novaCapta
SOFTWARE & CONSULTING

Dokument vom 10.06.2015

Zu dem Thema

„Verwalten von Dateizugriffsrechten mit Microsoft Rights Management Services“

TIMETOACT GROUP
SOFTWARE & CONSULTING

von novaCapta GmbH
Yvonne Melzer
Im Zollhafen 18
50678 Köln
Tel.: +49 (221) 58919343
Mobil: +49 (151) 54410950
E-Mail: y.melzer @novacapta.de

Verwalten von Dateizugriffsrechten mit Microsoft Rights Management Services

Inhalt

Verwalten von Dateizugriffsrechten mit Microsoft Rights Management Services 3
Folgende Möglichkeiten bieten die Microsoft RMS 4
Innovation der Azure RMS im Vergleich zu den Active Directory RMS 4
Einrichtung der Microsoft RMS 5
Systemvoraussetzungen für Microsoft RMS 5
Welches RMS-Abonnement benötige ich? 5
Betriebssysteme und Anwendungen, die RMS unterstützen 6
Vorbereitungen für die Nutzung von RMS 6
Zwei Möglichkeiten der Verwaltung des zentralen RMS-Mandantenschlüssels 7
Die Anwendung von RMS in der Unternehmenspraxis 7
Dokumente mit Microsoft Office schützen 7
RMS in Word, Excel und PowerPoint 8
RMS in Outlook 11
RMS in PDF-Readern 13
Dokumentenrechte im Foxit Reader verwalten 13
Weitere RMS-fähige PDF-Reader 16
Microsoft RMS-Freigabeanwendung 18
Dateien verschlüsseln 19
Dateien geschützt versenden 22
Geschützte Dateien öffnen 24
RMS auf mobilen Geräten verwenden 26
RMS mit dem Foxit MobilePDF Reader 27
Die RMS-Freigabeanwendung auf mobilen Geräten 27
RMS bei Dokumentbibliotheken und Listen in SharePoint 28
Zugriffsrechte auf eine Bibliothek mit Hilfe von RMS beschränken 29
RMS-unabhängige Zugriffsberechtigungen in SharePoint 32
Quellen und weiterführende Links 34

Verwalten von Dateizugriffsrechten mit Microsoft Rights Management Services

Dieser Artikel befasst sich mit der Einrichtung und Verwendung der Rechteverwaltungsdienste (Rights Management Services, RMS) von Microsoft, die eine sichere Verschlüsselung von Dateien bieten. Microsoft hat die RMS komplett überarbeitet und sie 2013 mit neuer, Cloud-basierter Topologie eingeführt. RMS bieten umfassenden Schutz von sensiblen Informationen in Dateien und Dokumenten über granulare Einstellungen von Zugriffsrechten, nun auch weitgehend unabhängig von Dateityp, Betriebssystem und Organisation. Für bestimmte Dateien festgelegte Zugriffsberechtigungen bleiben auch nach dem Kopieren oder Weiterleiten von RMS-verschlüsselten Dateien aktiv. Gleichzeitig können autorisierte Personen und Gruppen mit Hilfe der Microsoft RMS je nach zugewiesenen Zugriffsberechtigungen die Dateien weitgehend unabhängig von Benutzergerät (z. B. PC, Tablet oder Smartphone) oder Organisationszugehörigkeit (innerhalb oder außerhalb eines Unternehmens) verwenden. Die benutzerdefinierte Schutzfunktionalität wird in den neuen RMS größtmöglich gehalten bei gleichzeitig minimalem Einrichtungsaufwand für den Benutzer, dank der Cloud-basierten RMS-Topologie.

Zunächst wird ein Überblick zu den Microsoft RMS gegeben. Anschließend wird die Einrichtung der RMS einschließlich der benötigten Voraussetzungen und Vorbereitungen für die Nutzung erläutert. Der restliche Teil des Artikels befasst sich mit der Anwendung von den Microsoft RMS in der Praxis. Die Verwendung der RMS in Microsoft Office (Word, Excel, PowerPoint und Outlook) und in RMS-fähigen PDF-Readern wird zunächst Schritt für Schritt erklärt. Dazu zählen die Verschlüsselung von Word-, Excel-, PowerPoint- und PDF-Dokumenten sowie von E-Mails und die Wiedergabe verschlüsselter Dokumente. Der darauffolgende Abschnitt befasst sich mit der RMS-Freigabeanwendung, welche Dateien jeglichen Dateityps verschlüsseln kann. Die RMS-Freigabeanwendung kann über die in Office und RMS-fähigen PDF-Readern integrierbaren Funktionen oder über den Dateiexplorer verwendet werden, so dass sich sämtliche Dateien mit wenigen Klicks verschlüsseln und auch verschlüsselt per E-Mail versenden lassen. Mit der RMS-Freigabeanwendung lassen sich außerdem verschlüsselte Dateien entschlüsseln bzw. wiedergeben. Dabei ist die RMS-Freigabeanwendung nicht nur für Windows, sondern auch für weitere Betriebssysteme einschließlich mobilen Geräten verfügbar. Die Verwendung dieser Funktionen wird detailliert erläutert. Der letzte Abschnitt befasst sich schließlich mit dem Schutz von Dokumenten innerhalb von SharePoint. Mit Hilfe der Integration der RMS in SharePoint lassen sich Dokumentbibliotheken mit wenigen Klicks RMS-verschlüsseln. Dies bietet einen zusätzlichen Schutz zu den SharePoint-eigenen Zugriffsberechtigungen, da die in RMS-geschützten Dokumentbibliotheken hochgeladenen Dokumente auch außerhalb von SharePoint verschlüsselt bleiben.

Folgende Möglichkeiten bieten die Microsoft RMS

- Dateien unabhängig vom Dateityp schützen (mit unterschiedlichen Schutzleveln: Verschlüsselung von Office-, PDF-, Bild- und Textdateien oder Kapselung mit Autorisierung für alle weiteren Dateitypen)
- Dateien weitgehend unabhängig vom Speicherort bzw. Gerät schützen (durch Unterstützung der wichtigsten Betriebssysteme und Benutzergeräte)
- Dateien mit wenigen Klicks bestimmten Personen geschützt über E-Mail freigeben
- Dateien unabhängig von Administrationsrechten des einzelnen Mitarbeiters schützen (bei minimalem Einrichtungsaufwand für den Einzelnen)
- Granulare Personen- und Gruppen-gerichtete Zugriffsrechte für Dateien benutzerdefiniert oder nach unternehmensweiten Vorlagen festlegen (z.B. das Drucken oder Kopieren des Dokumenteninhalts verhindern oder die zeitliche Gültigkeit eines Dokuments beschränken)
- Inhalte von E-Mails verschlüsseln und nur bestimmten Personen freigeben (z. B. mit alleiniger Leseberechtigung um das Drucken, Kopieren oder Weiterleiten zu verhindern)
- Bestehende Office-Anwendungen, verbreitete PDF-Reader oder kostenlose RMS-Anwendungen für das Schützen von Dateien verwenden (mit wenigen Klicks einzurichten)
- Innerhalb von SharePoint Dateien in Dokumentenbibliotheken schützen
- Die Zugriffe bzw. Zugriffsversuche auf geschützte Dateien nachverfolgen
- Unternehmensweit und unternehmensübergreifend bei der Bearbeitung und Freigabe von geschützten Dateien zusammenarbeiten

Innovation der Azure RMS im Vergleich zu den Active Directory RMS

Es ist zu beachten, dass es derzeit sowohl Azure RMS als auch Active Directory (AD) RMS von Microsoft gibt (für eine Gegenüberstellung siehe hier). Die Azure RMS sind die in 2013 neu eingeführten RMS während die AD RMS bereits länger existieren und auf älteren Strukturen basieren. Dieser Artikel bezieht sich dementsprechend ausschließlich auf die neu eingeführten Azure RMS.

Wesentliche Unterschiede zwischen den RMS-Versionen bestehen darin, dass die älteren AD RMS nicht Cloud-basiert sind sondern nur über lokale Windows Server funktionieren. Der Einrichtungsaufwand für Unternehmen ist somit deutlich höher als mit den Azure RMS. Zudem sind Benutzer von AD RMS abhängig von der RMS-Einrichtung in ihrem Unternehmen, während bei Azure RMS auch eine Einzelperson unabhängig ihres Unternehmens die Azure RMS kostenfrei verwenden kann. Ebenfalls stark eingeschränkt ist die unternehmensübergreifende Zusammenarbeit mit AD RMS, die eine explizite Definition der Vertrauensbeziehungen und eine

entsprechende Einrichtung der Dienste benötigt, während mit Azure RMS jedes beliebige Unternehmen mit anderen auf Basis von RMS kollaborieren kann, solange auf beiden Seiten ein RMS-Abonnement besteht und die Zugriffsrechte entsprechend definiert wurden.

Die neuen Microsoft Azure RMS mit Cloud-basierter Topologie bieten somit im Vergleich zu der älteren AD RMS-Version eine erhöhte Flexibilität für den Dateischutz bei gleichzeitig stark verringertem Einrichtungsaufwand sowohl für das Unternehmen als auch für die Einzelperson. Weitere detaillierte Informationen zu den Funktionen und Grundlagen der neuen Microsoft RMS finden sich hier.

Einrichtung der Microsoft RMS

Systemvoraussetzungen für Microsoft RMS

Welches RMS-Abonnement benötige ich?

Um Microsoft Azure RMS für die Verwaltung von Zugriffsrechten auf Dokumente verwenden zu können, ist ein Cloud-Abonnement von Microsoft notwendig, welches RMS beinhaltet. Das sind die folgenden (Stand 06/2015):

- Office 365 in den Versionen Enterprise E3/E4, Education A3/A4 oder Government G3/G4
- ein eigenständiges Azure RMS-Abonnement (kompatibel zu Office 365, Exchange Online und SharePoint Plänen)
- ein Abonnement der Enterprise Mobility Suite (kompatibel zu Office 365, Exchange Online und SharePoint Plänen)
- ein Abonnement von RMS für Einzelpersonen in einem Unternehmen, welches über kein unternehmensweites Abonnement verfügt.

Die Abonnements sind stets unternehmensbezogen, d.h. Privatpersonen können Microsoft RMS leider noch nicht nutzen. Ein Abonnement von RMS für Einzelpersonen kann individuell über die unternehmensbezogene E-Mail-Adresse kostenfrei erworben werden, falls noch kein unternehmensweites RMS-Abonnement verfügbar ist. Somit können Nutzer unabhängig vom eigenen Unternehmen Dokumente schützen und mit anderen, über ein RMS-Abonnement verfügenden, Personen teilen sowie auf geschützte und mit ihnen geteilte Dokumente zugreifen. Details zur Registrierung für RMS für Einzelpersonen finden sich hier.

Betriebssysteme und Anwendungen, die RMS unterstützen

Auf dem Computer wird RMS in Windows 7, Windows 8/8.1 sowie Mac OS X (10.8 oder höher) unterstützt. Mobile Geräte benötigen Windows Phone 8.1, Android 4.0.3. oder höher, iOS 7.0 oder höher, oder Windows 8 RT/8.1 RT.

Wenn ein RMS-Abonnement vorhanden ist, kann man unter Windows bzw. anderen Betriebssystemen die Microsoft RMS mit diversen Anwendungen verwenden, je nach Dateityp. Für den RMS-basierten Schutz von Word-, Excel- oder PowerPoint-Dateien unter Windows wird Office 2010 Professional (Plus), Office 2013 Professional Plus oder Office 365 benötigt. RMS-unterstützende PDF-Anwendungen unter Windows sind der Foxit Reader (Enterprise/PhantomPDF) oder der Nitro PDF Reader. E-Mails lassen sich unter Windows RMS-verschlüsseln bzw. -entschlüsseln mit den Versionen 2010, 2013 oder Web App von Outlook.

Mit der RMS-Freigabeanwendung alle Dateitypen schützen

Für andere bzw. alle Dateitypen steht die RMS-Freigabeanwendung zur Verfügung, die man sich hier kostenlos herunterladen und installieren kann. Sie wird insbesondere von Einzelpersonen mit RMS Abonnement benötigt, ist aber grundsätzlich sehr nützlich für Unternehmen mit RMS-Abonnement, da sich damit nicht nur Office- oder PDF-Dateien verschlüsseln lassen. Bei Installation der RMS-Freigabeanwendung wird außerdem, soweit vorhanden, in Word, Excel, PowerPoint und Outlook der Versionen Office 2010 und 2013 ein Add-In integriert für erweiterte Sicherheitsfunktionalität bei der Freigabe von Dokumenten. Mehr Details zu den Funktionen der RMS-Freigabeanwendung gibt es im Abschnitt *Microsoft RMS-Freigabeanwendung* dieses Artikels. Zu den allgemeinen Voraussetzungen für die Verwendung von RMS finden sich hier weitere Informationen.

Vorbereitungen für die Nutzung von RMS

Bevor Microsoft RMS verwendet werden können, müssen sie in den relevanten Anwendungen aktiviert werden. Je nach Abonnement müssen die RMS im Office 365 Admin Center bzw. im Azure-Verwaltungsportal von einer Person mit entsprechenden Administrationsrechten aktiviert werden. Wie dazu vorzugehen ist, wird hier beschrieben. Für Einzelpersonen mit RMS Abonnement reicht es, die RMS-Freigabeanwendung herunterzuladen und zu installieren nachdem man sich für ein Einzelpersonen-RMS-Abonnement registriert hat. Soll die RMS-Freigabeanwendung für mehrere Benutzer in einem Unternehmen mit RMS-Abonnement installiert werden, ist nach dieser Anleitung vorzugehen. Die RMS-Freigabeanwendung muss außerdem installiert sein, um in Office 2010 die RMS zu verwenden. Für Office 2013 hingegen ist keine weitere Konfiguration notwendig, außer der allgemein in Office notwendigen Anmeldung mit den Anmeldedaten, die für das RMS-Abonnement registriert sind.

Zwei Möglichkeiten der Verwaltung des zentralen RMS-Mandantenschlüssels

Jedes Unternehmen, das die Microsoft RMS abonniert hat, bekommt (mindestens) einen sogenannten Mandantenschlüssel zugewiesen, der auch als SLC-Schlüssel (Server Licensor Certificate, lizenzgebendes Serverzertifikat) bekannt ist. Alle einzelnen im Unternehmen für die RMS-Ver- und -Entschlüsselung verwendeten Schlüssel werden wiederum mit dem RMS-Mandantenschlüssel verbunden. Standardmäßig wird der Schlüsselverwaltungsprozess von Microsoft durchgeführt, es sei denn, die eigene vollständige Kontrolle über die Schlüsselverwaltung ist gewünscht. In dem Fall kann man einen eigenen Mandantenschlüssel lokal generieren und ihn über sogenannte Hardwaresicherheitsmodule an Microsoft übertragen. Dies ist allerdings nicht für Einzelpersonen mit RMS-Abonnement möglich. Wie die Verfahren der Schlüsselverwaltung in beiden Fällen funktionieren und welche Schritte jeweils nötig sind, wird hier detailliert beschrieben. Wichtig zu wissen ist, dass die verschlüsselten Daten in beiden Fällen nicht von Azure bzw. Microsoft als Teil des Informationsschutzvorgangs gesehen oder gespeichert werden. Die genaue Funktionsweise der Ver- und Entschlüsselung wird hier detailliert beschrieben.

Die Anwendung von RMS in der Unternehmenspraxis

Dokumente mit Microsoft Office schützen

Die Zugriffsbeschränkung bei Microsoft Office Dokumenten, bestehend aus einer Verschlüsselung und Rechteerzwingung, ist nativ und wandert mit dem Dokument: Ob ein Dokument kopiert, in einem anderen Ort gespeichert oder per E-Mail weitergeleitet wird, die Verschlüsselung bleibt aktiv und die zugeordneten Berechtigungen werden beim Öffnen erzwungen und angezeigt. Eine Authentifizierung des Nutzers mit seinem RMS-verbundenen Konto ist zum Öffnen erforderlich. Das heißt, dass vertrauliche Dokumente wie z. B. Verträge an den Vertragspartner mit RMS-Abonnement weitergegeben werden können und dass dieser Vertragspartner die Verträge zwar ansehen und ggf. bearbeiten kann (je nach Rechtevergabe), dass er aber die Verträge nicht an (unbefugte) Dritte durch Kopieren oder Weiterleiten weitergeben kann, da diese (unabhängig davon, ob sie über ein RMS-Abonnement verfügen oder nicht) nicht die entsprechenden Rechte für die Verträge besitzen und dadurch auch die (Kopien der) Verträge nicht öffnen können. Auch das Drucken eines Dokuments, einschließlich Screenshots davon, können in den Zugriffseinstellungen in Microsoft Office verhindert werden. So können sensible Informationen aus einem Dokument weder durch Kopieren und Weiterleiten noch durch Drucken an unbefugte Dritte gelangen. Welcher Vertragspartner oder Mitarbeiter welche Rechte (lesen, bearbeiten, kopieren, drucken, etc.) bekommt, kann individuell festgelegt werden, so dass z. B. ein Mitarbeiter im eigenen Projektteam ein vertrauliches Dokument bearbeiten kann, während der Vertragspartner bzw. dessen Mitarbeiter ggf. nur eine Leseberechtigung bekommen.

Die Zugriffsrechte auf Word-, Excel- und PowerPoint-Dokumente lassen sich auf zwei Arten verwalten: In der jeweiligen Office-Anwendung oder über die (optionale) Microsoft RMS-Freigabeanwendung. In diesem Abschnitt wird die erste der beiden Arten beschrieben. Die zweite Art wird in dem Abschnitt *Microsoft RMS-Freigabeanwendung* erklärt. Die Zugriffsbeschränkung von E-Mails und E-Mail-Anhängen mit Outlook wird ebenfalls in diesem Abschnitt beschrieben.

RMS in Word, Excel und PowerPoint

Die Zugriffsrechte eines Word-Dokuments lassen sich beschränken über Datei > Informationen > Dokument schützen > Zugriff einschränken (siehe Abbildung 1). Bei Excel und PowerPoint findet sich die Zugriffsbeschränkung ähnlich: Datei > Informationen > Arbeitsmappe schützen > Zugriff einschränken, bzw. Datei > Informationen > Präsentation schützen > Zugriff einschränken.

Abbildung 1: Die Option in Word den Dokumentzugriff zu beschränken

Dort hat man die Möglichkeit, zwischen (vom Unternehmen) vordefinierten und benutzerdefinierten Einstellungen („Eingeschränkter Zugriff") zu wählen. Schreibgeschütztes Anzeigen geschützter Inhalte („Vertraulich – Nur Ansicht") sowie Schreib- oder Änderungsberechtigungen für geschützten Inhalt („Vertraulich") sind die zwei in Office 365 vordefinierten Rechtevorlagen. Unter „Eingeschränkter Zugriff" lassen sich eigene Einstellungen für einzelne Benutzer vornehmen, d. h. eine reine Leseberechtigung (kein Ändern, Drucken oder Kopieren des Inhalts) bzw. eine Änderungsberechtigung (inkl. bearbeiten, kopieren und speichern aber ohne drucken; siehe Abbildung 2).

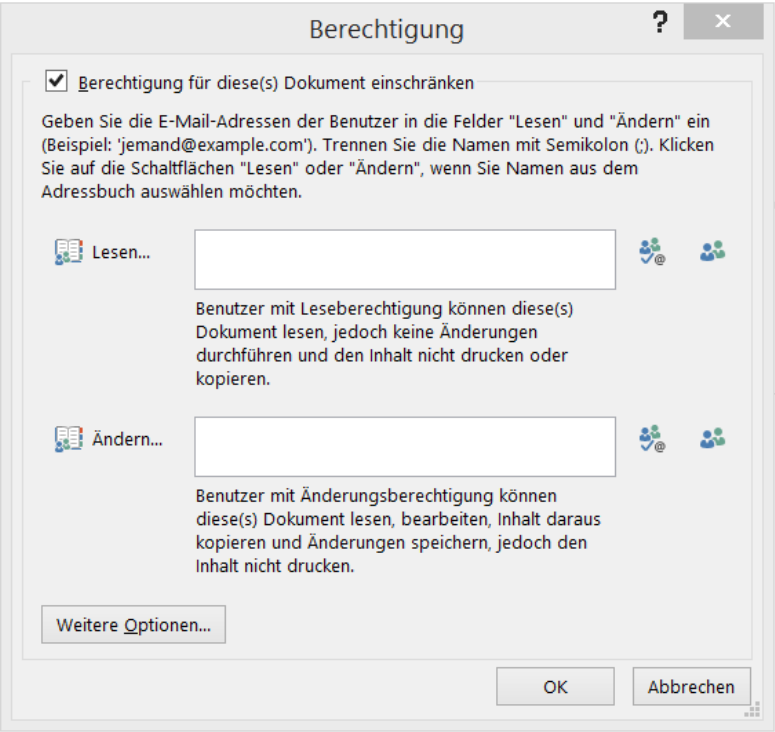

Abbildung 2: Lese- und Änderungsberechtigungen für ein Word-Dokument

Unter „Weitere Optionen“ lassen sich die Zugriffsrechte noch detaillierter bestimmen für einzelne Personen (siehe Abbildung 3). Dort lässt sich auch ein Ablaufdatum einrichten, ab dem der Zugriff auf das Dokument vollständig blockiert wird. Ob das Drucken (einschließlich Screenshots), das Kopieren des Inhalts für Leseberechtigte oder der programmatische Zugriff auf das Dokument erlaubt sein soll, lässt sich ebenfalls festlegen. Bei Bedarf kann man einem Nutzer ermöglichen, zusätzliche Berechtigungen anzufordern oder die Berechtigungsprüfung bei jedem Aufruf des Nutzers anfordern.

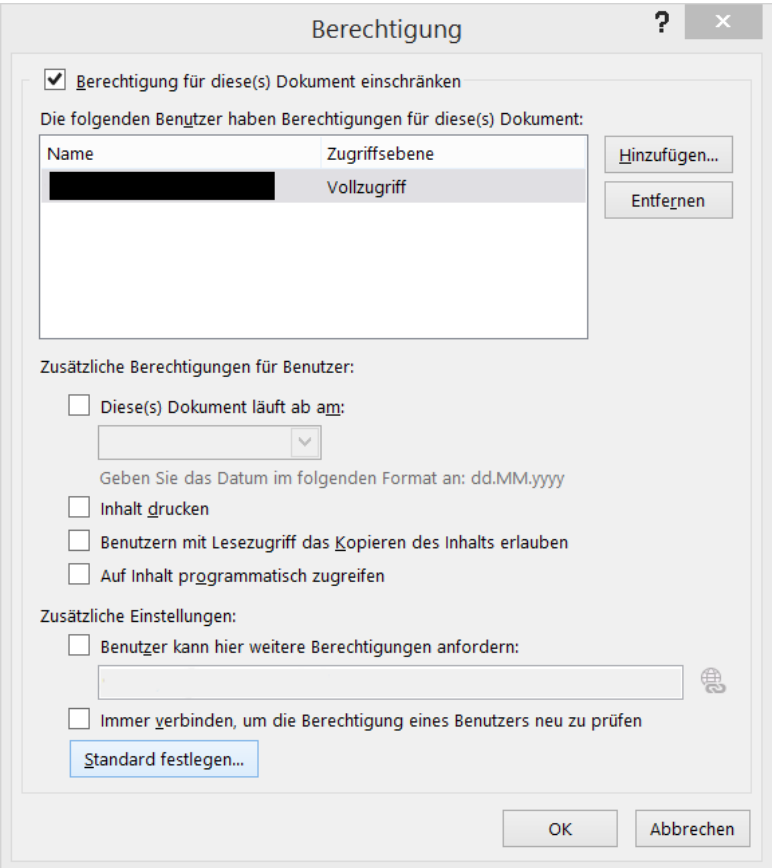

Abbildung 3: Weitere Optionen bei der Berechtigungsvergabe für Word-Dokumente

Als Administrator des Office 365 Kontos kann man weitere Rechtevorlagen definieren, die den Benutzern dann neben den Vorlagen „Vertraulich – Nur Ansicht“ und „Vertraulich“ beim Schützen eines Dokuments zur Auswahl stehen. Hier wird beschrieben, wie man entsprechend vorgeht.

Wenn man die Microsoft-RMS-Freigabeanwendung neben Microsoft Office auf dem PC installiert hat, ist in Word, Excel und PowerPoint eine zusätzliche Option des Dokumentschutzes integriert: Das geschützte Freigeben von Dokumenten per E-Mail, wobei das Office-Dokument als verschlüsselter Anhang einer E-Mail beigefügt wird. Die Option kann aufgerufen werden unter Start > Schutz > Geschütztes Freigeben (siehe Abbildung 4). Näheres dazu, wie man mit Hilfe der RMS-Freigabeanwendung diese Option verwendet und die einzelnen Zugriffsbeschränkungen für bestimmte Personen verwaltet, gibt es im Abschnitt *Microsoft RMS-Freigabeanwendung*.

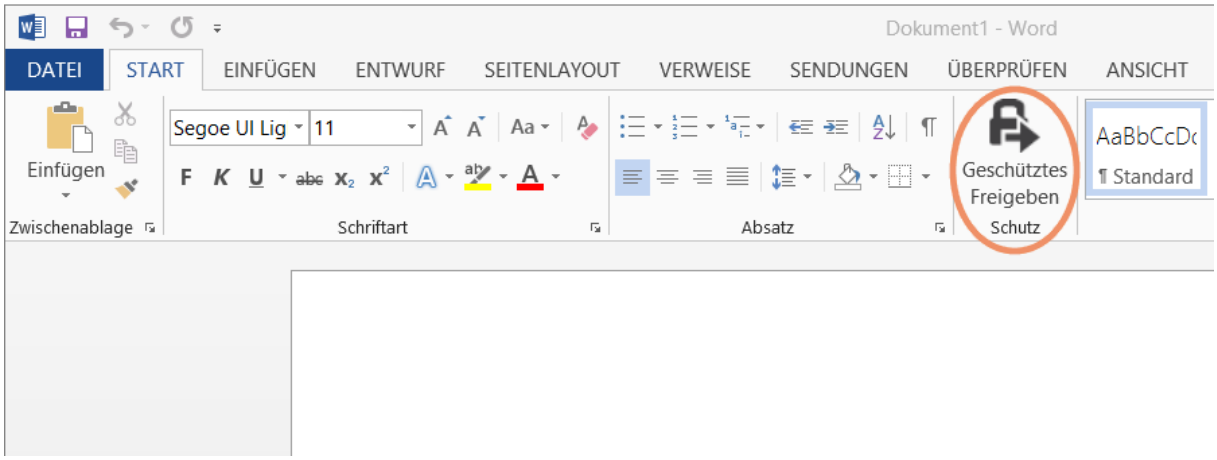

Abbildung 4: Option "Geschütztes Freigeben" in Word

Beim Öffnen von geschützten Word-, Excel- oder PowerPoint-Dateien in der jeweiligen Microsoft Office Anwendung werden die festgelegten Zugriffsrechte automatisch erzwungen. Sie werden dem zugriffsberechtigten Benutzer in einem Hinweis über dem Dokument mit der Möglichkeit angezeigt, die einzelnen Zugriffsrechte darstellen zu lassen oder ggf. als Autor des Dokuments zu ändern (siehe Abbildung 5).

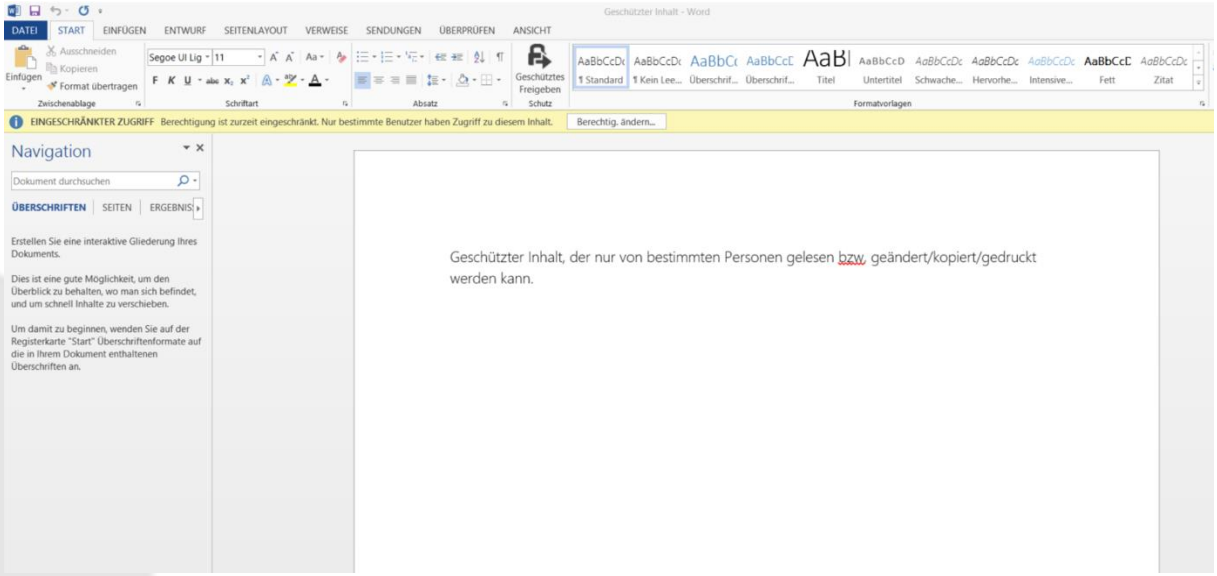

Abbildung 5: Geschütztes Word-Dokument in Word geöffnet

RMS in Outlook

In Microsoft Outlook lassen sich Inhalte einer E-Mail sowie Anhänge verschlüsseln und der Zugriff darauf schützen. Auf diese Weise kann man sensible Informationen, wie z. B. Kontodetails, verschlüsselt an andere Personen verschicken, wobei gleichzeitig verhindert werden kann, dass der Empfänger die Details an unbefugte Dritte weitergeben kann. Die Zugriffsrechte auf den Inhalt

einer E-Mail können im E-Mail-Fenster unter Optionen > Berechtigung angepasst werden (siehe Abbildung 6). Voreingestellte Optionen und die Option „Nicht weiterleiten“ (beinhaltet eine Leseberechtigung aber keine Berechtigung zum Drucken, Kopieren oder Weiterleiten der E-Mail) stehen zur Verfügung, um dem Empfänger der E-Mail nur beschränkte Zugriffsrechte auf den Inhalt der E-Mail zu geben.

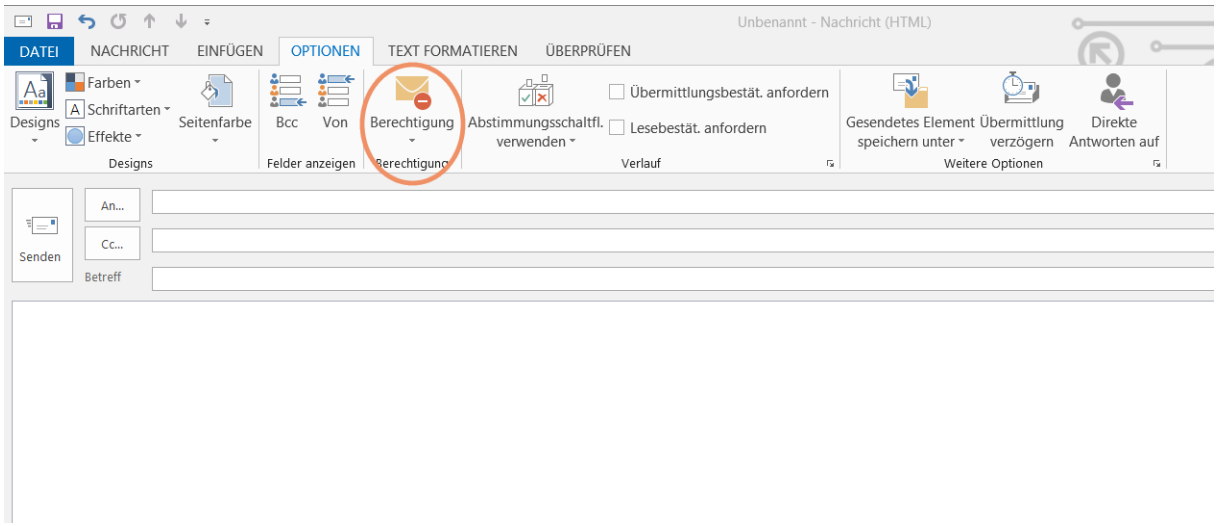

Abbildung 6: Berechtigungseinstellungen bei einer E-Mail in Outlook

Um die Anhänge einer E-Mail zu schützen, ohne vorher die entsprechenden Dateien auf dem PC mit Microsoft Office oder einem RMS-fähigen PDF-Reader geschützt zu haben, kann man in Outlook die zusätzliche Option „Geschütztes Freigeben“ im E-Mail-Fenster unter Nachricht > Schutz > Geschütztes Freigeben verwenden, sofern man die RMS-Freigabeanwendung installiert hat (siehe Abbildung 7). Die angehängten Dateien werden dann mit Hilfe der RMS-Freigabeanwendung verschlüsselt. Näheres dazu gibt es im Abschnitt *Microsoft RMS-Freigabeanwendung*.

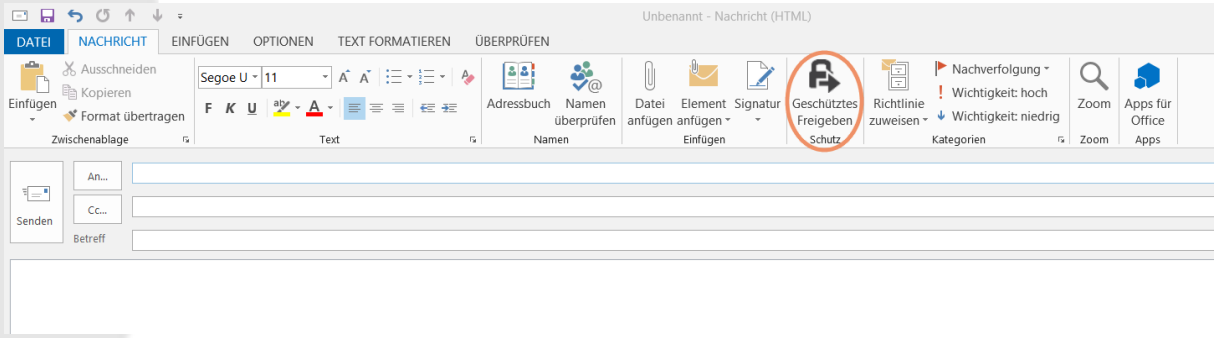

Abbildung 7: Geschütztes Freigeben von E-Mail-Anhängen in Outlook

RMS in PDF-Readern

Auch vertrauliche Dokumente abseits von Microsoft Office lassen sich mit den RMS schützen, wenn ein RMS-Abonnement im Unternehmen bzw. für die Einzelperson besteht. Für die Ver- und Entschlüsselung von PDF-Dateien wird ein Microsoft RMS kompatibler PDF-Reader oder die Microsoft RMS-Freigabeanwendung benötigt. Der Foxit PhantomPDF Business Reader und der Foxit Enterprise Reader unterstützen beide die RMS-basierte Ver- und Entschlüsselung von PDF-Dateien während der Foxit PhantomPDF Standard Reader nur die Entschlüsselung, also das Anzeigen von RMS-geschützten PDF-Dateien, unterstützt. Die Verschlüsselung von PDF-Dokumenten ist, ähnlich wie bei Office-Dokumenten, nativ. Das heißt, dass die festgelegten Zugriffsrechte immer erzwungen werden und auch nach dem Kopieren, Speichern oder Weiterleiten bestehen bleiben. Das heißt, dass auch vertrauliche Dokumente in PDF-Form an entsprechende Vertragspartner oder Teammitglieder zum Lesen oder Bearbeiten weitergegeben werden, ohne dass die Dokumente unverschlüsselt an unbefugte Dritte weitergegeben werden können.

Dokumentenrechte im Foxit Reader verwalten

PDF's verschlüsseln

Ähnlich wie in Microsoft Office lässt sich der Zugriff auf ein geöffnetes PDF-Dokument im Foxit PhantomPDF Business oder Foxit Enterprise Reader mit vordefinierten Rechtevorlagen (z.B. „View Only", eine alleinige Leseberechtigung) oder mit benutzerdefinierten Einstellungen („Restricted Access") verwalten. Die Optionen sind unter Protect > AD RMS Protect > Restricted Access zu finden (siehe Abbildung 8).

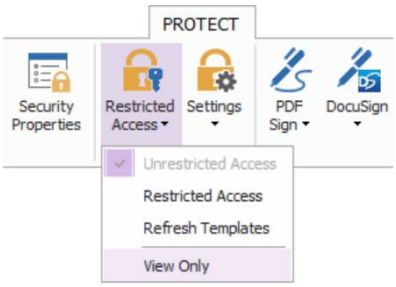

Abbildung 8: Die Option „Beschränkter Zugriff" im Foxit Reader

Beim ersten Zugriff auf ein RMS-geschütztes Dokument per Foxit Reader wird man zur Eingabe des Kontonamens und Passworts (vom Unternehmenskonto, das über ein Microsoft RMS Abonnement verfügt) für die Authentifizierung aufgefordert. Anschließend stehen wie bei Microsoft Office die Einstellungen zur Verfügung, bestimmten Personen eine Leseberechtigung (ohne Ändern, Drucken oder Kopieren des Dokumentinhalts) oder eine Änderungsberechtigung

(inkl. Berechtigungen zum Lesen, Ändern, Kopieren und Speichern aber ohne Druckberechtigung) zu geben sowie weitere Optionen unter „More Options“ in Anspruch zu nehmen, ähnlich wie in Word.

Die weiteren Optionen sind ebenfalls ähnlich wie in Microsoft Office: Man kann für bestimmte Personen detaillierte Zugriffslevel einstellen und zusätzliche Optionen wie Zugriffsablaufdatum, Druckerlaubnis, Kopiererlaubnis, programmatischer Zugriff, Erlaubnisanforderung und Authentifizierungsaufforderungen beim Dokumentenaufruf anwenden (siehe Abbildung 9). Darüber hinaus hat man die Möglichkeit, spezielle Beschränkungen in Bezug auf die Anzahl und Art der Dokumentenzugriffe unter „Extended policy…“ festzulegen sowie Wasserzeichen hinzuzufügen. Mit einem Klick auf „Save as template“ kann man die vorgenommenen Einstellungen als Vorlage für die Wiederverwendung speichern.

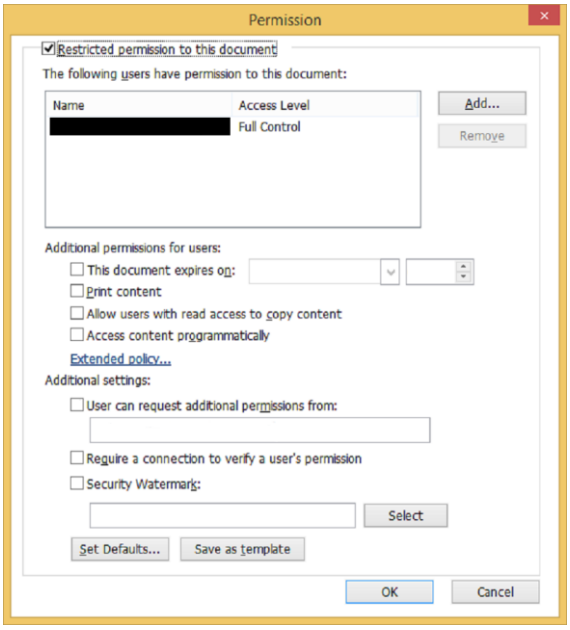

Abbildung 9: Weitere Optionen der Zugriffsberechtigungen im Foxit Reader

Verschlüsselte PDF's öffnen

PDF-Dokumente, die mit einen RMS-unterstützenden PDF-Reader zugriffsbeschränkt wurden, lassen sich mit einer der RMS-unterstützenden Version vom Foxit Reader (PhantomPDF Business oder Standard, Enterprise, oder die kostenlose Version zusammen mit dem Foxit RMS Plug-In) öffnen, wobei die zuvor im Dokument festgelegten Zugriffsbeschränkungen erzwungen werden und man sich entsprechend beim Öffnen der Datei mit dem RMS-verbundenen Konto authentifizieren muss. Beim Öffnen des geschützten Dokuments mit dem kostenlosen Reader mit RMS Plug-In wird ein Wasserzeichen im Dokument angezeigt (siehe Abbildung 10). Es werden

außerdem in jedem der Reader die Bezeichnung und Beschreibung der festgelegten Zugriffsbeschränkungen angezeigt (wie hier im Beispiel „Standard – Nur lesen“).

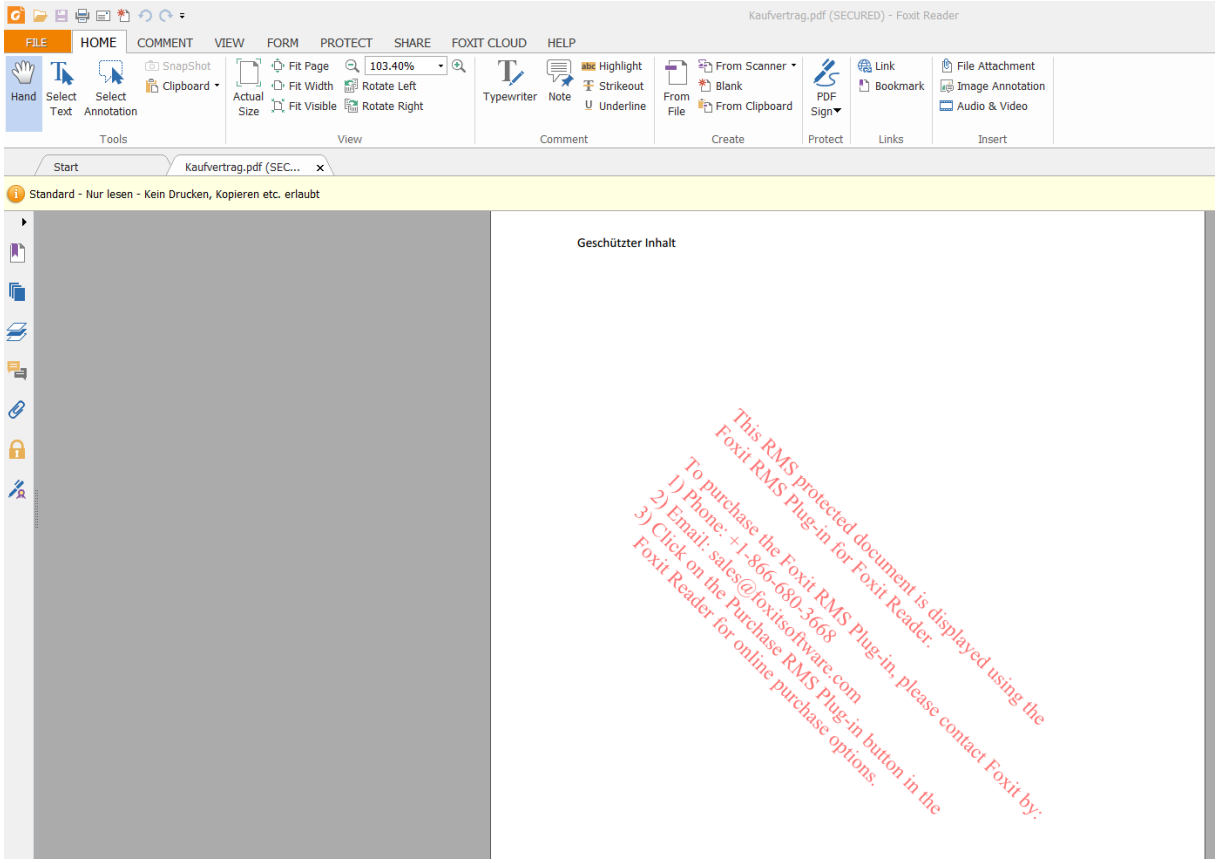

Abbildung 10: Geschütztes PDF-Dokument geöffnet mit dem kostenlosen Foxit Reader mit RMS Plug-In

Die Zugriffsbeschränkungen eines Dokuments lassen sich im Foxit Reader einsehen unter File > Properties > Security, wo sich auch weitere Zugriffsrechte beim Autor des Dokuments anfordern lassen durch einen Klick auf „Request additional permissions…“ (siehe Abbildung 11). In diesem Beispiel lässt sich der Autor des Dokuments die Zugriffsrechte anzeigen, die daher alle auf „Allowed“ stehen.

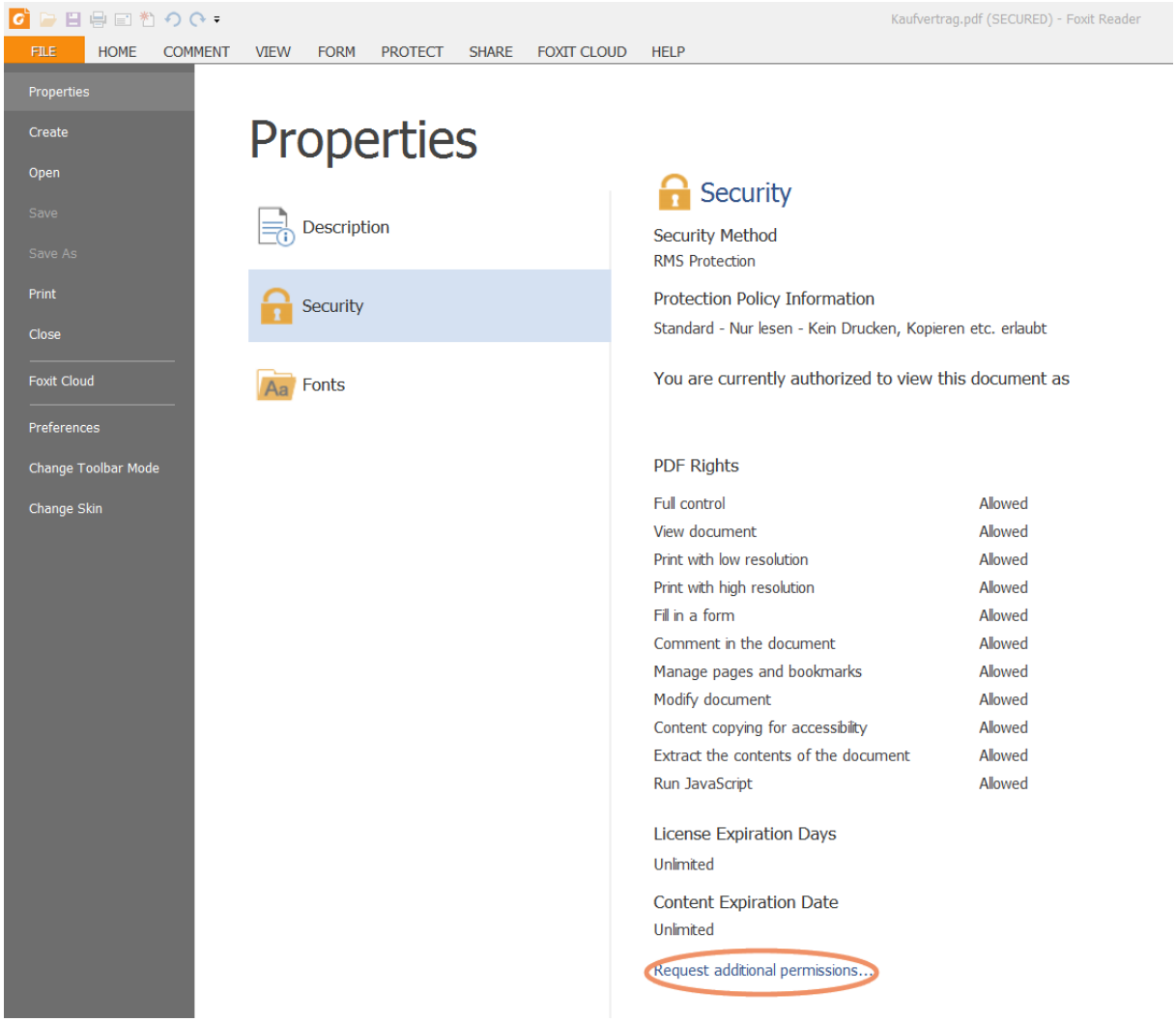

Abbildung 11: Die Zugriffsrechte eines geschützten PDF-Dokuments im Foxit Reader

Weitere RMS-fähige PDF-Reader

Neben dem Foxit Reader unterstützt auch der Nitro Pro Reader das Anzeigen von geschützten PDF-Dokumenten. Allerdings muss dafür die Microsoft RMS-Freigabeanwendung installiert sein, um diese Funktion zu aktivieren. Beim Anzeigen eines geschützten PDF-Dokuments wird im Nitro Pro Reader ein Hinweis auf den eingeschränkten Zugriff angezeigt (siehe Abbildung 12).

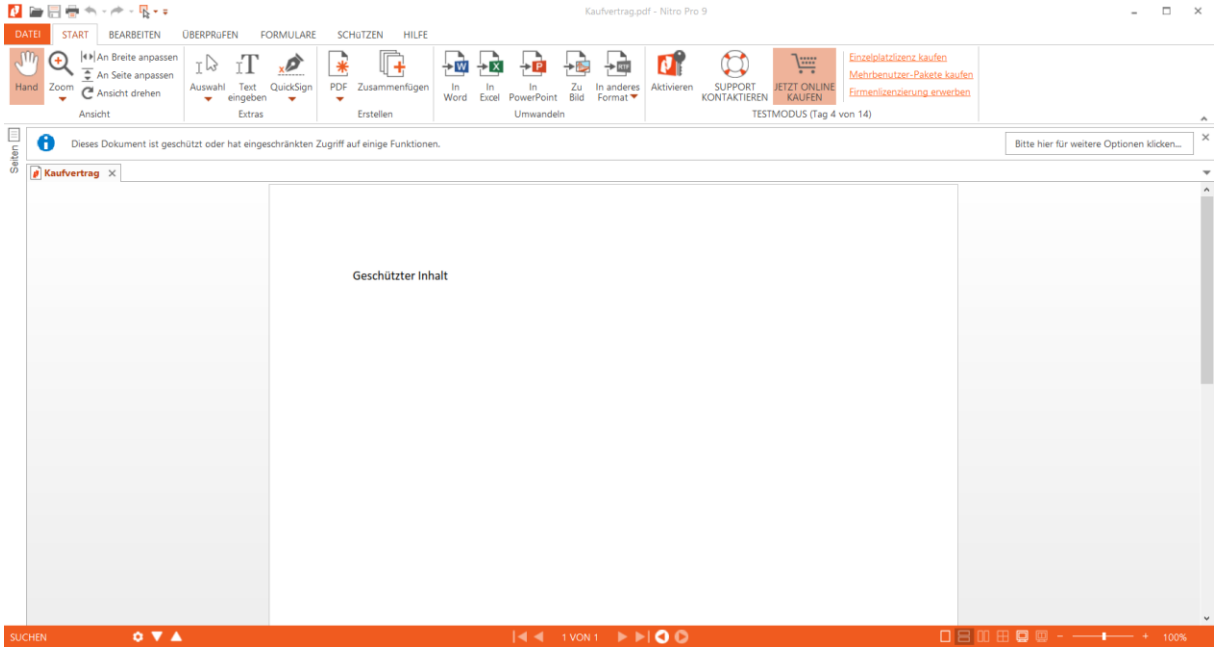

Abbildung 12: Geschütztes PDF-Dokument geöffnet mit dem Nitro Pro Reader

Mit einem Klick auf „Bitte hier für weitere Optionen klicken…“ kann man sich die einzelnen Zugriffsrechte ansehen (siehe Abbildung 13).

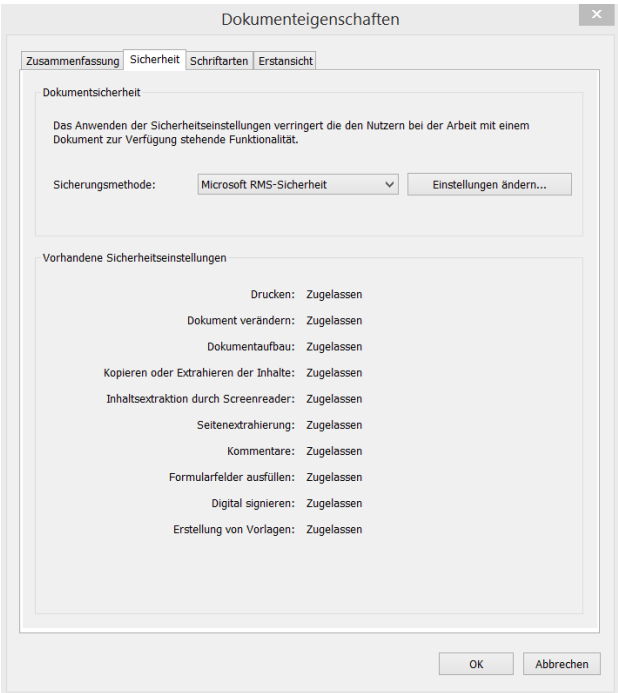

Abbildung 13: Anzeigen der Zugriffsrechte im Nitro Pro Reader

Um PDF-Dokumente RMS-basiert zu verschlüsseln, bietet sich neben dem Foxit Reader die RMS-Freigabeanwendung von Microsoft an, mit der sich Dokumente jeden Dateityps verschlüsseln lassen. PDF-Dokumente, die mit der RMS-Freigabeanwendung verschlüsselt wurden, lassen sich auch wieder damit öffnen mit dem in der Anwendung integrierten Viewer. Genaueres dazu gibt es im hierauf folgenden Abschnitt.

Microsoft RMS-Freigabeanwendung

Die RMS-Freigabeanwendung ermöglicht es, beliebige Dateien jeden Typs mit einem einfachen Klick im Dateiexplorer zu verschlüsseln und die genauen Zugriffsrechte für bestimmte Personen zu definieren. Auch ermöglicht sie das geschützte Versenden von Dateien über Outlook aus dem Dateiexplorer heraus. Beliebige Dateien, die zuvor nicht schon mit Microsoft Office oder einem PDF-Reader verschlüsselt wurden, können also mit wenigen Klicks geschützt werden, wobei sich genau festlegen lässt, wer (Vertragspartner, Teammitglieder etc.) welche Zugriffsrechte bekommt (lesen, ändern, kopieren, drucken etc.). Außerdem ermöglicht die RMS-Freigabeanwendung das Anzeigen von zuvor geschützten Dateien, für die man Zugriffsrechte bekommen hat, nach erfolgreicher Authentifizierung.

Bei der RMS-basierten Verschlüsselung unterscheidet man zwei Verschlüsselungslevel: den nativen und den generischen (siehe auch hier). Der native Level wird wie oben erwähnt auf Office- und PDF-Dokumente angewendet, so dass die festgelegten Zugriffsrechte immer beim Öffnen der Datei durch Authentifizierung erzwungen werden und auch nach dem Kopieren, Speichern oder Weiterleiten der Datei bestehen bleiben. Außerdem verschlüsselt die RMS-Freigabeanwendung die meisten Text- und Bilddateien auf dem nativen Level. Der generische Level hingegen beinhaltet eine Kapselung in einem speziellen Dateityp, welche die Zugriffsautorisierung und das zeitliche Erlöschen des Zugriffs kontrolliert, allerdings nicht die granularen Zugriffsbeschränkungen (wie z. B. separate Lese- oder Änderungsberechtigungen) ermöglicht wie auf dem nativen Level. Dieser Schutz wird auf alle anderen Dateitypen von der RMS-Freigabeanwendung angewendet. Wenn eine autorisierte Person die generisch geschützte Datei nach erfolgreicher Authentifizierung öffnet, hat sie automatisch Vollzugriff und kann die Datei auch ohne Kapselung kopieren, woanders abspeichern oder weiterleiten. Dabei wird der Schutz allerdings aufgehoben.

Dateien verschlüsseln

Wenn die RMS-Freigabeanwendung installiert ist, erscheinen beim Rechtsklick auf Dateien oder Ordner im Dateiexplorer zwei neue Optionen: „Direkt schützen“ und „Geschütztes Freigeben“ (siehe Abbildung 14).

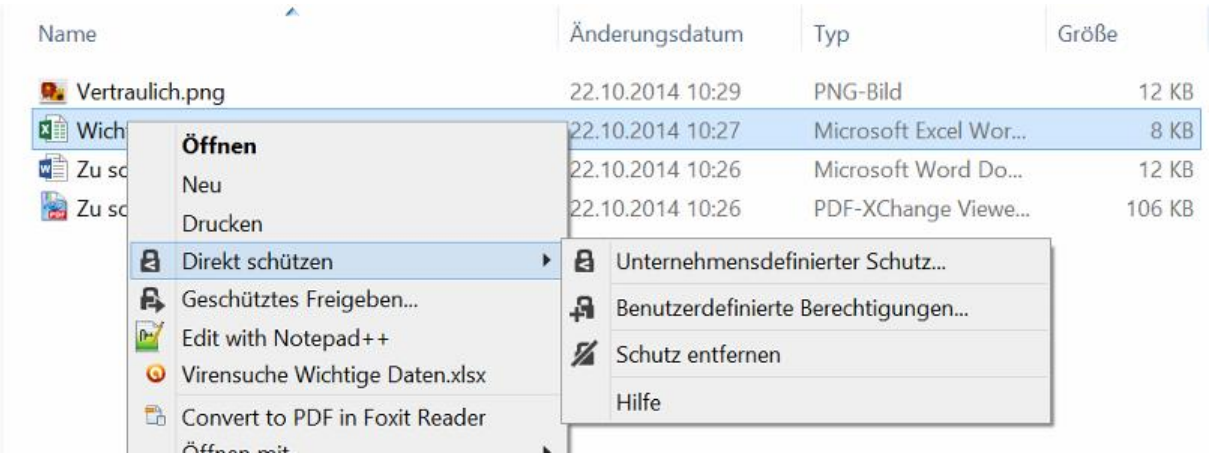

Abbildung 14: Dateischutz-Optionen im Dateiexplorer mit der RMS-Freigabeanwendung

Durch Klick auf „Direkt schützen“ hat man die Wahl zwischen unternehmensdefiniertem Schutz mit den Rechtevorlagen, die auch in Office verfügbar sind, und eigenen, benutzerdefinierten Berechtigungen. Beim Auswählen jeder dieser Optionen wird man zur Authentifizierung mit Kontoname und Passwort (des Unternehmenskontos mit RMS-Abonnement) aufgefordert. Danach öffnet sich die RMS-Freigabeanwendung, in der man die Möglichkeit der granularen Festlegung der Zugriffsrechte hat. Die benutzerdefinierten Berechtigungen lassen sich zunächst einteilen in einen generischen („Nutzung auf allen Geräten zulassen“) und nativen Level („Nutzungsbeschränkungen erzwingen“; siehe Abbildung 15). Letzteres ermöglicht die granulare Vergabe von Anzeige-, Änderungs-, Kopier- und Druck- sowie Vollzugriffsberechtigungen. Die Berechtigungen werden bestimmten Benutzern, die oben im Fenster über E-Mail-Adressen spezifiziert werden, zugewiesen. Zudem lassen sich ein Datum festlegen, an dem der Zugriff auf das Dokument enden soll, und eine E-Mail-Benachrichtigung bei unautorisierten Zugriffsversuchen anfordern.

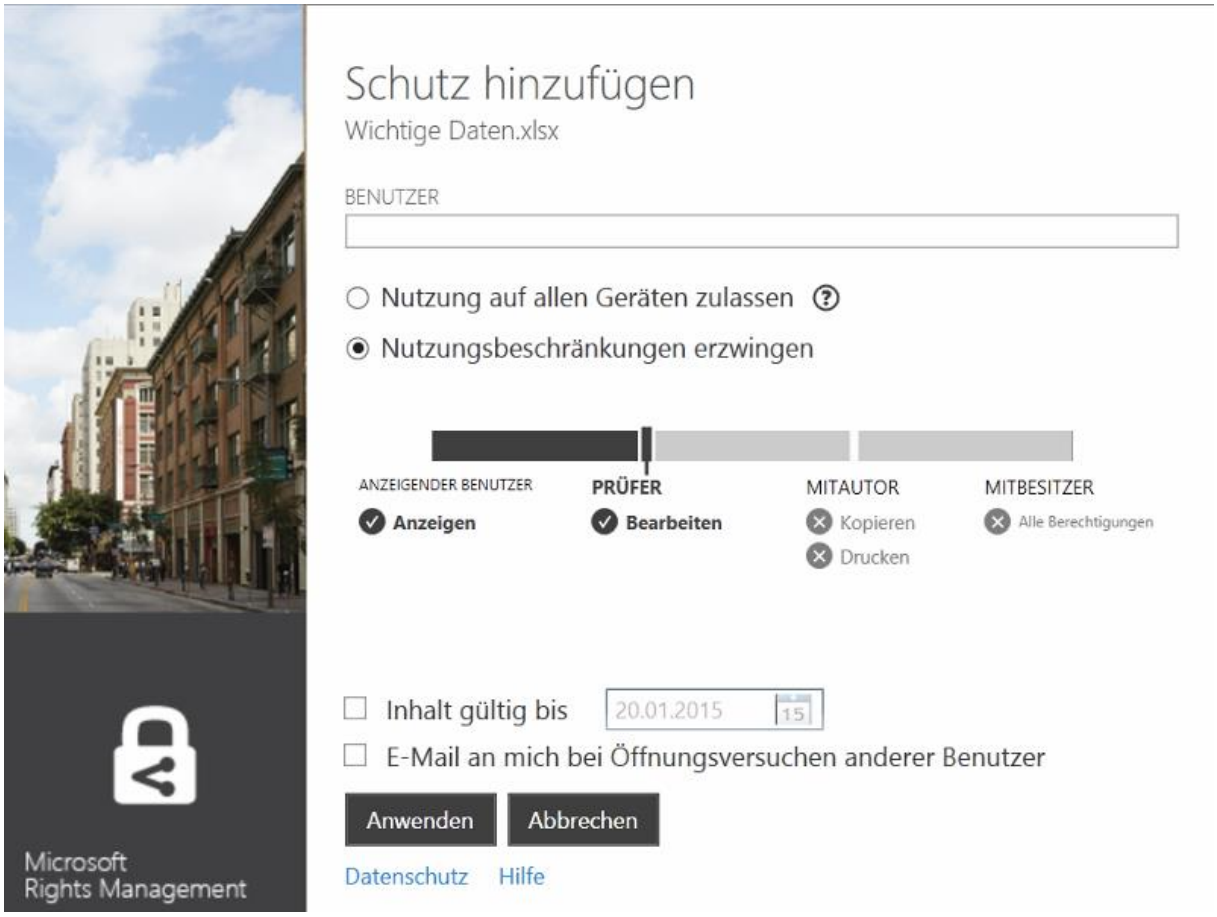

Abbildung 15: Dateien schützen mit individuellen Zugriffsberechtigungen in der RMS-Freigabeanwendung

Auf diese Weise lassen sich Word-, Excel-, PowerPoint-, PDF-, Bild- und Textdateien verschlüsseln. Für andere Dateitypen ist nur die generische Schutzoption mit Vollzugriff gegeben („Nutzung auf allen Geräten zulassen“) (siehe Abbildung 16).

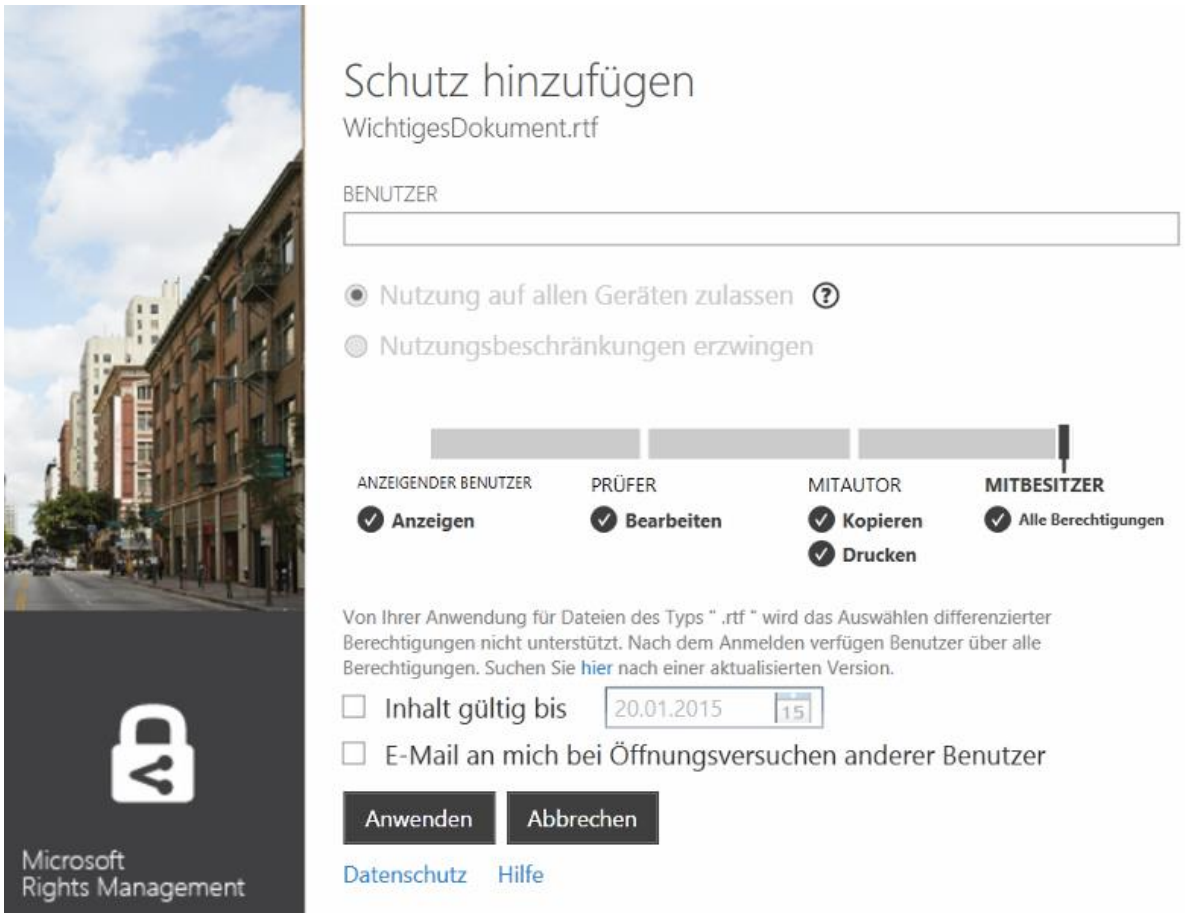

Abbildung 16: Dateien generisch schützen in der RMS-Freigabeanwendung

Eine Besonderheit beim Schützen von PDF-, Bild- und Textdateien mit der RMS-Freigabeanwendung ist, dass die Datei eine neue Endung erhält mit einem vorgesetzten „p" (z. B. .ppdf, .ppng etc.; siehe Abbildung 17). Damit sind diese Dateien nur mit der RMS-Freigabeanwendung zu öffnen, welche beim Öffnen die Benutzer-Authentifizierung erfordert und die Zugriffsrechte der jeweiligen Datei beim Benutzer erzwingt.

Name	Änderungsdatum	Typ	Größe
Direkt schützen.png	22.10.2014 10:37	PNG-Bild	30 KB
Vertraulich.ppng	22.10.2014 10:45	Protected Image Document	55 KB
Wichtige Daten.xlsx	22.10.2014 10:48	Microsoft Excel Worksheet	76 KB
WichtigesDokument.rtf.pfile	22.10.2014 10:51	Rights Protected Document	44 KB
Zu schützende Inhalte.docx	22.10.2014 10:26	Microsoft Word Document	12 KB
Zu schützende Inhalte.ppdf	22.10.2014 10:48	Protected Pdf Document	149 KB

Abbildung 17: Änderung der Endung von PDF-, Bild- und Textdateien nach der Verschlüsselung mit der RMS-Freigabeanwendung

Dateitypen, die nur den generischen Schutz unterstützen, erhalten durch die Kapselung eine völlig neue Endung: .pfile (siehe Abbildung 18). Dadurch ist auch hier die RMS-Freigabeanwendung zum Öffnen der Dateien notwendig. Allerdings wird die Datei nach der erfolgreichen Authentifizierung des Benutzers in der jeweils zugehörigen Anwendung auf dem PC wie gewohnt angezeigt. Der Benutzer hat vollen Zugriff auf die Datei.

Name	Änderungsdatum	Typ	Größe
Direkt schützen.png	22.10.2014 10:37	PNG-Bild	30 KB
Vertraulich.ppng	22.10.2014 10:45	Protected Image Document	55 KB
Wichtige Daten.xlsx	22.10.2014 10:48	Microsoft Excel Worksheet	76 KB
WichtigesDokument.rpt.pfile	22.10.2014 10:51	Rights Protected Document	44 KB
Zu schützende Inhalte.docx	22.10.2014 10:26	Microsoft Word Document	12 KB
Zu schützende Inhalte.ppdf	22.10.2014 10:48	Protected Pdf Document	149 KB

Abbildung 18: Änderung der Endung von anderen Dateitypen nach dem Schützen mittels RMS-Freigabenanwendung

Für eine Übersicht der Dateitypen und ihrer Endungsänderung nach dem Schützen mit der RMS-Freigabeanwendung siehe hier. Der Schutz einer Datei lässt sich wieder aufheben mit einem Rechtsklick auf die Datei unter Direkt schützen > Schutz entfernen.

Dateien geschützt versenden

Mit einem Rechtsklick auf eine Datei eines beliebigen Typs im Dateiexplorer kann man die Option Geschütztes Freigeben auswählen, woraufhin nach erfolgreicher Authentifizierung ein Fenster zur individuellen Festlegung der Empfänger und ihrer Zugriffsrechte geöffnet wird, ähnlich wie vorher bereits beschrieben (siehe Abbildung 19).

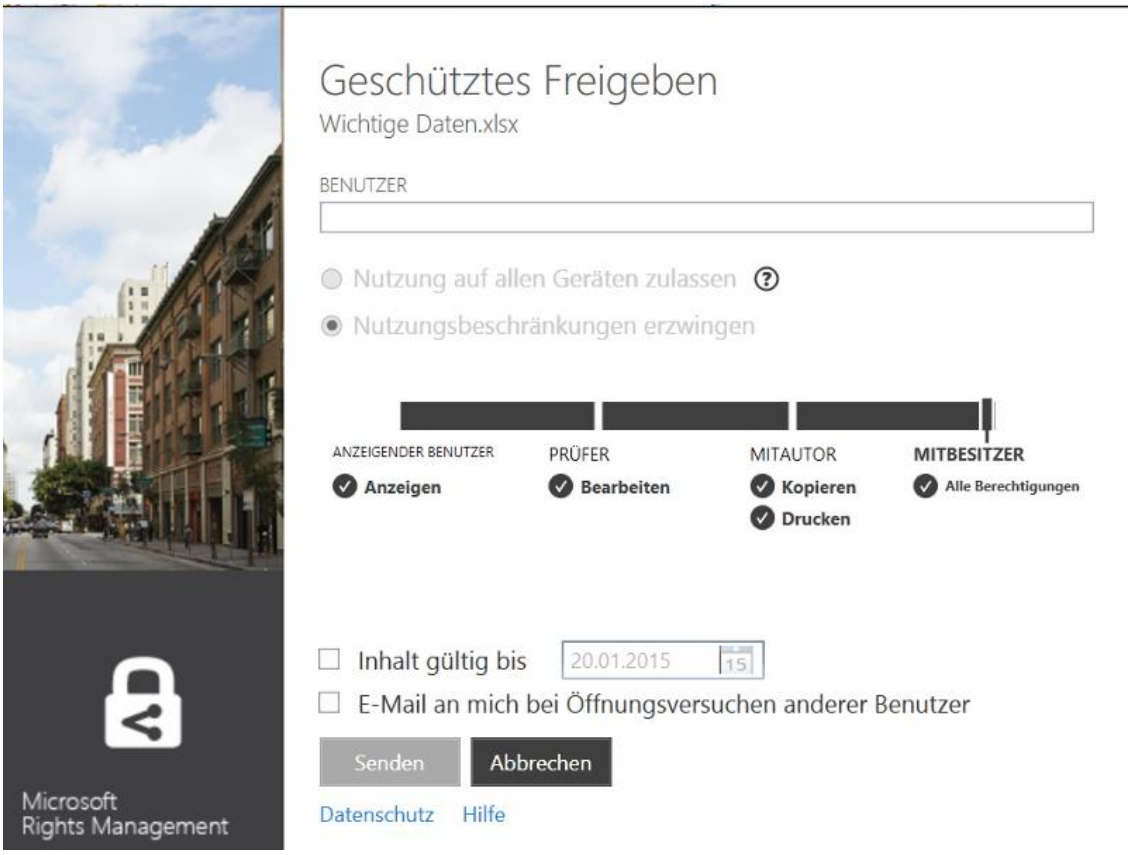

Abbildung 19: Individuelle Zugriffsberechtigungen für das geschützte Versenden einer Datei in der RMS-Freigabeanwendung

Mit Klick auf Senden wird automatisch im E-Mail-Programm eine neue E-Mail mit den geschützten Dateien generiert. Von jeder geschützten Word-, Excel-, PowerPoint- oder PDF-Datei wird außerdem eine .ppdf-Version erstellt, die mit der RMS-Freigabeanwendung geöffnet werden kann (siehe Abbildung 20). So können Nutzer auch ohne Microsoft Office oder einem RMS-fähigen PDF-Reader bzw. auf einem mobilen Gerät die Datei mit der RMS-Freigabeanwendung ansehen.

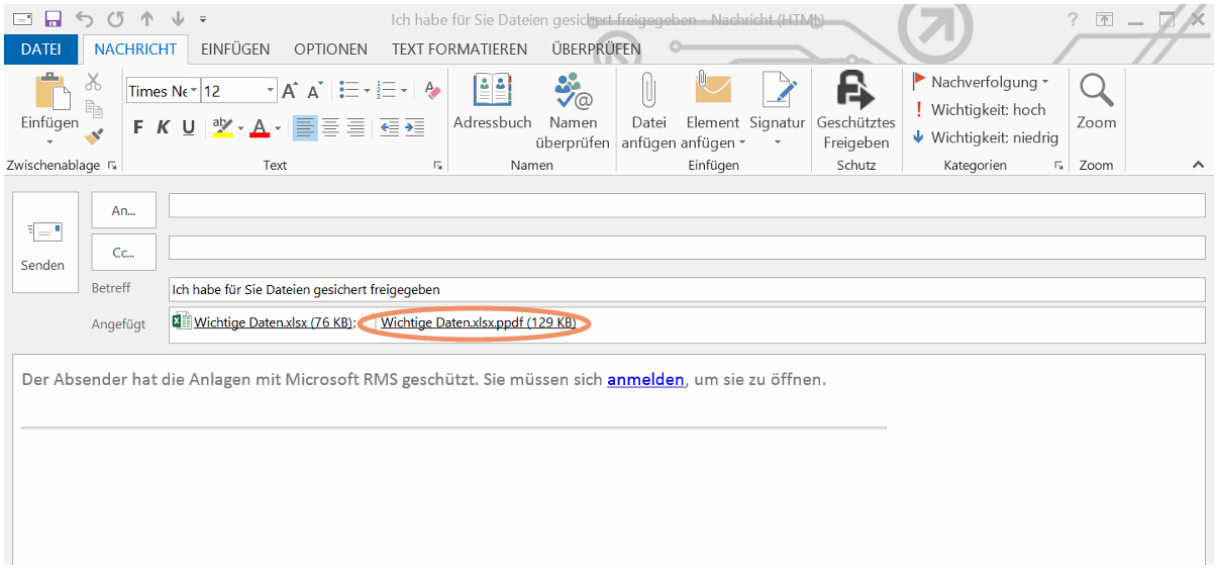

Abbildung 20: Versenden einer mit der RMS-Freigabeanwendung geschützten Datei mit Outlook

Durch einen Klick auf „Geschütztes Freigeben" in Word, Excel, PowerPoint (siehe Abbildung 4) oder Outlook (siehe Abbildung 7) lässt sich das entsprechende Dokument ebenfalls als geschützter Anhang einer E-Mail beifügen.

Geschützte Dateien öffnen

RMS-geschützte Dateien, für die man Zugriffsrechte bekommen hat, können mit der RMS-Freigabeanwendung geöffnet werden (auch, ohne dass Microsoft RMS auf Organisationsebene abonniert sind; es genügt eine Registrierung für die kostenlose RMS-Freigabeanwendung mit einer Unternehmens-E-Mail-Adresse). Geschützte PDF-, Text- oder Image-Dateien werden mit dem integrierten Viewer geöffnet, nachdem man seine Identität verifiziert hat (siehe Abbildung 21). Die Zugriffsberechtigungen werden dabei angezeigt.

Abbildung 21: RMS-geschützte Bilddatei geöffnet mit der RMS-Freigabeanwendung

Weitere Dateitypen, die generisch geschützt sind, werden mit dem jeweiligen Standardprogramm geöffnet, nachdem man in der RMS-Freigabeanwendung seine Identität verifiziert hat. Zuvor werden die Zugriffsrechte zur Kenntnisnahme angezeigt (siehe Abbildung 22).

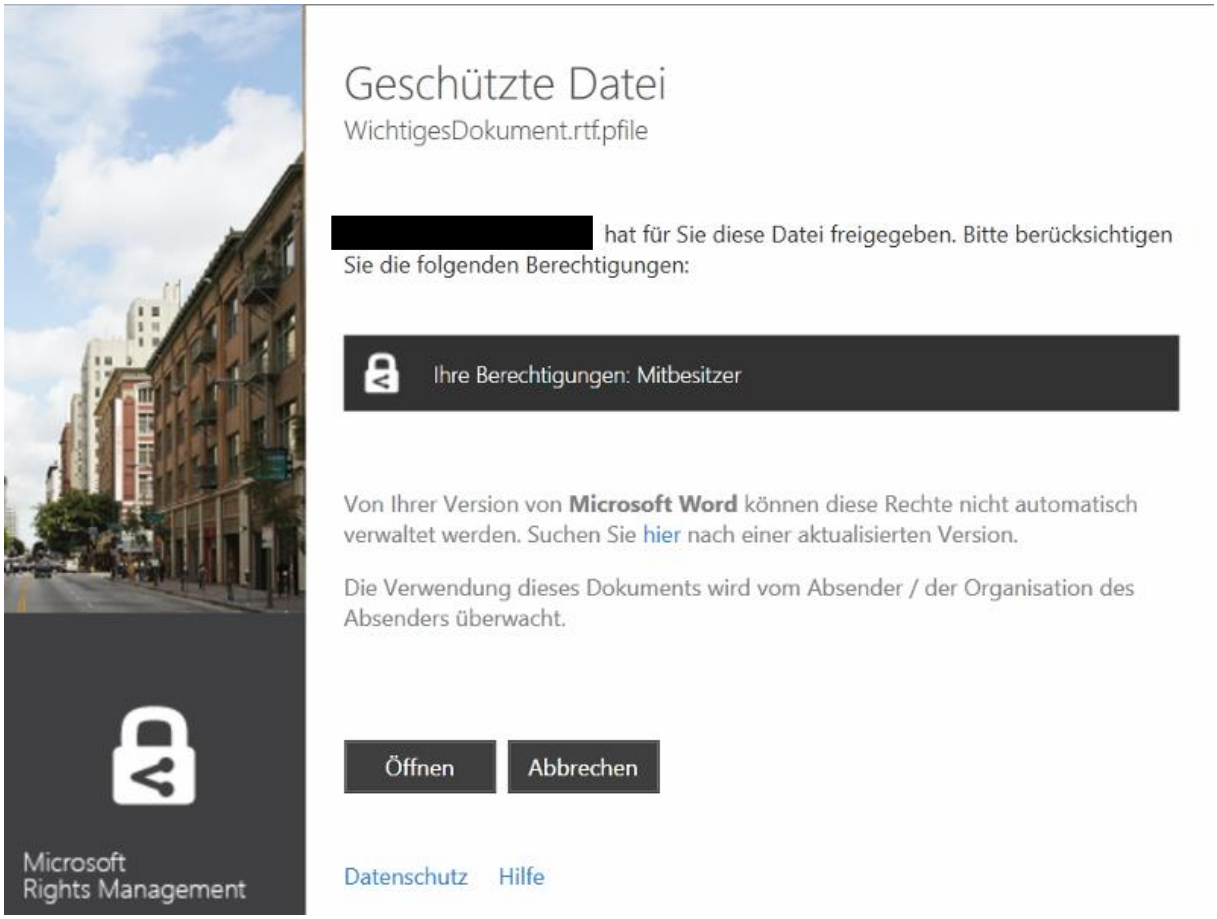

Abbildung 22: Anzeige der Zugriffsrechte für eine generisch geschützte Datei in der RMS-Freigabeanwendung

RMS auf mobilen Geräten verwenden

Die Microsoft RMS unterstützen die Mobilität und Flexibilität von RMS-Nutzern, indem sich RMS auch auf anderen Betriebssystemen als Windows sowie auf mobilen Geräten anwenden lässt. RMS-geschützte Dateien lassen sich damit auch überall von unterwegs anzeigen. Auf mobilen Geräten ist die Microsoft RMS-Funktionalität jedoch im Vergleich zum Windows-Computer etwas eingeschränkt. PDF-Dateien und Fotos lassen sich mit dafür geeigneten Mobilapplikationen verschlüsseln bzw. ansehen, sofern sie verschlüsselt wurden. Geschützte Office-Dateien lassen sich allerdings nicht direkt auf mobilen Geräten öffnen (außer in Office Online) und auch nicht verschlüsseln. Für das Verschlüsseln und entschlüsselte Anzeigen von PDF-Dateien eignet sich der Foxit MobilePDF Reader mit RMS, der z. B. für Android, Windows Phone, Windows RT und iOS verfügbar ist. Fotos kann man mit der RMS-Freigabeanwendung für mobile Geräte (d. h. Windows Phone, iOS und Android) verschlüsseln. RMS-verschlüsselte PDF-, Bild- und Text-Dateien lassen sich damit anzeigen, während sich allerdings andere Dateitypen damit weder anzeigen noch verschlüsseln lassen.

RMS mit dem Foxit MobilePDF Reader

Die Option der RMS-Verschlüsselung ist im Foxit MobilePDF Reader im Dokument bzw. Dokumentenbrowser unter dem Punkt „RMS Encryption" zu erreichen. Nach Auswahl der Option „RMS Encryption" erfolgen eine Authentifizierung des Benutzers mit dem RMS-fähigen Unternehmenskonto und die Auswahl einer Rechtevorlage (z.B. „Confidential" und „Confidential View Only" für eine Schreib-und Änderungsberechtigung bzw. eine Leseberechtigung; benutzerdefinierte Berechtigungen kann man hier nicht setzen; siehe Abbildung 23). Der Foxit MobilePDF Reader kann natürlich auch geschützte PDF-Dokumente öffnen, wobei in der kostenlosen Version (ohne RMS-Verschlüsselung) ein Wasserzeichen im Dokument erscheint, ähnlich wie bei der kostenlosen Version vom Foxit Reader für Windows (siehe Abbildung 10).

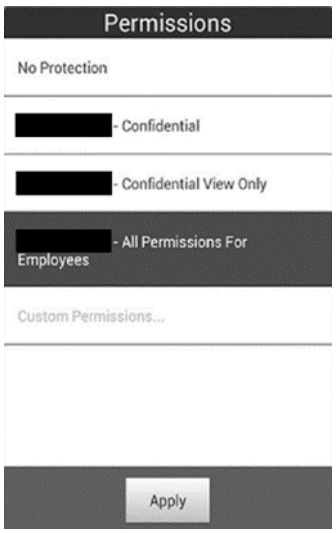

Abbildung 23: Rechtevergabe im Foxit MobilePDF Reader

Die RMS-Freigabeanwendung auf mobilen Geräten

Mit der RMS-Freigabeanwendung für Android, iOS oder Windows Phone hat man nur die Möglichkeit, ein Foto zu verschlüsseln oder RMS-verschlüsselte PDF-, Text- oder Bilddateien zu öffnen und nach erfolgreicher Benutzerauthentifizierung anzeigen zu lassen. Die RMS-Freigabeanwendung bietet dennoch eine (indirekte) Möglichkeit für das Anzeigen von zuvor auf einem PC geschützten Office-Dateien auf dem mobilen Gerät. Wie zuvor im Abschnitt *Dateien geschützt versenden* beschrieben, wird beim geschützten Versenden von Office-Dateien automatisch eine .ppdf-Datei erstellt und als zusätzlicher Anhang der E-Mail beigefügt (siehe Abbildung 20). Diese .ppdf-Datei lässt sich dann anstelle von der geschützten Office-Datei zumindest ansehen mit Hilfe der RMS-Freigabeanwendung auf mobilen Geräten.

Die Verschlüsselungs-Funktionalität der RMS-Freigabeanwendung ist bisher auf Foto-Dateien beschränkt. Im Hauptmenü der Anwendung lässt sich ein Foto zum Verschlüsseln durch Aufnahme oder Auswahl aus den auf dem Mobilgerät vorhandenen Fotos wählen (siehe Abbildung 24). Nachdem man ein Foto zum Verschlüsseln ausgewählt hat, wählt man eine der unternehmensdefinierten Vorlagen für die Zugriffsrechte (z.B. „Confidential" oder „Confidential View Only") (siehe Abbildung 25). Auch hier kann man keine benutzerdefinierten Zugriffsberechtigungen festlegen.

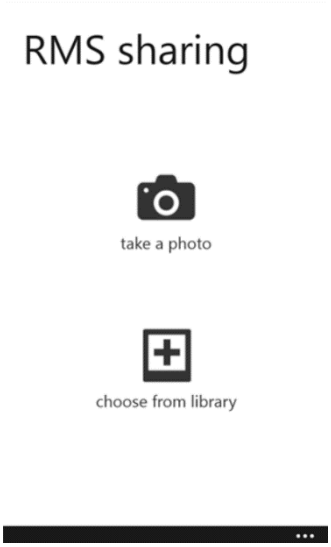

Abbildung 24: RMS-Freigabeanwendung auf mobilen Geräten

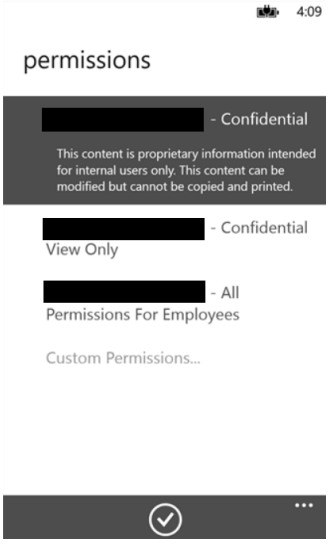

Abbildung 25: Zugriffsberechtigungen in der RMS-Freigabeanwendung für mobile Geräte

RMS bei Dokumentbibliotheken und Listen in SharePoint

RMS in SharePoint bieten optimale Schutzfunktionen für Dokumente, die über SharePoint miteinander geteilt werden bzw. die gemeinsam darin bearbeitet werden. Dokumente, die in geschützte SharePoint-Bibliotheken hochgeladen werden, müssen nicht extra in Office oder der jeweiligen Anwendung vorher explizit RMS-verschlüsselt werden; dies wird innerhalb einer geschützten SharePoint-Bibliothek durchgeführt. Das ist insbesondere nützlich, wenn mehrere Dokumente zugleich geschützt und geteilt werden sollen, wie z. B. bei zusammengehörenden Vertragsdokumenten oder Projektanforderungsdokumenten eines Kunden. Mit wenigen Klicks lässt sich eine ganze vertrauliche Dokumentbibliothek mit RMS schützen.

Bevor man RMS in SharePoint anwenden kann, muss die Informationsrechteverwaltung (Information Rights Management, IRM) zunächst in der SharePoint Administration aktiviert werden. Ein Benutzer mit Administrationsrechten kann hier einsehen, wie vorzugehen ist. Wenn das IRM aktiviert ist, können Bibliotheken und Listen in SharePoint mit Hilfe von granularen Zugriffsberechtigungen RMS-geschützt werden. Dabei werden die Zugriffsberechtigungen immer

auf eine ganze Bibliothek bzw. Liste angewendet und nicht auf einzelne Dokumente. Im Folgenden wird beschrieben, wie die Zugriffsrechte auf eine Dokumentbibliothek in SharePoint eingeschränkt werden und wie man mit zugriffsbeschränkten Bibliotheken arbeitet. Für IRM-Einstellungen in Listen ist ähnlich vorzugehen.

Zugriffsrechte auf eine Bibliothek mit Hilfe von RMS beschränken

Nachdem man eine Bibliothek oder Liste angelegt hat, gelangt man unter Bibliothek (bzw. Liste) zu den Bibliothekseinstellungen (bzw. Listeneinstellungen; siehe Abbildung 26).

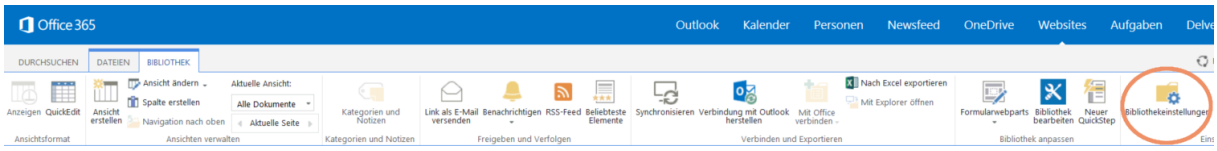

Abbildung 26: Bibliothekseinstellungen in SharePoint

In den Einstellungen findet man unter dem Punkt Berechtigungen und Verwaltung die Verwaltung von Informationsrechten (siehe Abbildung 27).

Abbildung 27: Verwaltung von Informationsrechten für eine SharePoint-Bibliothek

Neben einem Titel und einer Beschreibung der Berechtigungsrichtlinie für die Bibliothek kann man zusätzliche Optionen festlegen (siehe Abbildung 28). Grundsätzlich gibt es in SharePoint verschiedene voreingestellte Benutzergruppen (z.B. Besitzer, Besucher und Mitglieder) die jeweils bestimmte Zugriffsrechte auf Webseiten in SharePoint haben (z.B. Vollzugriff, Leseberechtigung und Änderungsberechtigung). Wie man die Benutzergruppeneinstellungen anpasst, wird im Folgenden noch erklärt. Die Berechtigungsvergabe über Benutzergruppen bietet jedoch nur den Schutz von Dateien innerhalb von SharePoint. Sobald ein berechtigter Benutzer eine Datei z. B.

herunterlädt oder ein Dokument ausdruckt, besteht der Schutz durch die Berechtigungsbeschränkungen nicht mehr und der Inhalt einer Datei kann potenziell von unbefugten Personen eingesehen werden (z. B. wenn der berechtigte Benutzer die Datei weitergibt oder das Dokument sonst irgendwie zugänglich für andere macht). Die Microsoft RMS bzw. das IRM in SharePoint schützen hiervor: Dateien, die aus IRM-geschützten SharePoint-Bibliotheken angezeigt oder heruntergeladen werden, bleiben verschlüsselt, so dass die Inhalte für unbefugte Personen nicht zugänglich sind.

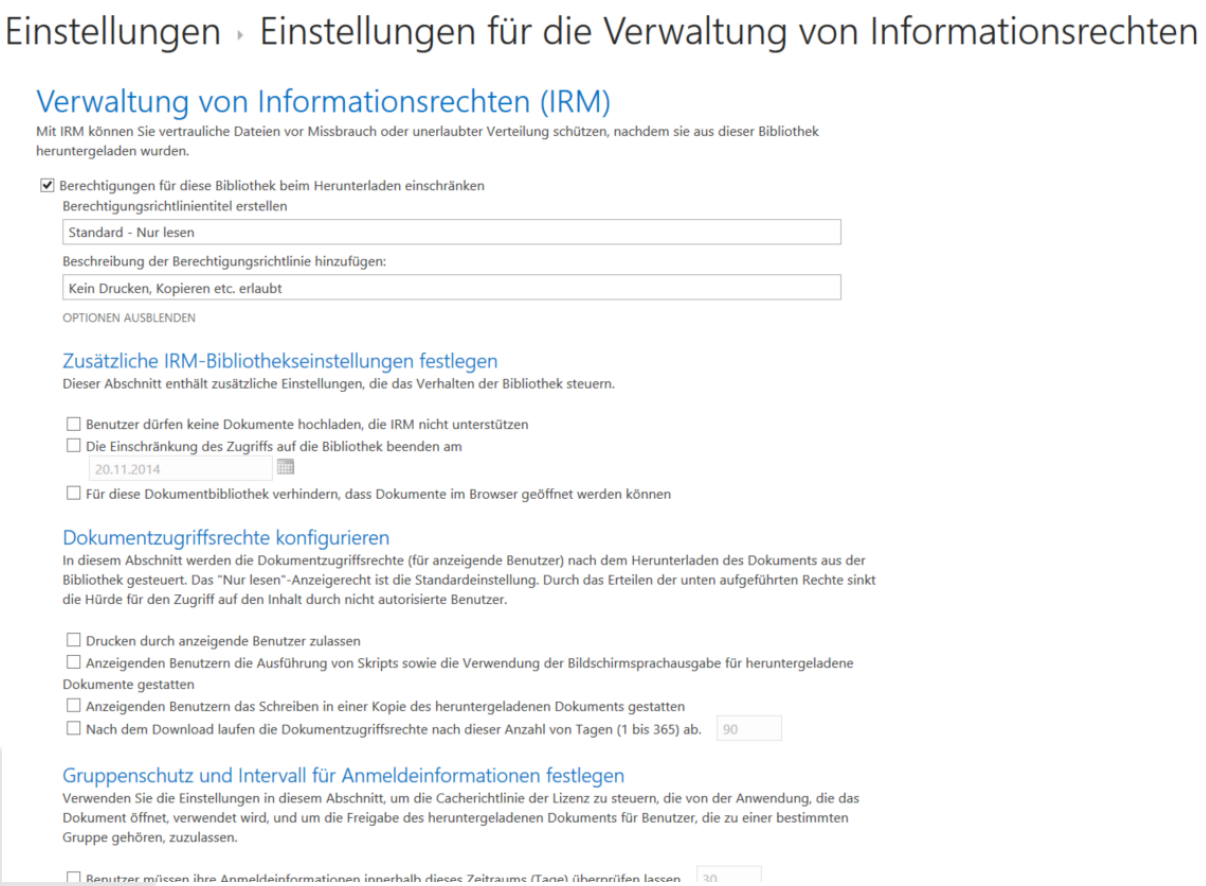

Abbildung 28: Einstellungen der Informationsrechteverwaltung für eine SharePoint-Bibliothek

In der Verwaltung von Informationsrechten aus Abbildung 28 lassen sich Einstellungen über die Benutzergruppeneinstellungen hinaus vornehmen. Die IRM-Einstellungen für eine Bibliothek beinhalten, dass die Benutzer bei Bedarf nur Dokumente in die Bibliothek hochladen können, die IRM in SharePoint unterstützen (hauptsächlich Word-, Excel-, PowerPoint- und PDF-Dateien). Der grundsätzliche Zugriff (aller Benutzergruppen) auf die Bibliothek lässt sich zeitlich bestimmt beenden. Es lässt sich außerdem verhindern, dass Dokumente im Browser geöffnet werden, wobei auch hier die Einschränkung für Word-, Excel-, PowerPoint- und PDF-Dateien gilt. Andere Dateitypen wie z.B. Bild-Dateien lassen sich zwar grundsätzlich nicht im Browser öffnen; dafür wird allerdings unabhängig von den IRM-Einstellungen eine Vorschau der Datei durch Klick auf die drei Punkte hinter der Datei angezeigt (siehe Abbildung 29).

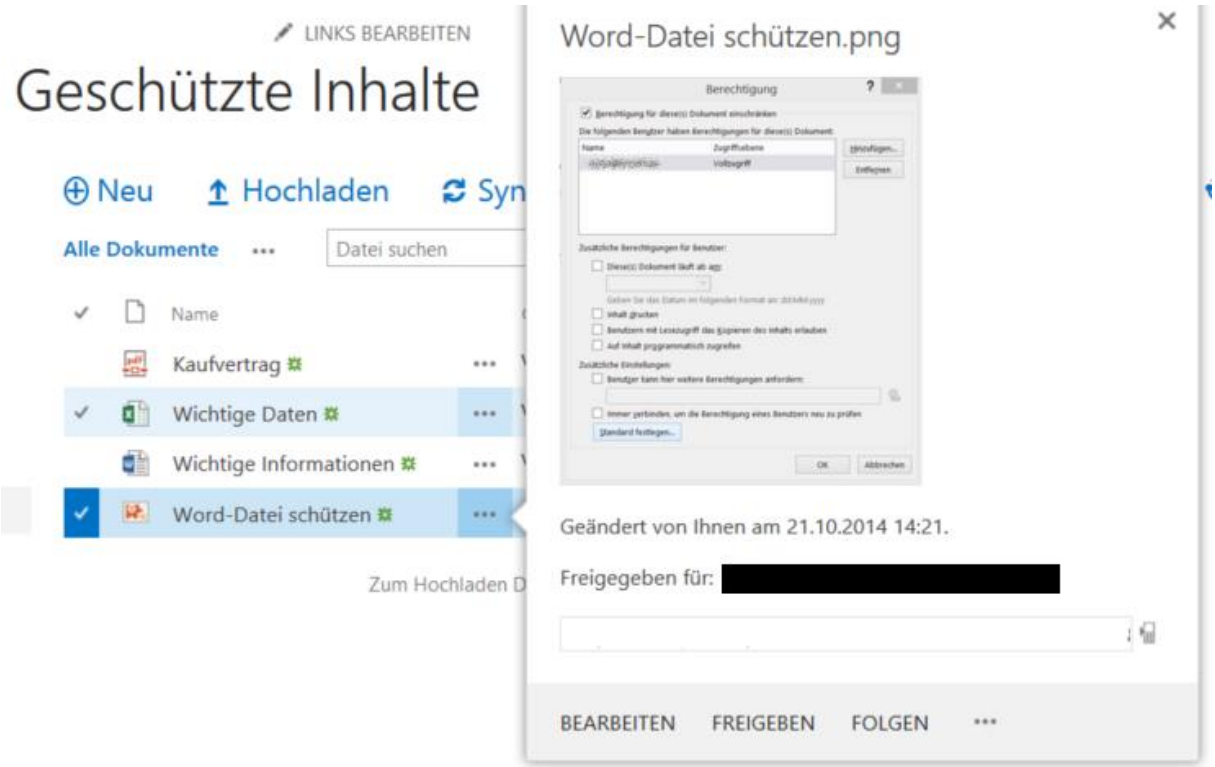

Abbildung 29: Vorschau einer Bild-Datei in einer IRM-geschützten SharePoint-Bibliothek

Die Vorschau von Office- oder PDF-Dateien wird beim Klick auf die drei Punkte hinter einer Datei in einer IRM-geschützten SharePoint-Bibliothek grundsätzlich unterdrückt (siehe Abbildung 30). Office- und PDF-Dokumente lassen sich normalerweise im Browser anzeigen durch Klick auf „Öffnen" bei einer PDF-Datei bzw. auf „Im Browser anzeigen" bei Office-Dateien, was sich wiederum durch Aktivieren der entsprechenden Option in der Informationsrechteverwaltung für eine SharePoint-Bibliothek verhindern lässt.

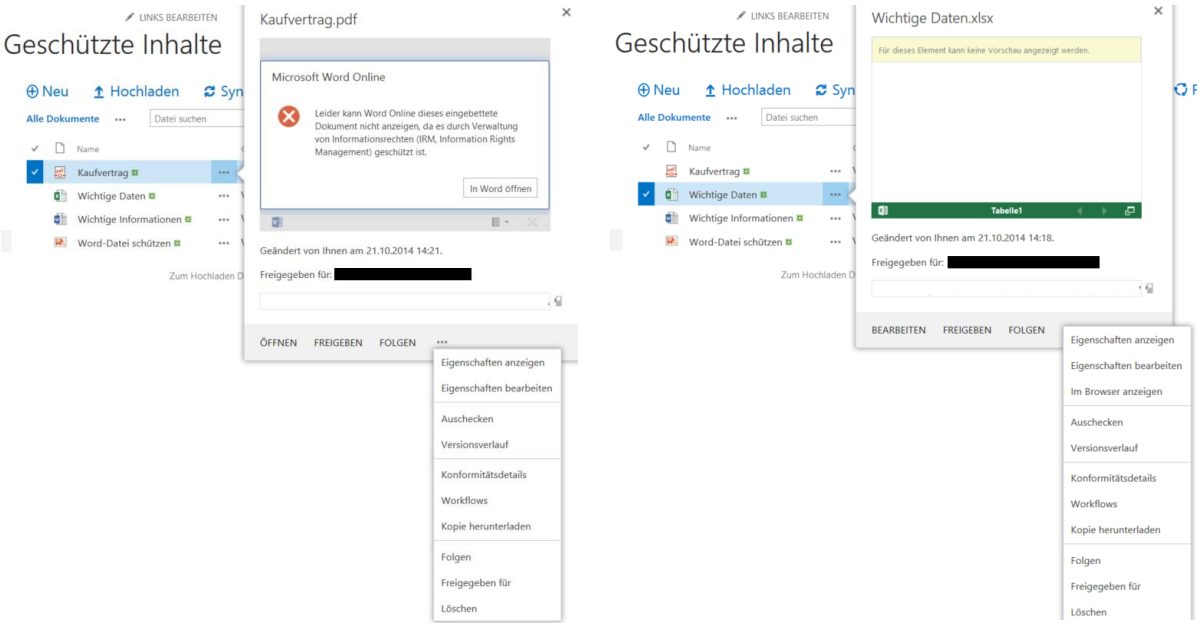

Abbildung 30: Unterdrückte Vorschau von PDF- und Office-Dateien in einer IRM-geschützten SharePoint-Bibliothek

In den IRM-Einstellungen einer SharePoint-Bibliothek lassen sich ferner die Zugriffsrechte auf die Dokumente in der Bibliothek über die Benutzergruppeneinstellungen hinaus granular festlegen. Das Drucken von Dokumenten, was z. B. Benutzern mit alleiniger Leseberechtigung normalerweise nicht möglich ist, kann ausdrücklich erlaubt werden. Allen Benutzern mit mindestens einer Leseberechtigung kann außerdem die Ausführung von Skripten und die Verwendung der Bildschirmsprachausgabe sowie das Schreiben in einer heruntergeladenen Kopie eines Dokuments erlaubt werden. Auch lässt sich der Zugriff auf ein Dokument nach dem Download zeitlich beschränken. Außerdem lässt sich ferner anfordern, dass Benutzer nach bestimmten Zeiträumen ihre Authentifizierung erneuern müssen, oder dass Benutzer Dokumente nur für Mitglieder einer bestimmten Active-Directory-Gruppe bzw. eines Exchange-Onlineverteilers freigeben können. Weitere Informationen zu der Verwaltung von Informationsrechten einer Bibliothek oder Liste in SharePoint finden sich hier.

RMS-unabhängige Zugriffsberechtigungen in SharePoint

Wie zuvor bereits erwähnt, bietet SharePoint grundsätzliche Einstellungen von Zugriffsberechtigungen für Bibliotheken und Listen an, die nicht an ein Abonnement von Microsoft RMS gebunden sind und die durch die zuvor beschriebenen IRM-Einstellungen erweitert werden. Diese Einstellungen, „Berechtigungen für Dokumentbibliothek“ (oder „Berechtigungen für Liste“ entsprechend), lassen sich ebenfalls in den Bibliothekseinstellungen unter Berechtigungen und Verwaltung finden (siehe Abbildung 31).

Abbildung 31: Berechtigungen für Dokumentbibliothek in den Einstellungen einer SharePoint-Bibliothek

Dort findet sich eine Übersicht der vorhandenen Benutzergruppen mit deren Berechtigungsstufen. Diese Einstellungen werden von der übergeordneten Websitesammlung übernommen und sind vordefiniert. Um neue Benutzergruppen mit eigenen Rechten zu erstellen, muss man das übergeordnete Element verwalten, also meist die Websitesammlung, für die man entsprechende Administrationsrechte benötigt. Um wiederum die Benutzergruppen der Bibliothek selbst bzw. ihre Berechtigungsstufen nach eigenem Bedarf anzupassen, muss zunächst die Berechtigungsvererbung beendet werden (siehe Abbildung 32).

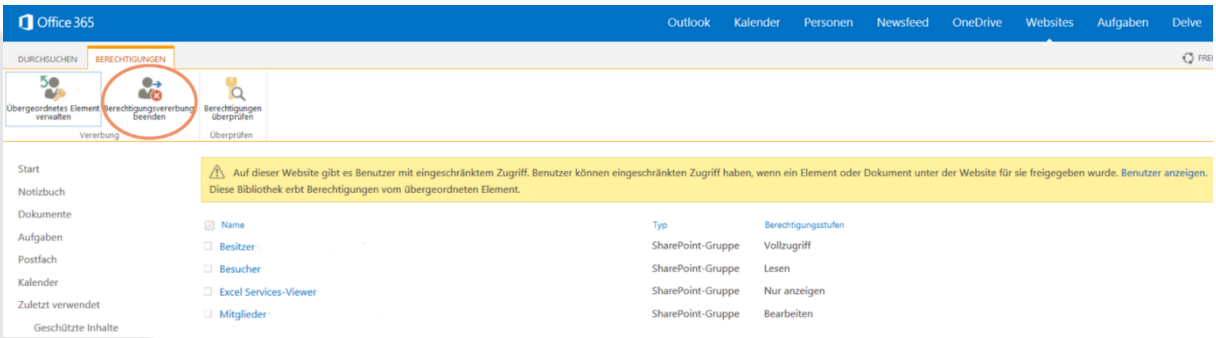

Abbildung 32: Berechtigungsvererbung in einer SharePoint-Dokumentbibliothek beenden

Dann lassen sich die Benutzerberechtigungen für ausgewählte Benutzergruppen bearbeiten (siehe Abbildung 33) oder unter „Berechtigungen erteilen“ einzelnen Benutzern bestimmte Rechte für die Bibliothek geben.

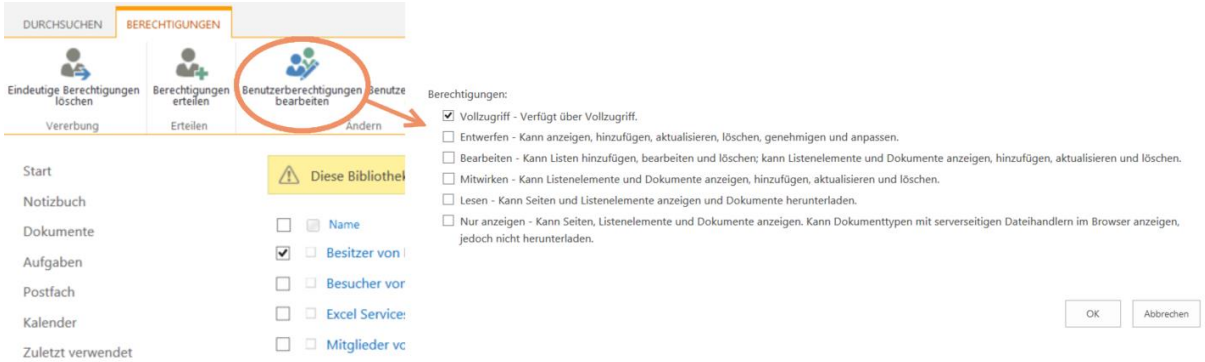

Abbildung 33: Benutzerberechtigungen einer SharePoint-Bibliothek bearbeiten

Quellen und weiterführende Links

Nachfolgend sind einige weitere Links aufgelistet, die als Quellen für diesen Artikel dienten und weiterführende Informationen zum Nachlesen sowie beispielhafte Demonstrationen von Funktionen bieten:

- TechNet Library: Azure Rights Management
- TechNet Library: Verwenden von Azure Rights Management
- TechNet Informationsportal für die Verwendung von Microsoft RMS
- TechNet Library: RMS-Freigabeanwendung
- Demonstrationsvideos von Drittanbietern:
  - Einrichtung von RMS für Einzelpersonen
  - RMS-Freigabeanwendung – Übersicht und Informationsschutz
  - RMS-Freigabeanwendung auf mobilen Geräten
  - Dokumente in SharePoint schützen