

Unternehmens integriert werden können, denn unterschiedliche Bearbeitung der Dokumente mit entsprechender Rollen- und Rechteverwaltung können im Unternehmen bereits etabliert sein. Dies wird beispielsweise bei der Vergabe von Nutzungsrechten für eine Datei oder eine E-Mail deutlich: In Organisationen ist es keine Seltenheit, dass Dateien von mehreren Mitarbeitern aus verschiedenen Abteilungen verwendet werden. Sie sollen die Informationen unter Umständen aber nicht alle in der gleichen Art verwenden dürfen. Die Vergabe von Nutzungsrechten per Hand für jeden Mitarbeiter wäre dabei mühselig und wenig effizient. Daher muss ein ERM-System in der Lage sein, die Identitäten, Rollen und Rechte eines Identitäts- und Zugangsmanagementsystems zu verwenden.

Um die Vergabe der Nutzungsrechte weiter zu vereinfachen, werden so genannte Policy Templates verwendet. Diese Vorlagen müssen in einem ERM-System erstellt und verwaltet werden können. Zudem kann es nach der initialen Vergabe von Nutzungsrechten nötig werden, die Rechte eines Mitarbeiters nachträglich zu erweitern, beschränken oder komplett zu entziehen. Ein ERM-System sollte dafür ein entsprechendes Rechtmanagement zur Verfügung stellen.

Wenn ein Benutzer auf eine geschützte Datei zugreifen will, muss er zunächst eine Lizenz anfordern. Dazu muss er eindeutig identifiziert werden können. Eine sichere Methode hierfür ist der Einsatz von PKI-Zertifikaten. Um die Kosten und den Verwaltungsaufwand zu minimieren, sollte ein ERM-System die Zertifikate einer bestehenden Unternehmens-PKI verwenden können. Wenn ein

ERM-System außerdem die Lizenzanfragen protokolliert, kann ein Unternehmen nachvollziehen, wer wann versucht, auf ein geschütztes Dokument zuzugreifen. Diese Möglichkeit bietet eine zusätzliche Ebene an Sicherheit, die durch ERM erreicht werden kann.

Ganzheitliches Sicherheitskonzept

Gerade der letzte Punkt – der Zugriff des ERM-Systems auf die vorhandenen Identitäten, Rollen und Rechte – macht deutlich, dass auch das Enterprise Rights Management Bestandteil einer Sicherheitslösung aus einem Guss sein sollte. Im gleichen Maß, wie die Zusammenarbeit in digitalen Arbeitsprozessen ausgebaut wird, steigt das Sicherheitsbedürfnis eines Unternehmens und damit auch die Notwendigkeit, Dokumente und Informationen vor unbefugtem Zugriff zu schützen. Eine ganzheitliche Lösung sollte ERM deshalb einerseits mit dem Identitätsmanagement im Unternehmen verknüpfen. Andererseits können durch den Einsatz von Zertifikaten organisationsübergreifende Kollaborations- und Geschäftsprozesse nachhaltig gesichert werden. ■

* Dr. Willi Kafitz ist Sicherheitsexperte und Senior Consultant bei Siemens Enterprise Communications in Frankfurt. Dirk Weissenbacher ist Consultant im Center of Competence Trusted Identity von Siemens Enterprise Communications in Essen.

Internet: www.siemens.de/open

Stichworte: Digital Rights Management (DRM), Enterprise Rights Management (ERM), Dokumentenschutz, Informationskontrolle, Identitätsmanagement

Bezugsquelle der Studie zu „Kosten von Datenpannen“

Die Studie zu den „Kosten von Datenpannen in Deutschland“ des Ponemon-Institute, über die in der letzten Ausgabe berichtet wurde (DSB 4/09, Seite 15), ist über die Firma PGP nach einer kostenlosen Registrierung verfügbar. Auch die Studien zu Großbritannien und den USA können heruntergeladen werden. Die Redaktion bittet die verse-

hentliche Nennung der Website des Europäischen Datenschutzbeauftragten auf Seite 17 zu entschuldigen. ■ SF

Internet: www.pgp.com/de/insight/research_reports/index.html

Stichworte: Studie, Ponemon, Datenpannen, Kosten