Access Governance – und was dahintersteckt

In Öffentlichen Verwaltungen kommt es im **Mitarbeitergefüge** ständig zu Veränderungen: Ein Angestellter wechselt die Abteilung, ein anderer kündigt, eine Kollegin geht in Elternzeit. Oft ist die IT-Abteilung das letzte Glied in der Kette, das davon erfährt. Entsprechend werden **sensible Zugriffsberechtigungen** der (Ex-)Kollegen meist nicht tagesaktuell verändert. An diesem Punkt greift ein häufig gehörtes, aber nicht immer verstandenes Konzept: Access Governance.

Bild: XtravaganT_Fotolia.com

In den Netzwerken Öffentlicher Verwaltungen tummeln sich Unmengen sensibler – und damit schützenswerter – Daten. Eine klassische Security-Software allein reicht nicht aus; zusätzlich sollten die Zugriffsberechtigungen der Mitarbeiter kontrolliert und dokumentiert werden. Denn: Mitarbeiter sind Menschen, und Menschen machen Fehler. Insbesondere bei der Verwaltung vertraulicher Daten spielt der „Faktor Mensch" eine entscheidende Rolle. Werden die einzelnen Zugriffsberechtigungen der Mitarbeiter nicht zentral überwacht, entsteht ein großes Durcheinander in Öffentlichen Verwaltungen.

Denn die Berechtigungsvergaben für Daten, Netzwerke & Co. sind ein sich stetig wandelndes Gebilde. Schließlich verändern sich auch interne Mitarbeiterstrukturen häufig – vor allem in Öffentlichen Verwaltungen, die örtlich verteilt sind. Verantwortliche in der IT-Abteilung wissen oftmals nicht, welcher Mitarbeiter aktuell welche Zugriffsrechte besitzt. Dieser Missstand könnte ausgenutzt werden: beispielsweise, wenn ein externer Kollege im Rahmen eines spezifischen Projekts auf interne Daten der Verwaltungsorganisation zugreifen darf und die IT-Abteilung versäumt, seine Zugriffsberechtigung nach Abschluss des Projekts aufzulösen. Denn der externe Mitarbeiter könnte sich jetzt unbemerkt im Netzwerk austoben und im schlimmsten Fall Manipulationsversuche starten.

Um entsprechenden Risiken vorzubeugen, müssten die IT-Verantwortlichen die Zugriffsberechtigungen kontinuierlich überwachen und kontrollieren. Doch gerade in Öffentlichen Verwaltungen, die dezentrale, meist nur schwer zu überblickende Strukturen aufweisen, ist ein einheitliches, schnelles und tagesaktuelles Reporting ohne unterstützende Software-Lösung quasi nicht möglich.

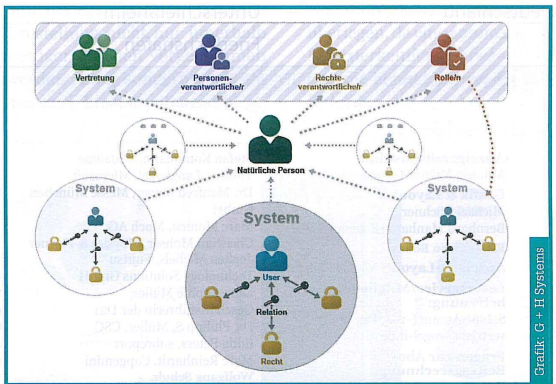
Schluss mit umständlicher Datenauslese

Auf dem Markt gibt es professionelle Access Governance-Lösungen, die alle Zugriffsrechte innerhalb der verwaltungsweiten IT-Landschaft zentral erfassen. Die Software ist bestenfalls zu allen genutzten Systemen (herstellerunabhängig) kompatibel, sodass es keine Übertragungs- oder Formatschwierigkeiten gibt. Ohne ein solches Tool müssten IT-Abteilungen aktuelle Zugriffsberechtigungen umständlich und zeitaufwendig auslesen, analysieren, abgleichen und aktualisieren – und das neben dem normalen Tagesgeschäft.

Eine Access-Governance-Lösung veröffentlicht die gesammelten Daten auf einer zentralen Web-Oberfläche. So erhalten IT-Teams schnellen Zugriff auf die erforderlichen Informationen zu den jeweilig gewährten Zugriffsrechten der Mitarbeiter, zum Beispiel wenn essenzielle Berechtigungen fehlen oder (Ex-)Kollegen fälschlicherweise immer noch Zugriffsmöglichkeiten besitzen.

Wichtig ist zudem, dass die Software alle Daten für Analysen, Bereinigungen von Berechtigungen oder Löschungsanträge strukturiert und visualisiert. Denn nur die Strukturierung aller Informationen bringt öffentlichen Verwaltungen einen Mehrwert – und diese Strukturierung kann recht simpel geschehen. In öffentlichen Verwaltungen arbeiten Personen, Personen haben Benutzerkonten, und Benutzerkonten besitzen Berechtigungen. Eine Access-Governance-Lösung hat exakt diese Aufgabe, teils komplexe Strukturen so anschaulich und so einfach wie möglich darzustellen und dadurch schnelle Antworten auf kritische Fragen zu geben (zum Beispiel welche Benutzerkonten und Berechtigungen ein Angestellter innerhalb der IT-Landschaft innehat). Neben diesen technischen Vorgängen im Backend der Software ist für Anwender aber vor allem das Frontend von Bedeutung.

Auch hier ist Übersicht und Einfachheit Trumpf. Eine professionelle Lösung stellt alle relevanten Informationen personalisiert und verständlich bereit: übersichtliche Reports statt verwirrender IT-Fachtermini. Nutzer sollen auf einen Blick sehen, welche Konten ungenutzt oder welche Benutzerkonten verwaist sind (beispielsweise weil ein Kollege mittlerweile im Ruhestand ist). Gerade diese verwaisten Benutzerkonten verursachen zusätzliche finanzielle Belastungen, da für jedes Benutzerkonto in der Regel Lizenzgebühren entrichtet werden müssen. Eine Access-Governance-Software deckt solche Mängel auf und hilft öffentlichen Verwaltungen somit beim Geldsparen.



Datenmodell der Access-Governance-Lösung „daccord"

Jede Abteilung kennen

Darüber hinaus bieten professionelle Lösungen zahlreiche Funktionen zur individuellen Konfiguration. Ein Beispiel dafür sind so genannte Soll-Berechtigungsmodelle. Richtet man diese Vorgaben ein, meldet die Software, wenn es bei der Analyse zu Abweichungen von den gewünschten und vereinbarten Berechtigungen kommt. Auf diese Weise können die Berechtigungen von Personen übergreifend bewertet werden, zum Beispiel gegenüber dem jeweiligen Stellen- und Tätigkeitsprofil oder gegenüber Kollegen, die eigentlich die gleichen Berechtigungen haben müssten.

Je größer eine Öffentliche Verwaltung, desto unwahrscheinlicher ist es, dass die IT-Abteilung das Berechtigungsprofil der einzelnen Mitarbeiter im Detail kennt. Eine Access-Governance-Software hingegen kennt jede Abteilung inklusive der dortigen Umstände und Besonderheiten. Die Berechtigungen können somit fachlich beurteilt und schnell in die richtigen Hände gegeben werden.

Ferner ist es möglich, die Verantwortlichkeit für komplette Systeme mit allen Benutzerkonten und Berechtigungen auch einzelnen Personen zuzuweisen. Der jeweilige Verantwortliche weiß in der Regel am besten, wer warum welche Berechtigung besitzen sollte und wer nicht.

Entsprechende Berechtigungskonzepte und -vorgaben, die Verwaltungen festlegen, müssen kontinuierlich auf ihre Einhaltung überprüft werden. Punktuelle Stichproben reichen nicht aus. Die Access-Governance-Lösung hat alle Zugriffsrechte stets im Auge und schlägt Alarm, falls eine vorgegebene Regel verletzt wird, ein Zugriffsprofil einer Person/Rolle nicht mit den dafür bestimmten Rechten übereinstimmt oder gar Berechtigungen bestehen, die gar nicht erlaubt sind. In diesem Fall alarmiert die Software die IT-Abteilung oder andere verantwortliche Führungskräfte umgehend, sodass sie reagieren können.

Die kontinuierliche Überwachung der Software unterstützt auch bei der Einhaltung gesetzlicher Vorgaben. Denn manche Öffentliche Verwaltungen könnten im Sinne des Datenschutzes der Pflicht unterliegen, in bestimmten Zyklen so genannte Rezertifizierungen durchzuführen. Dabei werden Benutzerkonten und Berechtigungen überprüft. Professionelle Access-Governance-Lösungen stellen diese Informationen übersichtlich bereit. Da die Software die Methode der fortlaufenden Überprüfung der Berechtigungen (Continuous Auditing) verfolgt, müssen bei der Rezertifizierung ausschließlich Veränderungen bestätigt werden, was der IT-Abteilung enorme Zeitersparnisse ermöglicht.

Cloud-Überwachung

Darüber hinaus helfen Access-Governance-Lösungen auch bei der kontinuierlichen Überwachung von Cloud-Anwendungen, die sich aktuell stark vermehren. Applikationen in die Cloud zu verlagern, spart zwar Ressourcen innerhalb der Infrastruktur, die Cloud-Apps sind jedoch ohne zusätzliches Überwachungs-Tool kaum zu kontrollieren. Mitarbeiter könnten beispielsweise unbemerkt ein Google Doc im Web anlegen, dort sensible Firmendaten mit Partnern teilen und selbstständig Zugriffsrechte verteilen. Dies geschieht nicht selten ohne Genehmigung der IT-Fachabteilung.

Damit sensible Unternehmensinformationen vor den Augen unbefugter Dritter geschützt werden, überprüfen Access-Governance-Lösungen auch die Zugriffsberechtigungen für Cloud-Anwendungen und stellen sie zusammen mit den Berechtigungen gewöhnlicher IT-Systeme auf dem zentralen User-Frontend der Software dar.

100 Prozent Transparenz

Die größte IT-Schwachstelle sind häufig die Mitarbeiter selbst oder deren unklar definierte Zugriffsberechtigungen. Von externer wie interner Seite entsteht dadurch ein erhöhtes Manipulationsrisiko. Access-Governance-Lösungen bringen die Kontrolle und Sicherheit zurück. IT-Abteilungen und -Verantwortliche wissen immer Bescheid, wer wann worauf zugreift – und die Erlaubnis dafür hat. Das schafft hundertprozentige Transparenz im Netzwerk.

Der Autor

René Leitz, Teamleiter Product Development bei G+H Systems GmbH

Weitere Informationen ...

... zum Unternehmen G+H Systems gibt es online unter

[www.guh-systems.de]