
Software-Evaluation von Information Rights Management (IRM) Systemen

Im folgenden finden Sie die wahrscheinlich einzige Softwareevaluation für Information Rights Management Systeme, die sowohl einen detaillierten Überblick über den Markt der Anbieter als auch einen praxisorientierten Vorschlag zur Vorgehensweise bei der Auswahl eines Produkts anbietet. Die Grundlage des Dokuments bildet ein vor kurzem abgeschlossenes Kundenprojekt.

Die Evaluation gliedert sich in mehrere Teile. Bevor mit den Hersteller- und Produktvorstellungen begonnen wird, finden Sie die Vorstellung einer Management-Methode zur Evaluation und eine Einführung in die rechtlichen und in die IT-Belange zum Thema Sicherheit. Unternehmen und die eingesetzte Software in diesem Umfeld müssen Anforderungen genügen, die sicherstellen, dass Gefahren minimiert oder ganz ausgeschaltet werden. Nur wer die Gefahren kennt, kann sich Gedanken darüber machen mit welchen Mitteln er sie abwehren möchte.

Um eine Softwareevaluation, die einem Softwareprojekt gleichzusetzen ist, erfolgreich gestalten zu können, ist es sinnvoll sich mit dem gewünschten Projekterfolg auseinanderzusetzen und dafür zu sorgen, dass mögliche Schwierigkeiten von vorne herein ausgeschaltet werden. Informationen dazu finden sie im Kapitel Projekterfolg.

Im Anschluss daran folgt die Einführung der sieben großen Player am Markt inklusive vorhandener Referenzen, gefolgt von einer Übersicht kleinerer, aber nicht minder interessanter Unternehmen und Lösungen. Danach finden Sie wichtige Hinweise und Vorgehensmodelle für eine professionelle und zügige Softwareauswahl. Nur wer die richtigen Vorbereitungen trifft, wird sich später auch für das passende System entscheiden können. Fehlentscheidungen lassen sich frühzeitig vermeiden. Die notwendigen Informationen und Tipps dazu finden Sie in diesem Teil der Ausarbeitung.

Sollten Sie selbst gerade vor der Aufgabe der Auswahl eines IRM-Systems stehen, so wird Ihnen dieses Dokument ein hilfreicher und zeitsparender Helfer sein.

Bei Interesse am Gesamtdokument melden Sie sich einfach mit einer eMail an:

info@hoffmann-consultingservices.de

Rechtliche Informationen

Dieses Dokument dient nur zu Informationszwecken. Die in diesem Dokument beinhalteten Informationen stellen die zum Zeitpunkt der Erstellung aktuelle Sicht der Hoffmann Consulting Services dar. Später statt gefundene Markt- oder Produktveränderungen können die Aktualität des Dokuments beeinflussen. Die Hoffmann Consulting Services übernehmen keine Gewährleistung für die Richtigkeit der Informationen und haften nicht für Fehler oder fehlerhafte Darstellungen. Die Inhalte des Dokuments können sich ohne Ankündigung ändern.

Ohne die explizite schriftliche Genehmigung der Hoffmann Consulting Services darf kein Teil dieses Dokuments reproduziert, gespeichert, sonstwie aufbewahrt oder in irgendeiner Form übertragen werden.

© 2012 Hoffmann Consulting Services. All rights reserved.

Adobe	Adobe, das Adobe Logo, Adobe AIR, Flash, Flex, und LiveCycle sind entweder registrierte Trademarks oder Trademarks der Adobe Systems Incorporated in den United States und/oder anderen Ländern.
EMC ²	EMC ² , EMC, Documentum, eRoom sind registrierte Trademarks der EMC Corporation.
Liquid Machines	Liquid Machines, Enabling Secure Business, The Freedom of Security, Policy Droplet und das Liquid Machines Logo sind Trademarks oder registrierte Trademarks der Liquid Machines Inc.
Microsoft	Microsoft, Active Directory, PowerPoint, SharePoint, Windows, und Windows Server sind entweder registrierte Trademarks oder Trademarks der Microsoft Corporation in den United States und/oder anderen Ländern.
Oracle	Oracle, JD Edwards, PeopleSoft, and Siebel sind registrierte Trademarks der Oracle Corporation und/oder seiner Niederlassungen.
SCQuARE	Sämtliche SCQuARE Programm-Materialien, das Konzept, Logos, Know-how and das Mnemonic sind Copyright der SCQuARE International Limited.
Docu Protection	Alle auf Basis DocuProtection genannten Produkte sind Eigentum der DocuProtection GmbH

Die Namen von Unternehmen und Produkten, die in diesem Dokument genannt werden, können Trademarks ihrer jeweiligen Besitzer sein.

Inhaltsverzeichnis

1	Softwareauswahl	6
2	IRM-Systeme.....	7
3	Kurzeinführung der SCQuARE Management-Methode.....	9
3.1	Denken und Kommunikation	10
4	Schutz von Informationen.....	12
4.1	Wichtige Begriffe der Informationssicherheit.....	13
4.2	Vorschriften und Gesetzesanforderungen.....	14
4.2.1	Gesetzliche Regelungen zur Informationssicherheit.....	15
4.3	Unzureichende Informationssicherheitsstrategien.....	17
4.3.1	Erhaltung eines Sicherheitsstandards.....	18
4.3.2	Kontrollmechanismen und Aufklärung.....	19
4.3.3	Unvollständige Konfiguration von IT-Systemen	19
4.3.4	Mangelnder Einsatz von Sicherheitsfunktionen.....	20
4.3.5	Vernetzung und Internet-Anbindung.....	20
4.3.6	Notwendige Sicherheitsanforderungen.....	21
4.3.7	Mangelhafte Ausbildung.....	21
4.3.8	Unzureichende Wartung.....	22
4.3.9	Passwörtern und Sicherheitsmechanismen.....	22
5	Projekterfolge - warum scheitern Projekte.....	24
6	Marktübersicht.....	26
7	Positionierung der Hersteller.....	29
7.1	ADOBE Inc.....	29
7.1.1	Technologie.....	31
7.1.1.1	Systemanforderungen.....	31
7.1.1.2	Unterstützte Formate.....	32
7.1.2	Referenzen.....	33
7.1.2.1	Bombardier.....	33
7.1.2.2	Castilla-La Mancha Community Council.....	34
7.1.3	Weitere Informationen.....	34
7.2	EMC.....	35
7.2.1	Technologie.....	37
7.2.1.1	Systemanforderungen.....	38
7.2.1.2	Unterstützte Formate.....	39
7.2.2	Referenzen.....	39
7.2.2.1	Novation (www.novationco.com).....	39
7.2.2.2	OffWall Street (www.offwallstreet.com).....	40
7.2.3	Weitere Informationen.....	41
7.3	Fasoo.....	42
7.3.1	Technologie	44
7.3.1.1	Systemanforderungen.....	44
7.3.1.2	Unterstützte Formate.....	45
7.3.2	Referenzen.....	46
7.3.2.1	KT Freetel.....	46
7.3.2.2	Korean Ministry of Information and Communications.....	46

7.3.2.3	Weitere Referenzen.....	47
7.3.3	Weitere Informationen.....	47
7.4	Liquid Machines.....	48
7.4.1	Technologie.....	49
7.4.1.1	Systemanforderungen.....	49
7.4.1.2	Unterstützte Formate.....	50
7.4.2	Referenzen.....	50
7.4.2.1	Pilz GmbH.....	50
7.4.3	Weitere Informationen.....	52
7.5	Microsoft.....	53
7.5.1	Technologie.....	55
7.5.1.1	Systemanforderungen.....	55
7.5.1.2	Unterstützte Formate.....	56
7.5.2	Referenzen.....	57
7.5.2.1	Dow Corning.....	57
7.5.3	Weitere Informationen.....	58
7.6	Oracle.....	59
7.6.1	Technologie.....	61
7.6.1.1	Systemanforderungen.....	62
7.6.1.2	Unterstützte Formate.....	64
7.6.2	Referenzen.....	65
7.6.2.1	Renault.....	65
7.6.2.2	Johnson Matthey Plc.....	66
7.6.2.3	Weitere Referenzen.....	66
7.6.3	Weitere Informationen.....	67
7.7	Seclore.....	68
7.7.1	Technologie.....	68
7.7.1.1	Formate.....	69
7.7.1.2	System Anforderungen für den Seclore FileSecure Policy Server.....	69
7.7.1.3	System Anforderungen für Seclore FileSecure auf dem File Server.....	69
7.7.1.4	System Anforderungen für den Seclore FileSecure Desktop Client.....	70
7.7.1.5	Seclore FileSecure Viewer.....	70
7.7.1.6	Hotfolder-Technologie.....	70
7.7.1.7	Konnektoren.....	70
7.7.1.8	FAQs.....	70
7.7.2	Kunden und Referenzen.....	71
7.7.3	Ansprechpartner.....	71
7.7.4	Sonstiges.....	71
7.8	Andere Hersteller.....	72
8	Verwandte Sicherheitstechnologien und -lösungen.....	73
8.1	DocuProtection.....	73
9	Der Softwareauswahlprozess.....	75
9.1	Das Vorgehensmodell.....	76
9.1.1	Das klassische Modell.....	76
9.1.1.1	Validierung und Scoping.....	77
9.1.1.2	Analyse und Anforderungsdefinition.....	77

9.1.1.3	Entscheidungsvorbereitung.....	78
9.1.2	Die alternative Vorgehensweise.....	79
9.1.2.1	Die Assessment-Phase.....	79
9.1.2.2	Die Planungsphase.....	80
9.1.2.3	Die Pilot-Phase.....	81
9.1.2.4	Rollout.....	81
9.2	Die Vorauswahl.....	82
9.2.1	Vorgehen in der Vorauswahl	84
9.3	Die Feinauswahl.....	85
9.4	Die Endauswahl.....	85
9.5	Festlegung Kriterienkatalog.....	86
9.5.1	Basisangaben zum Anbieter.....	87
9.5.2	Rahmenbedingungen.....	87
9.5.2.1	Kostenrahmen.....	87
9.5.2.2	Allgemeine Funktionalitäten.....	87
9.5.2.3	Betriebssystem, Datenbanken und Schnittstellen.....	88
9.5.2.4	Funktionale Abdeckung.....	88
9.5.2.5	Branchenlösungen.....	88
9.5.2.6	Anbieterleistungen.....	89
9.6	Erstellung der Checkliste.....	90
9.7	Analyse der Anforderungsabdeckung.....	90
10	Management Summary.....	91

Anhang

Kriterienkatalog

Checkliste

1 Softwareauswahl

Die Auswahl von Softwareprodukten stellt sowohl für Unternehmen und Organisationen als auch für private Nutzer immer eine Herausforderung dar. Jeder hätte gerne das Produkt mit der umfangreichsten Funktionalität, der besten Performance, dem optimalen Service und dem günstigsten Preis. Doch diese Ziele sind nur schwer zu vereinen. Zumeist bedarf es einer genauen Untersuchung der wirklichen Anforderungen. Nicht alles was man sich wünscht, ist unbedingt erforderlich. Viele Funktionen, die von umfangreichen Softwarepaketen angeboten werden, verwendet man letztlich doch nur gelegentlich oder überhaupt nicht. Um am Ende der Softwareauswahl zu einem von allen Seiten akzeptierten Ergebnis zu kommen, ist ein detaillierter Abgleich mit den notwendigen Kriterien und den angebotenen Produkten erforderlich. Viele Unternehmen machen den Fehler zu schnell zu Herstellerinformationen zu greifen und sich von glänzenden Marketingbroschüren und eloquenten Vertriebsmitarbeitern Lösungen anbieten zu lassen, die nicht oder nur wenig mit den notwendigen Anforderungen zu tun haben oder gar viel zu viel Funktionalität liefern, die man niemals wirklich verwenden wird.

Um dies zu verhindern, ist es unerlässlich sich vorab mit den notwendigen Anforderungen an das gewünschte System auseinander zu setzen. Doch auch diese Aufgabe ist nicht trivial, spielen doch viele Faktoren eine Rolle. Letztlich ist jedoch die Akzeptanz der Anwender entscheidend für den Erfolg einer Lösung. Doch bevor eine Entscheidung getroffen werden kann, gilt es alle Betroffenen anzuhören. Nur so kann man sich ein Bild über die

meist unterschiedlichen Standpunkte von Geschäftsführung, IT-Abteilung und den Anwendern machen. Für diese Anforderungsanalyse ist wiederum eine Vorgehensweise erforderlich um sicherzustellen, dass alle Betroffenen mit im Boot waren und jeder die Chance hatte seine Wünsche und Bedenken zu äußern. Am Ende dieser Analysephase ist es sinnvoll die Ergebnisse zu dokumentieren und sie sich schriftlich von den späteren Entscheidern bestätigen zu lassen. Damit wird die Softwareauswahl zu einem richtigen Projekt, das gut gemanagt und in einem vorher definierten Zeitraum stattzufinden hat.

Für die Anforderungsanalyse empfiehlt sich eine methodische Vorgehensweise. Mit der Managementmethode SCQuARE existiert ein Werkzeug, das für diese Phase prädestiniert ist. SCQuARE hilft den Beteiligten bei der Erfassung der gegenwärtigen Situation und konfrontiert sie dann mit den möglichen Veränderungen, die kurz- oder langfristig Einfluss auf die gesuchte Lösung haben werden. Daraus lassen sich viele Fragen ableiten, die letztlich in eine zentrale Frage münden, deren Beantwortung entscheidend ist und aus der die notwendigen Empfehlungen abgeleitet werden. Die mit dieser Methode erzielten Ergebnisse liefern die Grundlage für die weitere Vorgehensweise und bilden den notwendigen Konsenz bei allen Beteiligten. Die weiteren Schritte und Maßnahmen werden dann den jeweils Verantwortlichen aufgetragen und ein Zeitrahmen für die Erarbeitung der notwendigen Ergebnisse verabschiedet.

2 IRM-Systeme

IRM, Information Rights Management Systeme, bilden ein Herzstück im Bereich der Unternehmenssicherheit. Im Gegensatz zu Virenschernern, Firewalls oder anderer Sicherheitssoftware schützen sie Dokumente und Inhalte nicht nur innerhalb einer Organisation vor unberechtigten Zugriffen sondern auch außerhalb an jeder beliebigen Stelle.

Ein IRM-System ist eine Software, die es ermöglicht digitale Inhalte mit dazugehörigen Eigentümer- und Nutzerrechten binär zu verschlüsseln. Dabei werden die Inhalte und ihre Rechte auf separaten Systemen gespeichert. Nur autorisierte Nutzer haben die Möglichkeit auf die versiegelten Dokumente zuzugreifen. Die Rechte können jederzeit erteilt, geändert oder wieder entzogen werden. Bevor ein Dokument auf einem Clienten geöffnet werden kann, werden die Rechte dazu auf einem Server überprüft und mit entsprechenden Schlüsseln bestätigt. Nur durch die vom Server erzeugten Schlüssel erhält der Client die Berechtigung die Datei zu öffnen.

Einsatzmöglichkeiten und Berechtigungen

Eine der vielen Einsatzmöglichkeiten eines IRM-Systems besteht darin schützenswerte Inhalte zu versiegeln damit sie vor unberechtigten Zugriffen geschützt sind. Dadurch erhalten nur noch Personen die Möglichkeit diese Inhalte anzusehen, zu kopieren, zu drucken oder zu ändern, die dazu berechtigt sind. Berechtigungen können speziell auf einzelne Benutzer oder Gruppen zugeschnitten werden. Eine Weitergabe der geschützten Inhalte ist

ohne Einschränkung möglich, auch das Sichern auf externen Medien oder Notebooks. Bevor ein Dokument jedoch verwendet werden kann, muss eine Authentifizierung des Benutzers auf einem IRM-Server stattfinden. Dieser verifiziert die Identität und liefert entsprechende Konvertierungsschlüssel im Falle eines berechtigten Benutzers. Unberechtigte Benutzer haben keine Möglichkeit versiegelte Dokumente zu öffnen, da sie vom IRM-Server nicht authentifiziert werden und daher auch keine Schlüssel erhalten. Ihre Zugriffsversuche werden jedoch protokolliert, sofern die entsprechende Funktion auf dem Server aktiviert ist.

Der Einsatz eines IRM-Systems ist prinzipiell für jeden Benutzer und jede Organisation sinnvoll, die über schützenswerte Informationen verfügt. Schützenswerte Inhalte sind zum Beispiel nicht nur geistiges Eigentum, sondern jede Art von vertraulichen Informationen, die nicht in unberechtigte Hände gelangen sollen. Dies können Geschäftsberichte, Gesprächsprotokolle eines Firmenvorstands, einer Geschäftsleitung oder eines Aufsichtsrats, komplexe technische Dokumente, Personalverträge, Statistiken, Daten und Belege von Mandanten und alle anderen Arten von rohen oder aufbereiteten Daten sein, die sich in Dateien ablegen lassen.

Einen Großteil dieser Informationen findet man in Form von Office-Dateien oder PDF-Dokumenten. Aber auch Musik, Bilder, Videos und viele weitere können darunter fallen.

Informationen oder aufbereitete Inhalte sind dann als schützenswert zu erachten, wenn nur eine eingeschränkte Anzahl von Benutzern darauf Zugriff erhalten soll. Informationen, die der Öffentlichkeit beispielsweise auf einer Internetseite zur Verfügung gestellt werden sollen, fallen nicht unbedingt darunter, können aber als Bestandteil eines Content Management-Systems durchaus geschützt werden damit sie nur von berechnigte Personen geändert werden können.

Doch jede Art von persönlichen Dokumenten, wie beispielsweise der eigene Arbeitsvertrag, Bewerbungsunterlagen, die Steuererklärung, Briefe, Gehaltsinformationen und vieles andere haben in fremden Händen nichts zu suchen. Auch der Umgang mit Geschäftsunterlagen, wie Verkaufszahlen, Forecasts, geplante organisatorische Änderungen oder prozessbegleitende Informationen sind absolut schützenswert, da sie in Händen von

Wettbewerbern große Schäden für das eigene Unternehmen bewirken können.

IRM-Systeme können noch viele andere Aufgaben übernehmen bei denen es in irgendeiner Form um Zugriffsberechtigungen geht. Man kann sie auch in unternehmensweite Content-Management-Systeme integrieren und in Kommunikationsplattformen. Man kann sie auch als Bestandteil einer unternehmensweiten Sicherheitsstrategie nutzen und dafür sorgen, dass sowohl die Mitarbeiter als auch das Unternehmen optimal geschützt sind. Der Vollständigkeit halber muss man jedoch darauf hinweisen, dass auch IRM-Systeme nicht vollständig gegen kriminelles Vorgehen schützen können. Sie erschweren aber sehr wirkungsvoll den Zugriff auf geschützte Informationen und bieten aktuell einen sehr guten Schutz über lange Zeiträume für jeden Anwender.