



XXX

XXX

Es gibt Dinge, die jagen einem den kalten Schauer über den Rücken. Schon der Gedanke daran lässt uns nervös den Angstschweiß von der Stirn wischen: Datendiebstahl. Ein Vorgang, der heute alles oder nichts bedeuten kann, wird schneller möglich, als wir glauben, besonders dann, wenn vertrauliche Informationen aus Daten und Dokumenten, weitergeleitet, verändert oder ausgedruckt wurden. Auch wenn sie meist per Passwort auf dem Server geschützt sind, verliert man jede Kontrolle über sie, sobald sie geöffnet werden. Einmal gestohlen, kann dies mindestens zur Beeinträchtigung des wirtschaftlichen Erfolg führen - wenn nicht zu mehr.

Gut, dass es bei allem Schrecken hier dennoch Superlösungen, wie verschiedene Information Rights Management (IRM) Systeme gibt. Sie bieten Schutz für viele Dateiformate, angefangen von Microsoft Office über Adobe PDF bis hin zu Bildern und Autodesk AutoCAD. IRM Softwarelösungen kontrollieren nicht nur Zugriff, sondern auch Art, Zeitraum und Ort der Nutzung. Sie schützen Dokumente auch während und nach dem Versand und können durch Dritte nicht betrachtet, verändert, kopiert oder weitergeleitet werden.

Die Zugangsberechtigung wird hier in jeder Datei selbst gespeichert, während die zum Öffnen zusätzlich benötigte Lizenz auf einem zentralen Server hinterlegt wird. Mit Hilfe einer automatisierten Rechtevergabe können Dateien schnell Personen oder Gruppen, auch zeitlich eingeschränkt, zugeordnet oder entzogen werden. Dabei stellt ein IRM System sicher, dass immer mit der aktuellen Version eines Dokuments gearbeitet wird. Durch die Integration von IRM-Funktionen in etablierte Anwendungen, wie Office Programme, Dokumentenmanagement Systeme (DMS) oder Workflow Systeme, unterscheidet sich das Erstellen und Öffnen von geschützten Informationen kaum von der bekannten Arbeitsweise.

Trotzdem heißt es immer wachsam sein, denn auch IRM-Systeme sind nicht völlig unüberwindlich, da alle elektronischen Verarbeitungssysteme und Übertragungswege verletzlich sind. So schützt IRM nicht gegen die Anfertigung von Screenshots, bestimmter Spyware, Trojanische Pferde oder Systeme zur Speicherung von Tastatureingaben.