HZ208307 · ISSN 1868-5757 · www.datakontext.com Februar 1/2021

IT-SICHERHEIT

Magazin für Informationssicherheit und Datenschutz

Künstliche Intelligenz: Fair oder gefährlich?

Warum Ethik in der KI zum zentralen Thema wird

Schwerpunkt Cybersecurity:
Trends, E-Mail, Ransomware, Banking

Datenschutz:
Folgenabschätzung risikobehafteter Tools am Beispiel von Microsoft 365

Cloud-Forensik:
Blick in die großen „Verstecke“ von Cyberkriminellen

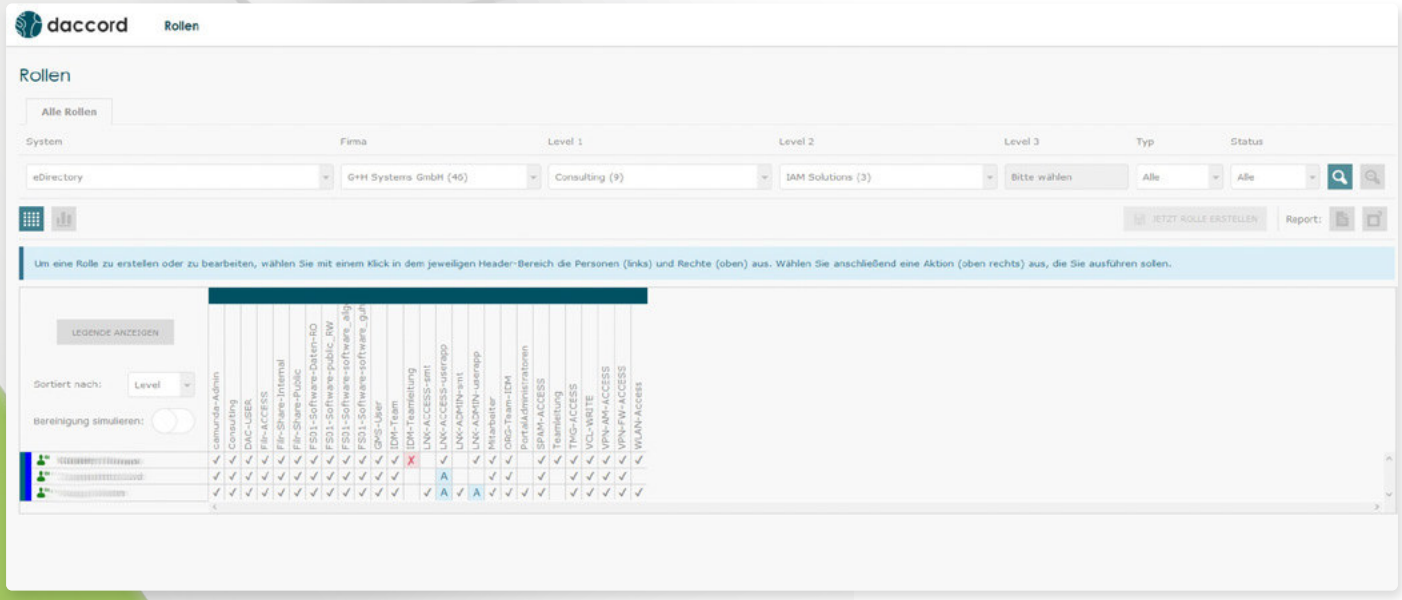
DATAKONTEXT

Vereinfachte Kontrolle des Berechtigungskonzepts durch ein Rollenmodell

GEORDNETE RECHTESTRUKTUREN

Je nach Abteilung und Position dürfen Mitarbeiter nur die IT-Berechtigungen besitzen, die sie für die Ausübung ihrer Tätigkeit benötigen (Need-to-know-Prinzip) – so sollte es zumindest sein. Denn in der Praxis sieht das häufig anders aus. Aufgrund von betrieblichen Anforderungen, wie beispielsweise dem Abteilungswechsel eines Mitarbeiters, müssen Berechtigungen immer wieder angepasst werden. Ebenso gut kann es vorkommen, dass ein Arbeitnehmer temporär Berechtigungen erhält, weil er Unterstützung in einem speziellen Projekt leisten muss. Um diese Berechtigungsveränderungen nachvollziehen, bewerten und kontrollieren zu können, hilft der Einsatz einer Access-Governance-Lösung; im Speziellen die Nutzung eines softwaregestützten Werkzeugs zur Rollenbildung. Durch ein entsprechendes Rollenmodell ist der Vergleich zwischen den Berechtigungen, die ein Mitarbeiter haben sollte (Soll-Rollenmodell), und den tatsächlich vergebenen Berechtigungen (Ist-Zustand) auf Knopfdruck möglich.

Abhängig davon, in welcher Position und Abteilung ein Mitarbeiter arbeitet, benötigt er bestimmte Rechte. So muss beispielsweise der Personalleiter auf andere Applikationen und Daten zugreifen als Verantwortliche in der Fertigung. Insgesamt gilt es, alle Angestellten mit den essenziellen Rechten auszustatten, aber Überberechtigungen unter allen Umständen zu vermeiden. Denn mit jeder falsch vergebenen Berechtigung steigt das Risiko, dass durch Überberechtigungen Sicherheitslücken oder falsche Berechtigungskonstellationen entstehen („Segregation of Duties"), die unbedingt vermieden werden müssen. Daher sollten Rollen und Rechte innerhalb des Unternehmens eindeutig festgelegt sein und jederzeit in einer anschaulichen Übersicht eingesehen werden können. Dabei kann eine Access-Governance-Lösung unterstützen.



Matrix-Ansicht im daccord RoleBuilder von G+H Systems (Quelle: G+H Systems)

STRUKTURIERTE RECHTEVERGABE ÜBER EIN ROLLENMODELL

Für gewöhnlich gibt es in Unternehmen mehrere Mitarbeitergruppen, die die gleichen Rechte haben sollten. Dies trifft zum Beispiel häufig auf Personen aus derselben Abteilung zu. Ist dies der Fall, können diverse Rechtekombinationen mit einer entsprechenden Access-Governance-Lösung softwaregestützt zu Rollen und Rollenstrukturen zusammengefasst werden. Mitarbeiter aus derselben Abteilung haben dann gegebenenfalls die gleiche Rolle. Führt man diese Schritte für das komplette Unternehmen weiter aus, erhält man ein Soll-Rollenmodell, das sich jederzeit mit dem aktuellen Ist-Zustand vergleichen lässt. Fallen hierbei Missstände auf, können diese mit Blick auf den Soll-Zustand einfach behoben werden.

Kommt es zu Änderungen, werden neue Arbeitnehmer eingestellt, oder stellt sich generell die Frage, wer welche Berechtigungen haben soll, müssen dem jeweiligen Arbeitnehmer die Rechte durch den Einsatz einer Access-Governance-Lösung nicht mehr einzeln zugewiesen werden. Stattdessen kann man dieser Person eine oder mehrere Rollen zuweisen. Dadurch wird der Prozess deutlich vereinfacht und fehlerhaften Rechtestrukturen effektiv begegnet.

INTELLIGENTE UND EFFIZIENTE ROLLENMODELLIERUNG

Unternehmen haben die Notwendigkeit, ein Rollenmodell auf Basis der aktuell vergebenen Berechtigungen aufzubauen. Doch was ist hier eine sinnvolle und vor allem effiziente Herangehensweise? Und was sollte ein softwaregestütztes Werkzeug zur Rollenbildung unbedingt mitbringen? Sechs Schritte führen zum passenden Rollenmodell:

1. Darstellung der Mitarbeiter und deren Berechtigungen nach Organisationseinheiten (Position, Team, Abteilung)
2. Analyse des gewählten Personenkreises auf ähnliche Rechtekombinationen
3. Übersichtliche Ansichten und Filtermöglichkeiten über Systeme, Personen und deren Berechtigungen
4. Unterstützung bei der Rollenbildung durch Aufzeigen prozentualer Verteilung eines Rechtes, beispielsweise innerhalb einer Abteilung
5. Bündelung der Berechtigungen zu Rollen
6. Zuordnung der Rollen zu Personen

Insgesamt stellen die Themen Berechtigungsvergabe, -entzug und -kontrolle eine große Herausforderung für Unternehmen dar. Mit einem erarbeiteten Rollenmodell und der Einbettung in eine Access-Governance-Lösung lassen sich jedoch Zeit und Kosten hinsichtlich der Administration reduzieren. Darüber hinaus werden die Qualität der Vergabe und Kontrolle von Berechtigungen erhöht und gleichzeitig Sicherheitsrisiken minimiert. ■

SEBASTIAN SPETHMANN,
Account Manager bei G+H Systems