Interview

Unter digitalem Verschluss

[25.03.2021] Früher waren sensible Akten unter Verschluss. Heute werden digitale Informationen mithilfe von Zugriffsrechten geschützt. Andreas Ahmann, Experte für Informationsmanagement, spricht über die Vorteile digitaler Rechtekonzepte für mobiles Arbeiten.

Herr Ahmann, was sind die Voraussetzungen für die Arbeit im Homeoffice?

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.

Welche Funktion haben Zugriffsberechtigungen?

Es ist klar, dass nicht jede verfügbare Information in einer Behörde auch für jeden Mitarbeiter bestimmt ist. 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 dieses Verfahren ist teuer und unflexibel.

Was ist die Alternative?

Heute erfolgt der Informationsschutz mithilfe digitaler Zugriffsrechte. Ein Mehrwert gegenüber dem analogen Verfahren ist die Möglichkeit, neben dem schlichten Zugriff auch ganz bestimmte Rechte zu erteilen. Am bekanntesten sind wohl die Rechte, ein Dokument zu erzeugen, zu lesen, zu verändern oder zu löschen.
Wie hängen Zugriffsberechtigungen mit Rollenkonzepten zusammen?
Die Komplexität der Rechtevergabe wächst mit der Größe einer Organisation. 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 einen hohen administrativen Aufwand bei diesem Vorgehen zu vermeiden, gibt es Rollenkonzepte. Dabei 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, Mitarbeiter einer bestimmten Rolle zuzuordnen, damit sie alle zugehörigen Berechtigungen erben.

„Die Komplexität der Rechtevergabe wächst mit der Größe ?einer Organisation.“

Wie kann ein Enterprise-Information-Management-System (EIM) dabei helfen, die Zugriffsrechte zu verwalten?

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 zusammenfließen, ist das

EIM prädestiniert für diese Aufgabe. Zudem bieten solche Lösungen die schon angesprochenen Rollenkonzepte, was bei herkömmlichen File-Systemen meist nicht der Fall ist.

Was sollte das eingesetzte System im Idealfall bieten?

Interessant sind hier nicht nur die Berechtigungen, 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 die Vergabe von passenden Rechten erlauben: Wer darf einen Workflow starten, pausieren oder abschließen? Außerdem muss es möglich sein, eigene, unternehmensspezifische Regelwerke zu implementieren.

Welche Besonderheiten sind beim mobilen Arbeiten zu beachten?

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 zusätzlich zur Anwender-Authentifizierung, ob das verwendete Gerät als unbedenklich deklariert wurde. Vermehrt kommt heute die Zwei-Faktor-Authentifizierung zum Einsatz, bei der neben den Anmeldedaten zum Beispiel noch eine TAN eingegeben werden muss. Der Trend geht ganz klar in diese Richtung.

()

Mehr Infos zur Verwaltung von Zugriffsrechten erhalten Sie im Ceyoniq-Podcast „SchonDigital?“
Dieser Beitrag ist im Titel der Ausgabe März 2021 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Homeoffice