

PRESSEMITTEILUNG

Fünf Fragen an ... / INTERVIEW

Digitale Rechteverwaltung: „Mehrwert gegenüber analogen Verfahren“

- Digitale Lösung erleichtert Vergabe von Zugriffsrechten
- Rollenkonzepte verringern administrativen Aufwand
- Welche Leistungsmerkmale bietet eine geeignete Lösung?

Bielefeld, 02.12.2020 – Durch die Corona-Pandemie hat die Etablierung des Home-Office in deutschen Unternehmen einen Schub erhalten. Damit Dokumente ortsunabhängig bearbeitet werden können, müssen sie digital vorliegen. Das bringt viele Vorteile mit sich, macht aber auch ein konsistentes System für Zugriffsrechte nötig. Andreas Ahmann, Experte und Berater für Informationsmanagement, beantwortet im Interview alle wichtigen Fragen rund um das Thema und zeigt die Vorzüge von digitalen Rechte- und Rollenkonzepten auf.

Frage: Welche Funktion haben Zugriffsberechtigungen für Unternehmen?

Andreas Ahmann: Nicht jede verfügbare Information in einem Unternehmen ist auch für jeden Mitarbeiter bestimmt. Ein gutes Beispiel sind Personalakten. Die darin enthaltenen Daten sind sensibel und dürfen nur von Personen eingesehen werden, die auf diese Informationen im Zuge ihrer Arbeit zugreifen müssen. Also werden die Akten entsprechend geschützt. Früher wurden schützenswerte Informationen unter Verschluss gehalten und nur wer zugriffsberechtigt war, besaß einen Schlüssel. Doch war dieses Verfahren

teuer und unflexibel. Heute erfolgt der Informationsschutz mithilfe digitaler Zugriffsrechte. Ein Mehrwert gegenüber dem analogen Verfahren ist die Möglichkeit, neben dem schlichten Zugriff beliebig auch ganz bestimmte Rechte zu erteilen. Am bekanntesten sind wohl „create“, „read“, „update“ und „delete“ – also die Rechte, ein Dokument zu erzeugen, zu lesen, zu verändern oder zu löschen.

Frage: Wie hängen Zugriffsberechtigungen mit Rollenkonzepten zusammen?

Ahmann: Die Komplexität der Rechtevergabe wächst mit der Unternehmensgröße. Um beim Bild des Schlüssels zu bleiben, den ein Mitarbeiter besitzen muss, um auf eine Information zugreifen zu können: Mehr Mitarbeiter, mehr Dokumente und somit mehr schützenswerte Informationen führen dazu, dass es sehr viele verschiedene Schlüssel geben muss. Um hohen administrativen Aufwand bei diesem Vorgehen zu vermeiden, gibt es Rollenkonzepte. Es werden bestimmte Personengruppen gebündelt – zum Beispiel die Buchhaltung – denen eine Rolle zugewiesen wird. Diese Rollen folgen bestimmten Regeln. Eine solche Regel könnte lauten: „Personen mit der Rolle Buchhaltung dürfen auf die Finanzbuchhaltung zugreifen.“ Es ist also nicht mehr nötig, einzelne Schlüssel zu verteilen. Es reicht aus, Mitarbeitern einer bestimmten Rolle zuzuordnen, damit sie alle zugehörigen Berechtigungen erben.

Frage: Wie kann ein Enterprise-Information-Management-System (EIM) helfen?

Ahmann: Als zentrale Informationsplattform kann eine EIM-Lösung eine entscheidende Bedeutung bei der Verwaltung von Zugriffsrechten besitzen. Moderne Systeme integrieren alle geschäftskritischen Vorgänge wie zum Beispiel das Vertragsmanagement, die Eingangsrechnungsverarbeitung und den digitalen sowie analogen

Posteingang. Dadurch, dass hier alle Dokumente und Informationen eines Unternehmens zusammenfließen, ist das EIM prädestiniert für diese Aufgabe. Zudem bieten solche Lösungen die schon angesprochenen Rollenkonzepte, was bei herkömmlichen Filesystemen meist nicht der Fall ist.

Frage: Was sollte das eingesetzte System im Idealfall bieten?

Ahmann: Hier sind nicht nur die Berechtigungen interessant, auf bestimmte Informationen zugreifen zu können. Führende Lösungen ermöglichen zusätzlich auch die Vergabe von Zugriffsrechten auf Prozesse. Ein EIM sollte entsprechende Funktionen integrieren, also etwa die Gestaltung von Workflows unterstützen. Darüber hinaus muss es auch die Vergabe von passenden Rechten erlauben: Wer darf einen Workflow starten, pausieren oder abschließen? Außerdem muss es möglich sein, eigene, unternehmensspezifische Regelwerke zu implementieren.

Frage: Welche Besonderheiten sind beim mobilen Arbeiten zu beachten?

Ahmann: Außerhalb des Büros ist die Gefahr größer, dass sich Kriminelle Zugriff auf wichtige Informationen verschaffen. Die Verschlüsselung dieser Informationen ist eine wirkungsvolle Schutzmaßnahme. Auch der Einsatz eines clientseitigen Zertifikats ergibt Sinn. Hierbei prüft der Server in der Unternehmenszentrale zusätzlich zur Anwender-Authentifizierung auch, ob das verwendete Gerät als unbedenklich deklariert wurde. Vermehrt kommt heute auch die Zwei-Faktor-Authentifizierung auf, bei der zusätzlich zu den Anmeldedaten zum Beispiel noch eine TAN eingegeben werden muss. Der Trend geht ganz klar in diese Richtung.

Erhalten Sie mehr Infos zur Verwaltung von Zugriffsrechten in der neuen Folge des Ceyoniq-Podcasts „SchonDigital?“:

<https://www.ceyoniq.com/news/create-read-update-and-delete>

Über die Ceyoniq Technology GmbH:

Die Ceyoniq Technology GmbH ermöglicht Unternehmen und öffentlichen Verwaltungen einen einfachen und sicheren Umgang mit Informationen durch passgenaue digitale Lösungen, die Prozesse beschleunigen und den Weg in die digitale Zukunft bereiten.

Seit mehr als 30 Jahren entwickeln wir intelligente Software-Lösungen für das Informations- und Dokumentenmanagement. Die Basis bildete unsere Archivierungssoftware, aus welcher unser heutiges Enterprise Information Management (EIM) System nscale entstand. Mit einem starken Team von mehr als 160 Kolleginnen und Kollegen verstehen wir uns als Digitalisierer, Impulsgeber, Entwickler, Berater, Prozessoptimierer und Möglichmacher für unsere Kunden.

Die Ceyoniq Technology GmbH mit Hauptsitz in Bielefeld und weiteren bundesweiten Standorten ist ein Tochterunternehmen der KYOCERA Document Solutions Inc.

Kontakt für Journalisten & Redaktionen:

Malte Limbrock
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Marie-Curie-Straße 5
53359 Rheinbach
Tel.: +49 (0)228 / 30412-630
Fax: +49 (0)228 / 30412-639
limbrock@sputnik-agentur.de
www.sputnik-agentur.de

Arne Kleinekathöfer
Ceyoniq Technology GmbH
Leiter Marketing
Boulevard 9
33613 Bielefeld
Tel.: +49 (0)521 9318-1612
Fax: +49 (0)521 9318-1111
a.kleinekathoefer@ceyoniq.com
www.ceyoniq.com