unternehmen Dienstleistungen rund um Open-Source-Technologien wie Linux oder PHP, über die sie mit Wissen und Erfahrung verfügen. So können sie kompetent Dienstleistungen wie Beratung, Implementierung, Erweiterungen, Schulung und Wartung anbieten. In dem sich diese Open-Source-Firmen aktiv an der Weiterentwicklung der unterstützten Open-Source-Produkte beteiligen, indem sie Mitarbeitern Arbeitszeit dafür zur Verfügung stellen, eignen sie sich Know-how über die jeweiligen Open-Source-Lösungen an. Der Zugriff auf diese sogenannten Kernentwickler befähigt die Firmen, rasch und kompetent Probleme von Kunden zu beheben und Änderungen am Quellcode vorzunehmen. Dies wiederum ermöglicht das Abschätzen von Risiken und lässt den Abschluss von Service Level Agreements zu – ein klares Bedürfnis von Kunden, die Open-Source-Technologien einsetzen.

Andere Arten von Geschäftsmechanismen des Dienstleistungsmodells sind beispielsweise bei der Open-Source-E-Learning-Lösung Moodle erkennbar. Um diese etablierte Webapplikation an ihre Bedürfnisse anzupassen, erteilen Kunden Firmen nicht nur den

Auftrag, spezifische Veränderungen vorzunehmen, sondern wünschen zwecks langfristiger Wartung in gewissen Fällen sogar die offizielle Weiterentwicklung des Open-Source-Projekts mit bestimmten Funktionalitäten. Viele solcher Anfragen treffen über die internationale Plattform www.moodle.com ein, auf der ausschliesslich akkreditierte Moodle-Partner aufgeführt sind. Diese wiederum verpflichteten sich, 10 Prozent ihres Umsatzes mit Moodle-Dienstleistungen der australischen Firma Moodle Headquarters abzugeben, die für die nachhaltige Weiterentwicklung des Open-Source-Projekts verantwortlich ist.

Der Mix von Open Source und Closed Source

Hybrid-Modelle, die zweite Art von Geschäftsmodellen, vermixt in gewissem Sinne Open-Source-Software mit proprietärer Software. Firmen wie Alfresco oder Sun Microsystems bieten ihre Softwareprodukte sowohl unter einer Open-Source-Lizenz als auch unter einer proprietären Lizenz an. Andere Unternehmen wie IBM veröffentlichen Open-Source-Technologien, erreichen dabei eine hohe Marktdurchdringung und verkaufen so erfolgreich proprietäre Erweiterungen. Auch Google und Nokia betreiben mit Android und Maemo ein Mix zwischen offener und geschlossener Software, obwohl dabei der eigentliche Umsatz noch einmal mit anderen Quellen (Werbung respektive Hardwareverkauf) erwirtschaftet wird. Nichtsdestotrotz zeigen all diese Beispiele, dass ohne Weiteres mit «Gratis-Software» erfolgreich Geld verdient werden kann.

Digitale Nachhaltigkeit im Enterprise Content Management

Abschliessend bleibt die Frage, welchen Einfluss das Konzept der Digitalen Nachhaltigkeit auf den Bereich Enterprise Content Management ausübt. Zwei grundlegende Anforderungen an ECM-Systeme zeigen deutlich die Wichtigkeit der Nachhaltigkeitsthematik in diesem Bereich auf: Die langfristige Speicherung der Inhalte (Content) und die integrierte Verwaltung (Management) der Daten. Open-Source-Lösungen, basierend auf offenen Schnittstellen und Standards, sind eine Antwort auf dieses Bedürfnis, Daten flexibel zugreifbar zu verwalten und nachhaltig abzulagern. Welche offenen Standards in welchen ECM-Lösungen künftig verwendet werden, ist eine Diskussion, zu der alle ECM-Anbieter und -Anwender aufgerufen sind. Plattformen wie das ECM-Forum bieten dafür einen wichtigen Rahmen, um Pionierprojekte vorzustellen und neue Lösungswege aufzuzeigen.