Datenkontrolle mit Software für Informationsrechteverwaltung

Dennis Scherrer

BLUESITE Beratungsgesellschaft für die
Informationstechnologie mbH
scherrer@bluesite.de

Zusammenfassung

Digitale Rechteverwaltung (englisch Digital Rights Management, kurz DRM) unterstützt bei der Einhaltung (englisch Compliance) von Informationsrechten, bspw. wenn ein nicht übertragbares Anrecht auf Information einräumt wurde. Dazu werden die zu schützenden Daten (Schutzziel „Vertraulichkeit“) mit jeweils für die Daten individuellen, symmetrischen Schlüsseln verschlüsselt. Dieses symmetrische Schlüsselmaterial wird mit asymmetrischen Schlüsseln verschlüsselt und mit einem zentralen Schlüsselmanagement ausgetauscht. Diese, durch Kryptografie geschaffene Umgebung, räumt Informationsrechte der im Schlüsselaustausch eingebundenen Software ein, in der die Übertragung der Informationsrechte jeweils kontrolliert wird. Der Beitrag zeigt zunächst auf wie diese eingerichtet wird, welche Komponenten und Methoden verwendet werden, und wie es sich eine Implementierung auf das Risikobild auswirkt. Alternativ oder ergänzend lassen sich die Datenweitergabe genutzten Schnittstellen blockieren (Data Loss/Leak Prevention, kurz DLP), es wird verdeutlich worin der Unterschied zwischen DRM und DLP begründet liegt.

1 Analyse Hardware-unabhängige DRM-Software

1.1 Systemüberblick

Wenn eine Software DRM-Funktionen unterstützt, d.h. die Kontrolle der Informationsrechte erlaubt, wird dieser der symmetrische Schlüssel zur Entschlüsselung der Daten vom Schlüsselspeicher überlassen. Die Software-Komponente Schlüsselspeicher ‚vertraut‘ zu diesem Zweck der Software.

Die Informationsrechte selbst werden Benutzern zugeschrieben, die dem Schlüsselspeicher mittels des Zertifikates der Benutzer-Zertifizierungsstelle vertraut sind, vergleichbar einer Zugriffssteuerungsliste eines Dateisystems.

Dieses jeweilige ‚Vertrauen‘ basiert bspw. bei Software mit DRM-Funktionen (Abbildung1 rechts) zum einen auf einem Hashwert des Programmcodes (Integrität des Programmcodes) und zum anderen auf einer digitalen Signatur eben dieses Hashwertes durch die Software-Zertifizierungsstelle (Abbildung1 rechts oben). Beim Benutzer der auf DRM-geschützte Inhalten zugreifen möchte, verhält es sich ähnlich: Identifikation an der Komponente Benutzer Zertifizierungsstelle (Abbildung1 links) mittels eines Identitätsmerkmals und eines mit der Komponente

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 170-178.

geteilten Geheimnisses; bspw. Benutzername/E-Mail-Adresse (Identitätsmerkmal) und Password (geteiltes Geheimnis). Die kryptografischen Methoden sind heute in vielen Software-Umgebungen/Betriebssystemen praktisch implementiert und bspw. in [AJM96] beschrieben.

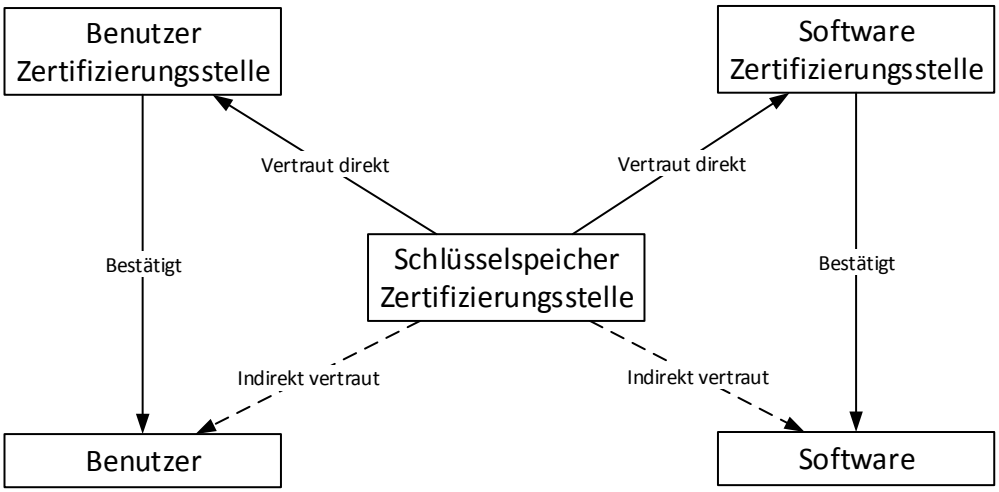

Abb. 1: Digitales Rechtemanagement mit Zertifikaten: System

Die Abbildung 1 zeigt die resultierenden Vertrauensbeziehungen. Zertifizierungsstellen für Software und Benutzer ermöglichen jeweils mehrere verschiedene Benutzer und verschiedene Software. Der Schlüsselspeicher ‚vertraut' mehreren Benutzern und mehreren Kopien der Software, da deren Zertifikate jeweils mit dem öffentlichen Zertifikat der jeweiligen Zertifizierungsstelle signiert sind.

1.2 Einrichten und Ausführung ‚vertrauten Umgebung'

1.2.1 Beispiel der Funktion zur Verschlüsselung

Um das symmetrische Schlüsselmaterial auf wechselnder Hardware, mit mehreren Benutzern für den Zugriff auf die Daten auszutauschen, wird wie folgt eine ‚vertraute' Laufzeitumgebung eingerichtet (nachfolgend ‚Instanz').

Nur ein vertrauter Benutzer (siehe Abbildung1) erhält nach dem Start der DRM-Software ein Schlüsselpaar (öffentlichen und privaten Schlüssel) zur Einrichtung einer Instanz.

Da es mit dem öffentlichen Schlüssel des Benutzers verschlüsselt wurde lässt sich das Schlüsselpaar eben nur mit dem privaten Schlüssel, eben also durch den Benutzer entschlüsseln.

Die eigentlichen zu verschlüsselnden Daten werden mit schnelleren - und damit für größere Datenmengen als lediglich Schlüsselmaterial < 1 MB geeigneten - symmetrischen Methoden verschlüsselt.

Nur der Schlüsselspeicher entschlüsselt den Schüssel für die symmetrische Verschlüsselung, welcher vom der Software-Instanz generiert wurde, da dieser mit dem öffentlichen Zertifikat des Schlüsselspeichers verschlüsselt wurde. Dass dieser Schlüssel aus der Instanz stammt belegt die Signatur mit temporären Schlüsseln der Instanz, die eingangs an die Software übergeben wurden.

Eine Liste der Informationsrechte wird ebenfalls mit dem zu den Daten gehörenden symmetrischen Datenschlüssel verschlüsselt und gemeinsam mit den Daten bspw. in einer Datei in einem Dateisystem gespeichert.

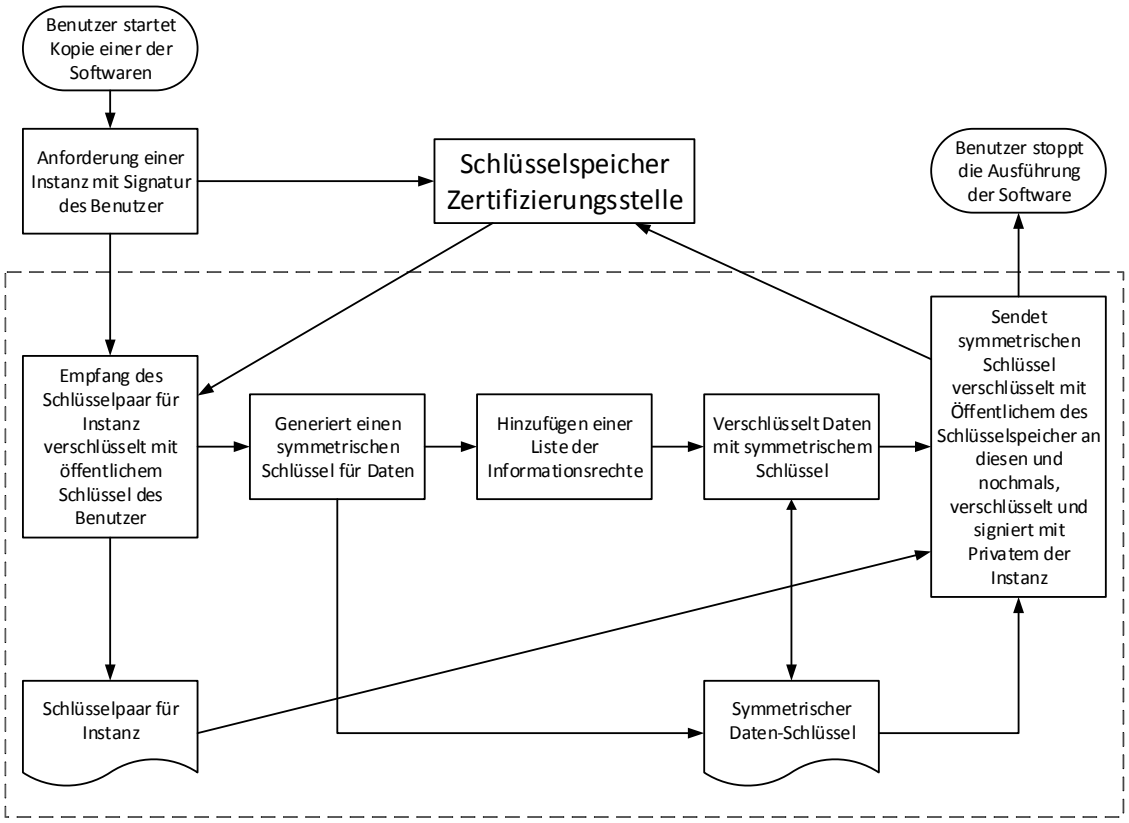

Abb. 2: Digitales Rechtemanagement mit Zertifikaten: Schreiben

Bei dieser Vorgehensweise werden auch private Schlüssel (für die Einrichtung der Instanz) übertragen! Geschützt wird dieses Schlüsselmaterial für asymmetrische Verschlüsselung durch eine kürzere Gültigkeitsdauer das Zertifikates mit privatem Schlüssel relativ zur Schlüssellänge des Schlüsselmaterials der Krypto.-Umgebung: es wird darauf spekuliert, dass die Schlüssel der Sitzung/Instanz nicht kompromittiert werden in der Kürze der Gültigkeit der Benutzerzertifikates.

1.2.2 Beispiel einer Funktion zur Entschlüsselung

Eine Instanz der Laufzeitumgebung wird auch beim Entschlüsseln verwendet. Bei der Entschlüsselung werden die Liste der Informationsrechte und die Daten entschlüsselt. Die vertraute Software bietet Funktionen gemäß den bei den Daten gespeicherten Informationsrechten. Die Software durchläuft dafür eine Qualitätssicherung vor Einrichten des ‚Vertrauens' seitens des Schlüsselspeichers.

Abbildung3 zeigt, dass sowohl der private Schlüssel der Instanz (welche wiederum vom Schlüsselspeicher an die Software übergeben wurden), als auch der private Schlüssel des Benutzer benötigt werden um den vom Schlüsselspeicher zur Verfügung gestellten Schlüssel für die symmetrische Inhaltsverschlüsselung zu erhalten.

Es wird deutlich, dass die Software danach über den Schüssel für die Inhaltsentschlüsselung verfügt. Die Vertrauenswürdigkeit dieser Software wird durch zusätzliche Krypto.-Umgebungen geschützt (siehe Abbildung1) - siehe auch Angriffe 3.3.2 und Maßnahmen 3.4.4.

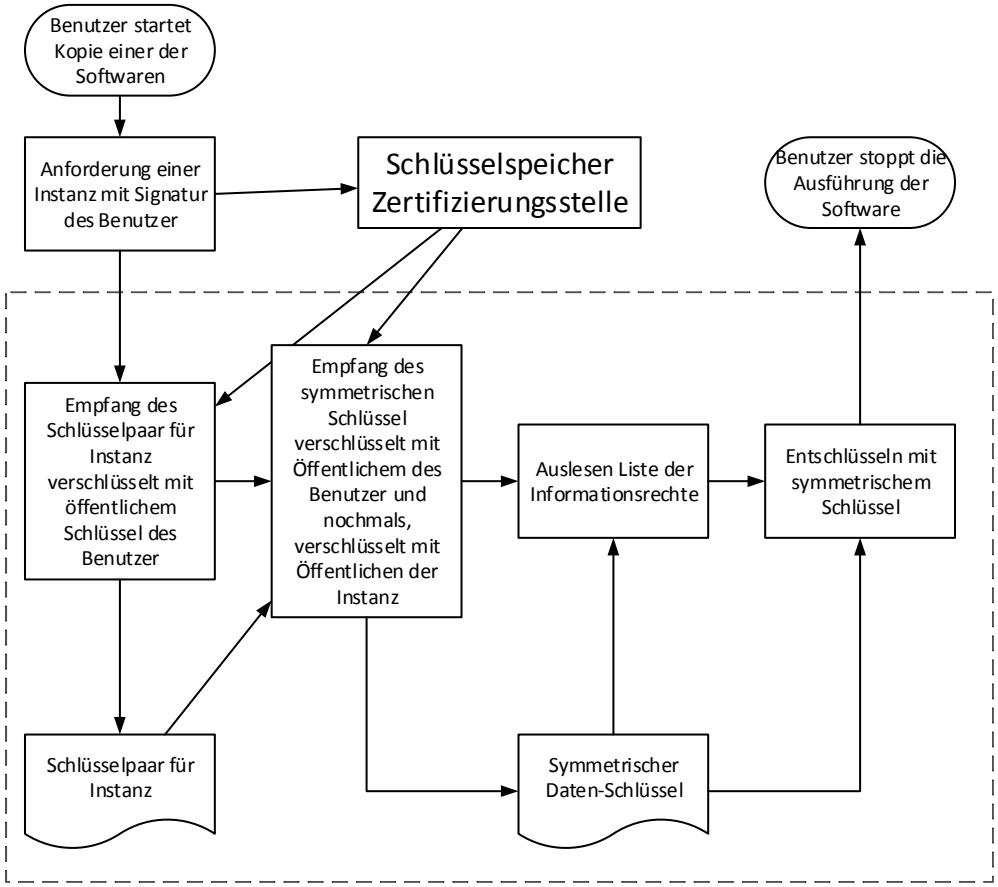

Abb. 3: Digitales Rechtemanagement mit Zertifikaten: Lesen

2 Identitäts- und Schlüsselmanagement bei DRM

Die Komponente ‘Schlüsselspeicher Zertifizierungsstelle‘ signiert zum einen die Instanzen mit einer relativ kurzen Gültigkeitsdauer. Zum anderen werden dort die jeweiligen, symmetrischen Datenschlüssel mit denen die Informationsrechte-Liste und die Daten selbst verschlüsselt sind, gespeichert. Die symmetrischen Datenschlüssel werden in der vertrauten Software-Kopie generiert.

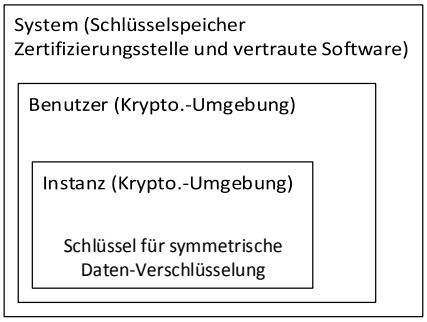

Abb. 4: Digitales Rechtemanagement mit Zertifikaten: Schema

Das Schema verdeutlicht den Schutz des Schlüsselmaterials für symmetrische Verschlüsselung durch die Laufzeitumgebung (Instanz). Der jeweiligen Instanz wird auf Grundlage des Material

für asymmetrische Verschlüsselung der Benutzer und der Software durch das System vertraut (siehe Abbildung 1).

2.1 Verschlüsselung beim Formular-/Dokumentenschutz

Zum Schutz der Vertraulichkeit (Schutzziel) von Formularen und Dokumenten (allgemein hier Daten) kommen symmetrische Verschlüsselungsverfahren zum Einsatz.

Word, Excel und PowerPoint (nachfolgend Dokumente) verwenden ein bis zu 255 Zeichen langes Kennwort für AES Verschlüsselung [MSFT07]. OpenOffice [OASI11] und LibreOffice bieten nach OpenDocument Version 1.2 Kennwortschutz mit Blowfish anstelle von AES. Auch das Öffnen einer PDF Datei (Formular und Dokument, allgemein ‚Daten') lässt sich durch ein Kennwort kontrollieren (bspw. bei Adobe eben AES).

Tab. 1: Anwendungsbeispiele

Beispiele	
Adobe Acrobat Pro	Sicherheitsoptionen (AES-Verschlüsselung), Einschränkung für Bearbeitung und Drucken des Dokuments
PDFCreator	PDF Verschlüsseln mit AES und schützen mit Kennwort.
Microsoft Office	AES-Verschlüsselung von Dokumenten

Quellen dieser Beispiele finden sich im Anhang bei ‚Literatur' [ABSP01…03].

2.2 Zentraler Schlüsselspeicher

Wird jede Datei mit Daten, unter Verwendung eines jeweils individuellen Schlüssels wahlweise nach Anwendung mit AES oder Blowfish verschlüsselt, wird die Notwendigkeit einer Verwaltung (englisch Management) für das Schlüsselmaterial deutlich.

Alternativ zur Verschlüsselung der Dateien und der Verwaltung der Schlüssel, wird diese Dokumentenverschlüsselung auch ersetzt durch die Verschlüsselung des Speicherortes selbst oder des Transportweges.

Tab. 2: Alternativen (Auszug)

Beispiele	
BitLocker	Laufwerkverschlüsselung Windows 7
TLS Protocol	Netzwerk-Transportverschlüsselung

Quellen dieser Beispiele für Alternativen im Anhang bei ‚Literatur' [ABSP04…05].

Bei diesen Alternativen wird eine Überwachung des Datenabflusses an den logischen Schnittstellen, die zu Speichern oder Transport ohne Verschlüsselung führen, durchgeführt. Kurzum eine Überwachung ungewollten Datenabflusses (englisch Data Loss/Leak/Leakage Prevention, kurz DLP).

Beim Einsatz eines zentralen Schlüsselmanagements für Datei-Schlüssel hingegen wird der symmetrische Schlüssel nur an vertraute Software, die die zur Datenweitergabe integrierten Funktionen kontrolliert, weitergegeben (Informationsrechteverwaltungs-Software, kurz IRM).

Tab. 3: Beispiele Informationsverwaltungs-Software

Beispiele	
Adobe	Adobe LiveCycle Rights Management ES4
EMC	Documentum Information Rights Management (IRM)
Microsoft	Microsoft Active Directory-Rechteverwaltungsdienste
Oracle	Oracle Access Management

Quellen dieser Beispiele für Alternativen im Anhang bei ‚Literatur' [ABSP06…09].

3 Planung und Implementierung für Organisationen

Im Rahmen der Implementierung von Informationstechnik (Software und Hardware) für die Informationsrechteverwaltung (englisch Information Rights Management, kurz IRM) bietet sich eine Risikoanalyse an. Risiken sind bspw. nach Handelsgesetzbuch bei großen Kapitalgesellschaften jährlich im Lagebericht auszuweisen (‚nichtfinanzielle Leistungsindikatoren' HGB § 289, Abs. 3).

3.1 Relevante Schutzbedarfe

DRM leistet einen Beitrag zum Schutzziel 'Vertraulichkeit', da gespeicherte Kopien der Daten zur unverschlüsselten Anzeige mit dem Schlüsselmaterial entschlüsselt werden. Durch die notwenige Kryptografie erhöht sich dich Komplexität, was das Schutzziel ‚Verfügbarkeit' berührt.

- Schutzziel ‚Vertraulichkeit'
- Schutzziel ‚Verfügbarkeit'

3.2 Ergänzung der Risikobetrachtung

3.2.1 Unberechtigter Zugriff auf die Informationen erhalten

Ziel eines DRM für Dokumente und Formulare ist es, eine hohe Vertraulichkeit (Schutzziel) für die betroffenen Daten zu erreichen. Dem entgegen steht das Risiko; dass ein nicht autorisierter Zugriff auf die Daten erfolgt.

- Schutzziel 'Vertraulichkeit': erhöht

3.2.2 Berechtigte greifen nicht mehr auf Daten zu

Da DRM-geschützte Daten verschlüsselt gespeichert werden, reduziert dies die Verfügbarkeit: das Ausgeben der Daten erfordert die Entschlüsselung, die nur mit dem entsprechenden Schlüsselmaterial aus dem Zentralen Schlüsselspeicher möglich ist. Selbst wenn das Schlüsselmaterial (also der Zentrale Schlüsselspeicher) höchst verfügbar ist, reduziert alleine die Abhängigkeit von diesem die Verfügbarkeit der Daten.

- Schutzziel 'Verfügbarkeit': verringert

3.2.3 Gewichtung der Risiken

Die gegenläufigen Einflüsse auf die Schutzziele 'Verfügbarkeit' und 'Vertraulichkeit' fließen in die Risikobetrachtung des Zieles der Organisation, der Mission, des Unternehmens ein. Je nach möglicher Schadenssumme einzelner Risiken wird jeweils individuell gewichtet werden.

3.3 Angriffe

Im Folgenden ein Auszug möglicher und wahrscheinlicher Angriffe auf ein DRM/IRM. Viele weitere Angriffe würden in entsprechende Konzeptionen zur Implementierung aufgenommen.

3.3.1 Hardware: Übertragung am Ausgabegerät

Die zu schützenden Informationen werden am wiedergebenden Gerät optisch kopiert. Beispiel Smartphone-Kamera am Arbeitsplatzcomputer mit sensiblen Dokumenten/Daten.

3.3.2 Manipulierte Software erhält Schlüsselmaterial

Das Qualitätsmanagement für die Software zum Laden/Verschlüsseln der Daten hat versagt, die Software ist manipuliert ausgeliefert und bietet nicht erlaubte Funktionen.

3.4 Maßnahmenverzeichnis

Folgende Maßnahmen oder Merkmale wirken sich ggf. mindernd auf den Risikobericht aus, sind jedoch nur ein Auszug der Punkte für eine Implementierung eines solchen Systems.

3.4.1 Ad-hoc Entschlüsselung

Es wird eine Methode geschaffen, die die mit jeweils individuellem, symmetrischem Schlüsselmaterial verschlüsselten Daten (Dateien) auf Anforderung automatisiert entschlüsselt. Diese Methode wird bei einem drohenden Verlust des Zentralen Schlüsselmanagements angewendet oder bei Abschaltung/Außerbetriebnahme der Informationstechnik zur Informationsrechteverwaltung.

3.4.2 Aufbewahrung unverschlüsselter Kopien

Hierbei werden von den jeweils mit individuellem, symmetrischem Schlüsselmaterial verschlüsselten Daten (Dateien) unverschlüsselte Kopien gespeichert.

Die Frische der unverschlüsselten Kopien gegenüber dem verschlüsselten Material entscheidet über die Wirksamkeit dieser Maßnahme (Schutzziel Verfügbarkeit und Freshness).

Denkbar ist ebenfalls, das Informationsrechtemanagement/DRM lediglich bei Kopien der Dateien anzuwenden, die einem größeren Nutzerkreis zur Verfügung gestellt werden und damit einem höheren Risiko ausgesetzt sind. Praxis-Beispiele von DRM finden sich hierzu bei Medien-Verteilung (E-Books, Filmproduktionen, Audio-Dateien). Eben dann, wenn eine (Massen-)Verteilung (englisch Distribution) Bestandteil der Anwendung ist.

3.4.3 Integration eines Speichersystems für RAW-Kopien

Wie bei Punkt 3.4.2 werden hier RAW Dateien aufbewahrt. Hier jedoch in der Form, dass die Dateien verschlüsselt werden, sobald diese vom Speichersystem zu einem weiteren System übertragen werden. Praxis-Beispiel: Herunterladen von Dokumenten aus einem elektronischen Inhaltsverwaltungssystem für Geschäftsdaten (englisch Enterprise Content Management, kurz ECM) [MSFT10].

3.4.4 Vertrauenswürdige Computerplattform

Eine vertrauenswürdige Computerplattform (englisch Trusted Computer Plattform), erschwert das Einschleusen manipulierter Software, die Schlüsselmaterial unberechtigt abgreift oder unberechtigterweise Funktionen zu Datenabgriff anbietet. Software wird vor Installation auf Hardware auf eine gültige, digitale Signatur überprüft. Dies würde bei Starten der Hardware und der Ausführung der Betriebssystemsoftware mit sicherem Code aus der Firmware beginnen.

3.5 Microsoft Rights Management

Verzeichnis der Informationsrechte bei Microsoft Software, Stand Server-Version 2012 R2 (Windows Version 6.3.9600).

Tab.4: Informationsrechte bei Microsoft

Benutzerrechte (Auszug aus Richtlinie)	Verfügbar in Office 2013 als
Vollzugriff	Zugriffsebene: Vollzugriff
Rechte anzeigen	Zugriffsebene: Vollzugriff
Rechte bearbeiten	Zugriffsebene: Vollzugriff
Ansicht	Zugriffsebene Lesen
Bearbeiten	Zugriffsebene Ändern
Drucken	Inhalt Drucken
Exportieren (Speichern unter)	Benutzern mit Lesezugriff das Kopieren des Inhalts erlauben
Bei jedem Zugriff auf den Inhalt neue Nutzungslizenz anfordern (…)	Immer verbinden, um Berechtigungen eines Benutzers zu prüfen

4 Fazit: DRM vergleiche DLP

Ein DRM (Digitales Rechtemanagement) für Dokumente und Formulare erhöht die Vertraulichkeit von Daten durch

- Verschlüsselung der Dateien und
- Kontrolle der Informationsrechte an den Daten

in der jeweiligen Software (siehe Beispiele in Tabelle der Informationsrechte bei Microsoft). Bei Medien (1:n Empfänger) ist der Begriff DRM gebräuchlich - bei Dokumenten und Formularen der Begriff Informationsrechteverwaltung (englisch, kurz IRM).

Dem gegenüber stehen

- verschlüsselter Transport und Speicherung und
- Verhindern der Datenweitergabe an den Schnittstellen.

Dies ist unter dem Begriff DLP (kurz, englisch für Data Loss/Leak/Leakage Prevention) zusammengefasst.

Der entscheidende Unterschied besteht dahin, dass DRM in der Software zur Anzeige/Ausgabe/Bearbeitung der Informationen integriert ist, DLP vielmehr Funktionen dieser Software

einschränkt. Ersteres scheint der effizientere Weg: er setzt entsprechend aufeinander abgestimmte Software voraus. Mangels fehlender Standards setzten sich hier scheinbar marktbeherrschende Anbieter durch.

Literatur

[MSFT07] Microsoft Corporation (MSFT): Password protect documents, workbooks, and presentations, 2007. http://Office.com

[UBM06] UBM LLC. (UBM): EMC Acquires Authentica, 2006. http://www.networkcomputing.com/storage/emc-acquires-authentica/d/d-id/1216228?

[OASI11] OASIS (OASI): Open Document Format for Office Applications (OpenDocument) Version 1.2, 3.4.2 Encryption Process, 2011. http://docs.oasis-open.org/office/v1.2/os/OpenDocument-v1.2-os-part3.html

[ABSP01] http://help.adobe.com/de_DE/acrobat/pro/using/WSD012A4E1-51D1-4bcd-BA9F-EF03C6F20BB6.html

[ABSP02] http://de.pdfforge.org/pdfcreator

[ABSP03] http://office.microsoft.com/en-us/word-help/password-protect-documents-workbooks-and-presentations-HA010148333.aspx

[ABSP04] http://windows.microsoft.com/de-DE/windows7/products/features/bitlocker

[ABPS05] https://tools.ietf.org/html/rfc2246

[ABPS06] http://www.adobe.com/de/products/livecycle/modules.displayTab3.html

[ABPS07] http://www.emc.com/enterprise-content-management/information-rights-management.htm

[ABPS08] http://technet.microsoft.com/de-de/windowsserver/dd448611.aspx

[ABPS09] http://www.oracle.com/us/products/middleware/identity-management/access-management/overview/index.html

[MSFT10] Microsoft Corporation (MSFT): Architektur des IRM-Frameworks in SharePoint Foundation, 2010.
http://msdn.microsoft.com/de-de/library/ms439625(v=office.14).aspx

[AJM96] Alfred J. Menezes: Handbook of applied cryptography. CRC Press LLC, 1996.

[BS05] Bruce Schneier: Angewandte Kryptographie - Der Klassiker. Protokolle, Algorithmen und Sourcecode in C., WILEY, Ausgabe 2005.