

Wer benötigt IRM?

Information Rights Management



© www.hoffmann-consultingservices.de

Das IRM System

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 Client 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.

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.



© www.hoffmann-consultingservices.de

Umgang mit Daten

Prinzipiell wird der Umgang mit Daten heutzutage in den einzelnen Unternehmen unter einem Vertrauensaspekt gesehen. Die Mitarbeiter unterschreiben bei ihrer Einstellung eine sogenannte Verpflichtungs- und Datenschutzerklärung, in der sie versichern, vertrauensvoll und im Sinne des Unternehmens zu handeln. Doch im täglichen Umgang mit vielen Megabytes von Informationen werden die Inhalte der Verpflichtungserklärung schnell vergessen. Zu einfach sind die Werkzeuge um Daten herunterzuladen, zu kopieren oder nur auszudrucken. Zu schnell lassen sich Dokumente an eine eMail anhängen oder auf einen USB-Stick ziehen. Man kann diese Vorgänge sicherlich überwachen oder protokollieren, doch kaum jemand macht sich wirklich die Mühe die dabei entstehenden Informationen auszuwerten und entsprechend zu reagieren. Der Aufwand dafür und die damit in Verbindung stehenden Kosten sind einfach zu hoch. Im übrigen lassen sich einmal versandte Daten oder Dokumente nicht wieder zurückholen. Die Verwendung von digitalen Inhalten jeglicher Art lässt sich somit im heutigen Internetzeitalter kaum mehr steuern und die Folgen davon sind nicht abzusehen.

Nun kann man sich überlegen, die Mitarbeiter dazu anzuhalten wichtige Dokumente mit Passwörtern zu schützen oder Dateien ganz zu verschlüsseln. Jedes Office-Paket verfügt heutzutage über einen Passwortschutz und es gibt einfache kostenlose Tools im Internet mit denen man Dateien schnell verschlüsseln kann. Dabei ist es jedoch erforderlich dem Empfänger ein



Passwort mitzuteilen mit dessen Hilfe er die Dokumente wieder entschlüsseln kann. Wer also über das Passwort verfügt hat den Zugriff. Auch diese Methode ist somit nicht sicher und hat verschiedene Schwachstellen. Mit Hilfe von Entschlüsselungssoftware lassen sich auch Passwortschutzgeschützte Dateien entschlüsseln und dann verwenden.

Da auch Passwörter zumeist nicht nach sicherheitstechnischen Vorgaben entworfen werden, sondern oft einfache Namen oder Geburtstage enthalten, ist es in vielen Fällen nicht sonderlich schwer sie herauszufinden. Somit sind die herkömmlichen Methoden um Informationen vor unberechtigten Zugriffen zu schützen relativ eingeschränkt und wenig vertrauensbildend. Trotzdem ist es erforderlich und mehr als wünschenswert Informationen zu schützen. Informationen bilden letztlich die Grundlage für das Geschäft eines Unternehmens und es ist in den meisten Fällen nicht zu verantworten offen, ungeschützt und transparent damit umzugehen.

Informationen und Internet

Zu viele Informationen landen heute schon fälschlicherweise im Internet. Dies betrifft einzelne Unternehmen genauso wie staatliche Behörden. Aber auch Privatpersonen sind davon betroffen. Unzählige private Bilder, Musikaufnahmen oder Videos lassen sich finden, die möglicherweise niemals von den Eigentümern zu Präsentationszwecken freigegeben wurden. Der Verwendung von fremden geistigen Eigentums sind dadurch kaum Grenzen gesetzt und die Ausschöpfung von rechtlichen Schritten dagegen ist teuer und langwierig.

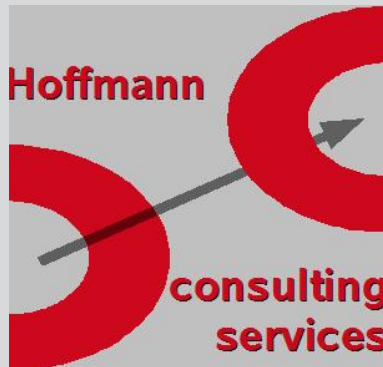


© www.hoffmann-consultingservices.de

Schützenswerte Inhalte

Wer der Meinung ist keine schützenswerten Informationen zu besitzen, sollte sich einfach einmal vorstellen, sein Rechner würde ohne Virenschoner und Firewall im Internet agieren. In kürzester Zeit wären alle Daten abgesaugt, der Rechner verseucht und unbrauchbar oder von Fremden in Beschlag genommen um dessen Rechenpower für andere Zwecke zu missbrauchen. Sofern ein Benutzer Internetbanking verwendet, wären auch seine Kontodaten verloren und möglicherweise auch sofort ein finanzieller Verlust die Folge. Sämtliche Informationen, die sich im Mailsystem finden, wären ebenfalls verloren. Adressdaten, Steuernummern, private Unterlagen, die Fotosammlung von Familien und vieles weitere wäre vernichtet oder würde von Fremden missbraucht. Ähnlich verhält es sich, wenn Notebooks von Geschäftsreisenden abhanden kommen. Der Schaden, den das gestohlene Gerät hinterlässt, ist nicht wirklich relevant. Die verlorenen Daten sind ein viel größeres Problem. Diese können einen kaum abzuschätzenden finanziellen Schaden für den einzelnen oder einen nur schwer zu verhindernden Imageverlust für ein ganzes Unternehmen nach sich ziehen.

Da die Anzahl der Diebstähle, beispielsweise an Flughäfen, extrem zunimmt, ist es erforderlich dem Rechnung zu tragen und entsprechend vorzubeugen. In den kommenden Jahren ist davon auszugehen, dass sich Datenmissbrauch und Datendiebstahl weiter extrem erhöhen werden. Daten werden heutzutage bereits wie Schmuck oder Kunst in der Vergangenheit gehandelt.



Nur wer entsprechend reagiert und vorbeugende Maßnahmen unternimmt, kann sich davor schützen. Wer trotz allem immer noch glaubt keine schützenswerten Informationen auf seinem Rechner zu haben, sollte sich überlegen sein Mailsystem für seine Kollegen, Vorgesetzten und einem möglicherweise vorhandenen Betriebsrat freizugeben.

Eventuell auch noch seinem Lebenspartner und Freunden. Allein die Vorstellung wird manch einem einen kalten Schauer über den Rücken laufen lassen. Nur wer kein EDV-System verwendet, hat wahrscheinlich keine schützenswerte Inhalte, zumindest weiß er dann nichts darüber.

IRM ist die einzige Lösung, die einen beinahe vollkommenen Schutz liefert und es Unberechtigten so gut wie unmöglich macht an fremde Inhalte zu gelangen. Dazu bietet IRM die Möglichkeit die Berechtigungen für einzelne Benutzer individuell zu konfigurieren.

Berechtigungen entscheiden

Wer über Leseberechtigungen verfügt, kann sich Dokumente ansehen, sie aber nicht kopieren oder ändern. Er kann sich die Inhalte zwar abschreiben oder mit Hilfe einer Digitalkamera abfotografieren, dies ist dann jedoch möglicherweise als Datendiebstahl oder -missbrauch zu werten und kann firmenintern entsprechend geahndet werden.



© www.hoffmann-consultingservices.de

Mit einer IRM-Lösung lassen sich auch Inhalte nach Monaten oder Jahren noch sperren um so die Weiterverwendung zu unterbinden. Dabei spielt es keine Rolle wieviele Kopien davon bereits erzeugt wurden. Nebenbei erwähnt, lässt sich damit auch sehr gut die Verwendung von veralteten Dokumenten steuern. Wenn sich beispielsweise Preislisten geändert haben, so entzieht man ganz einfach den berechtigten Nutzern die Erlaubnis auf alte Versionen zuzugreifen. So einfach lassen sich mögliche Probleme verhindern und es wird sichergestellt, dass jeder Betroffene immer mit den neuesten Informationen arbeitet. Aber auch fehlerhafte Dokumente lassen sich jederzeit sperren und durch neue ersetzen, unabhängig davon wo sie sich bereits überall befinden.

Durch Berechtigungszuteilung, -änderung oder -entzug lassen sich auch unternehmensweite Workflows und Arbeitsprozesse steuern. Daran sollte man unbedingt denken, wenn ein Mitarbeiter intern andere Aufgaben übernimmt oder sich sein Verantwortungsbereich erweitert. Man sperrt ihm ganz einfach den Zugriff auf seine alte Umgebung und schaltet ihn durch die Zuordnung in eine andere Gruppe für die neuen Aufgaben frei.

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.



KONTAKT

email: info@hoffmann-consultingservices.de

Tel: +49 (7141) 24 22 473

mobil: +49 (172) 83 22 925