

IT-Sicherheit außerhalb des Firmmentors

In den letzten Jahren wurde viel in die IT-Sicherheit investiert. Ein großer Bereich blieb dabei aber unberücksichtigt: Was geschieht mit den Daten, die per E-Mail verschickt werden oder per USB-Stick das Unternehmen verlassen. Die Software Oracle Informations Rights Management bringt Abhilfe.



› Schutzmaßnahmen

Damit vertrauliche Informationen nicht versehentlich in die falschen Hände gelangen und damit unberechenbaren Schäden und Imageverluste für das Unternehmen bringen, muss es möglich sein:

- nachzuvollziehen wer das Dokument gelesen, geändert oder gedruckt hat;
- unbefugte Zugriffe oder Änderungen zu verhindern;
- den Zugang zu den Informationen auch jederzeit widerrufen zu können, vor allem auch dann, wenn das Dokument das Firmmentor bereits verlassen hat.

Viele Unternehmen investieren in IT-Sicherheit: beispielsweise in Perimeterschutz, Firewall oder in die Hochverfügbarkeit des Systems. Die große Gefahr lauert aber anderswo. Tag für Tag werden Dokumente von Mitarbeitern kopiert, verändert, ausgedruckt oder per E-Mail verschickt. Sobald Dokumente mit sensiblen Daten per E-Mail, auf Laptops oder USB Sticks nach außen getragen werden, entziehen sie sich der Kontrolle der IT-Abteilung. Somit könnten diese Dokumente auch von nicht autorisierten Personen innerhalb und außerhalb der Unternehmensfirewall geöffnet, gelesen, modifiziert und weitergeleitet werden. Das große Sicherheitsproblem liegt also nicht nur in den gezielten Aktivitäten von Cyberkriminellen, sondern auch in der unbewussten Nachlässigkeit von Anwendern im Umgang mit „vertraulichen Informationen“.

[**Die Lösung**] Mit der automatischen Rechtevergabe von Oracle Information Rights Management (IRM) können unerlaubte Dokumentenzugriffe verhindert und die Verwaltung zentral und einfach abgewickelt werden, und zwar ohne dabei die Anwender mit neuen Programmen oder Arbeitsabläufen zu belasten.

Mit IRM können Dokumente mit standardisierten oder spezifischen Rechten eindeutig Einzelpersonen, Benutzergruppen oder Abteilungen zugewiesen werden. Die Rechte können Lese-, Zugriffs- und Bearbeitungsrechte umfassen und können notfalls manuell oder auch automatisch, wie zum Beispiel bei Fälligkeit, wieder entzogen werden. Der Zugriff ist zentral und einfach zu verwalten, indem die vordefinierten Rechte auf dem Dokument mit dem zentralen Server vorab abgeglichen werden.

Auch offline kann man die Dokumente, falls man in Besitz der notwendigen Rechte ist, noch lesen oder bearbeiten, da die lokal zwischengespeicherten Rechte angewandt werden, aber ohne der transparenten „Freischaltung“ durch diese PC-Software ist das Dokument nicht verwendbar.

Die einfach zu installierende Software kann auch bei einer sehr großen Dokumentenanzahl



Alexander Kiesswetter, Geschäftsführer von Dexea - Unternehmensgruppe Dedagroup

eingesetzt werden und lässt sich nahtlos mit der Windows-Umgebung und Anwendungen wie Microsoft Office und Adobe Reader integrieren.

[**Zielgruppe**] Oracle Information Rights Management, als zentral organisierte und digitale Zugriffsrechteverwaltung, bietet sich vor allem für Unternehmen mit verzweigten Standorten oder großen Dokumentenaustausch mit Lieferanten und Partnern an.

Die Einführung von Oracle IRM muss aber in ein organisatorisches und technologisches Gesamtkonzept eingebunden werden, um nicht wieder nur einzelne Sicherheitslücken zu stopfen. [X]

› info

Dexea GmbH
Messeplatz 1
39100 Bozen
Tel. 0471 500 403
Fax 0471 203 251
www.dexea.it
a.kiesswetter@dexea.it