Administratoren, IT-Systemverantwortliche und IT-Leitungen kennen dieses dumpfe, sorgenvolle Gefühl nur zu gut, wenn es um die Einstellungen und Konfigurationsparameter im **Active Directory** und den **Zugriffsrechten auf den Dateiservern** geht. Mit den Jahren wurden so viele Werte angepasst, Gruppen gebildet, Gruppen geschachtelt und Benutzerrechtezuweisungen vorgenommen, dass an sich niemand mehr ganz genau weiß, ob die entstandene Gesamtkomposition den geltenden Sicherheitsstandards entspricht. So etwas wie eine „TÜV-Prüfung" für Microsoft Domänen existiert ja nicht. Oder womöglich doch!? Es gibt Best Practice-Vorgaben, um Missstände schneller zu erkennen und Möglichkeiten, Compliance-Lücken zu schließen – mit der **Microsoft Edition von daccord**. Hinter daccord steht die G+H Systems, ein bundesweit agierendes Software- und Consulting-Unternehmen mit Sitz in Offenbach am Main.

Die große Mehrheit der IT-Administratoren nutzt zur Verwaltung von Zugriffsberechtigungen und für die Verwaltung von Benutzerkonten den Verzeichnisdienst von Microsoft, das Active Directory. Über die NTFS Zugriffsberechtigungen steuert der Systemverantwortliche, welcher Mitarbeiter Zugriff auf welche Ressourcen hat. Diese Rechtevergabe ist die elementare Basis für die Benutzerverwaltung, und viele Branchenlösungen mit ihrer speziellen Software greifen auf das AD zu. Fehlerhafte Zuweisungen von NTFS-Rechten und falsche Gruppenzugehörigkeiten bieten somit aber auch die Basis für fatale Fehlkonfigurationen, die sich auf den ersten und auch zweiten Blick nicht unbedingt zeigen.

Je größer die Umgebung wird, desto unübersichtlich wird es mit den Standardbordmitteln, die Microsoft dem IT-Verantwortlichen zur Verfügung stellt. Es fehlt die detaillierte, grafische Übersicht, die es dem Administrator erlaubt, die Sicherheitseinstellung schneller und unkomplizierter einzusehen. Eine manuelle Analyse von AD-Objekten und Fileserver-Strukturen ist äußerst zeitaufwendig und birgt zudem ein hohes Fehlerpotenzial.

Exakt an dieser Stelle setzt die daccord Microsoft Edition an und bietet dem Administrator eine ganze Reihe an flexibel einsetzbaren Werkzeugen, um diese Übersicht zu gewinnen und vor allem über beliebig lange Zeiträume festzuhalten, um **Veränderungen nachzuverfolgen**. Die Auswertungen von Verzeichnissen, Ordnern, Dateien und Freigaben sind detailliert und sind das Hauptfunktionsmerkmal der Software. Besonders hervorzuheben ist die spezielle „Effektive-Rechte-Sichtweise", zur zügigen Beantwortung der in der Praxis so häufig gestellten Frage: **Wer darf was?**

Moderne Bereitstellung in kürzester Zeit

Das Thema **Installation und Inbetriebnahme** reduziert sich bei der daccord Microsoft Edition auf wenige Arbeitsschritte, und diese sind komplett Wizard gesteuert. Wer die gut geschriebene und auch auf Deutsch verfügbare Anleitung Schritt für Schritt verfolgt, hat innerhalb weniger Minuten die Einrichtung abgeschlossen. Zunächst einmal entscheidet sich der Administrator entweder für eine Installation unter Linux oder nutzt die Container-Virtualisierung mit Docker, auch unter Windows. Der Docker-Installer in der Desktop-Variante sorgt dafür, dass die erforderlichen Komponenten, beispielsweise Hyper-V, automatisch eingerichtet werden. Docker ist eine Software, mit der sich Anwendungen Container-gestützt virtualisieren und inklusive der benötigten Abhängigkeiten in ein Image packen lassen. Container benötigen weniger Ressourcen als virtuelle Maschinen, da sie auf das Starten eines eigenen Betriebssystems verzichten und stattdessen im Kontext des Host-Betriebssystems laufen. Eine spezielle Engine führt die so verpackte Anwendung in den Docker-Container aus. Dies macht die Bereitstellung der Software äußerst schnell und einfach.

Nach Abschluss der Basiseinrichtung verlaufen die weiteren Schritte identisch. Hierbei gilt es, ganz klassisch, ein Passwort zu vergeben, das EULA abzunicken und festzulegen, ob es sich bei der aktuellen Installation um eine komplett neue daccord Microsoft Edition Konfiguration handelt, oder ob eine bereits bestehende Plattform zu ergänzen ist. Es folgt das Auslesen von Benutzerkontendaten aus dem Active Directory und der Import von Personalstammdaten aus dem HR-System mithilfe eines CSV-Templates. Diese Vorlage hat für den Administrator den großen Vorteil, dass er die möglichen Felder, die die Software für eine Richtlinienprüfung nutzen kann, auf einen Blick erkennt. Praktischerweise muss das Einlesen der Personaldaten nicht im Zuge der Erstkonfiguration vorgenommen werden – diesen Schritt kann der Systemverantwortliche jederzeit nachziehen oder bisher getroffene Entscheidungen anpassen.

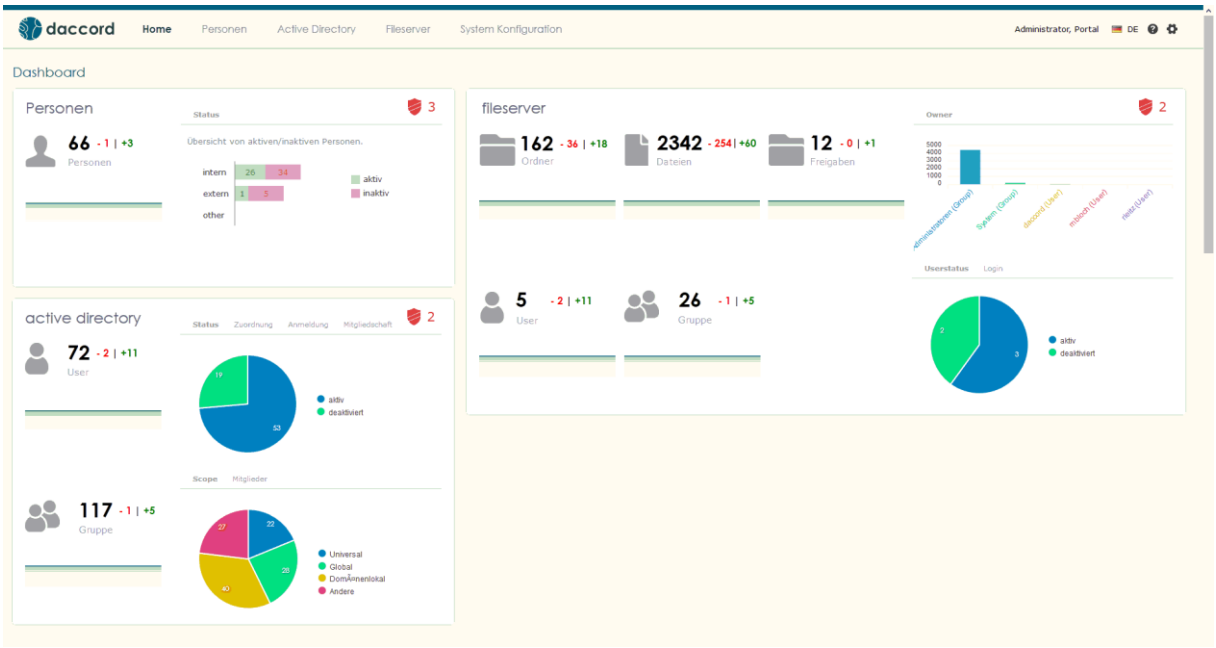
Für beide Abgleichvorgänge kann der Administrator unterschiedliche Intervalle festlegen, bei denen die Daten zu aktualisieren sind. Neben den typischen Scheduler-Werten mit den bekannten Mustern gibt es zudem die Möglichkeit, dies stets manuell vorzunehmen. Bereits während der Ersteinrichtung erkennt der Systemverantwortliche, ob das Einlesen erfolgreich ist. Falls nicht, macht das Programm farblich und per Fehlertext auf sich aufmerksam.

Ein weiterer Einrichtungsschritt betrifft die Windows-Fileserver, bei denen ein oder mehrere Laufwerke gemäß der Berechtigungsvergabe zu prüfen sind. Ehe der Administrator diesen Schritt realisieren kann, gilt es, eine kleine Agent-Software auf einen Dateiserver zu installieren. Während der Einrichtung muss ein Benutzername und Passwort eines Accounts angegeben werden – dieses Konto bedarf des Rechts „Anmeldung als Dienst“. Mithilfe der Anleitung gelingt auch diese Konfiguration ohne Probleme.

Klare Gliederung – einfache Bedienung

Nach Abschluss der Installation zeigt der Wizard die Browser-URL an, unter der das Webfrontend der Software zu erreichen ist. Alle weiteren Schritte bei der Interaktion mit der daccord Microsoft Edition erledigt der Administrator über den Browser. Die typischen Arbeitsschritte sind die Auswertung serverlokaler Benutzerkonten und Gruppen und die Analyse von Active Directory Benutzerkonten, Gruppen, Gruppenmitgliedschaften und -verschachtelungen – und das primäre Einsatzgebiet: Die Auswertung und Übersicht von Zugriffsrechten auf Dateiservern.

Aber nun einmal ganz der Reihe nach: Die Weboberfläche bietet eine ganz klare Struktur mit dem obligatorischen **Dashboard**, in dem alle aktuellen Veränderungen grafisch ansprechend zur Darstellung gebracht werden. Fast alle Objekte sind gleichzeitig ein Link auf eine feinere Darstellung – hier gibt es, in Bezug auf die Bedienung, an sich keine Überraschung. Der Klick auf „System“ führt den Administrator zurück zum „System Gadget“ – der schrittweisen Konfiguration, die schon bei der Einrichtung zur Verfügung stand.



Im Dashboard gewinnt der Administrator den schnellen Überblick über alle Veränderungen in Bezug auf Personendaten, AD-Konten und Fileserverstrukturen. (Bildquelle: G+H Systems GmbH)

Am oberen Fensterrand thront eine Menüleiste mit den Einträgen Personen, Active Directory und Fileserver. Am rechten, oberen Rand entdeckt der Anwender erwartungsgemäß die Menüeinträge zur Änderung des Passworts, zum Wechsel der Oberflächensprache zwischen Englisch und Deutsch und zum Zugriff auf ein weiteres Fenster mit Namen „Systeme“. Von dort aus kann der Administrator beispielsweise das Einlesen von Personendaten außerhalb des Zeitzyklus anstoßen oder weitere Festplatten auf einem Server in die Auswertung einfügen.

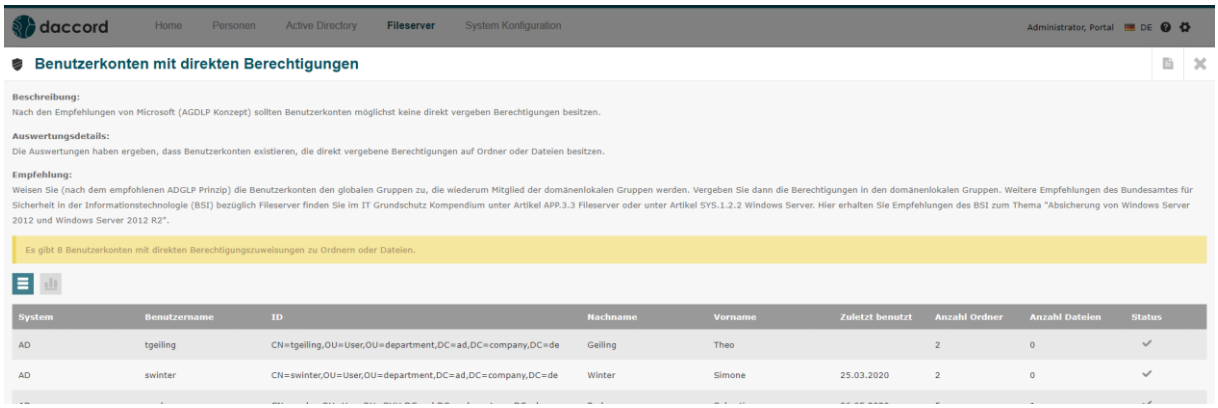
Sicherheit durch Richtlinien

Während der Installation forderte der Wizard zu jedem Hauptpunkt ein entsprechendes **Richtlinienpaket** einzulesen. Die Inhalte findet der IT-Profi auch in einer Komplettübersicht. Einerseits könnte der Anwender eine Richtlinie, beispielsweise dass eine zu hohe Anzahl von aktiven Administrationskonten ein Risiko darstellt, komplett deaktivieren oder die jeweiligen Schwellwerte anpassen. Die mitgelieferten Richtlinien sind keine Eigengewächse aus dem Hause daccord, sondern basieren beispielsweise auf den **Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI)**.

Einen Richtlinieneditor für die Software gibt es nicht. Wohl aber die Möglichkeit, sich individuelle Richtlinienpakete als Dienstleistung vom Hersteller erzeugen zu lassen. Individuelle Anforderungen an die eigenen Compliance-Richtlinien können sich Firmen momentan einkaufen – eine interessante und womöglich einzigartige Dienstleistung. Der Hersteller bereitet zusätzlich vor, einen Policy Builder als Modul zu integrieren, der bei der Einrichtung von kundenspezifischen Policies noch weiter unterstützen soll.

Exemplarisch sei nun auf die Richtlinie „6.2.1 (40000) Benutzerkonten mit direkten Berechtigungen“ eingegangen. In der Beschreibung heißt es hierzu: „Nach den Empfehlungen von Microsoft (AGDLP Konzept) sollten Benutzerkonten möglichst keine direkt vergebenen Berechtigungen besitzen.“ Die Auswertungsdetails geben an: „Die Auswertungen haben ergeben, dass Benutzerkonten existieren, die direkt vergebene Berechtigungen auf Ordner oder Dateien besitzen.“

Findet daccord im Zuge der Untersuchung eine solche Konstellation, werden die entsprechenden Berechtigungen aufgelistet und mit folgender Empfehlung versehen: „Weisen Sie (nach dem empfohlenen AGDLP Prinzip) die Benutzerkonten den globalen Gruppen zu, die wiederum Mitglied der domänenlokalen Gruppen werden. Vergeben Sie dann die Berechtigungen in den domänenlokalen Gruppen. Weitere Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) bezüglich Fileserver finden Sie im IT Grundschutz Kompendium unter Artikel APP.3.3 Fileserver oder unter Artikel SYS.1.2.2 Windows Server. Hier erhalten Sie Empfehlungen des BSI zum Thema ‚Absicherung von Windows Server 2012 und Windows Server 2012 R2‘“.

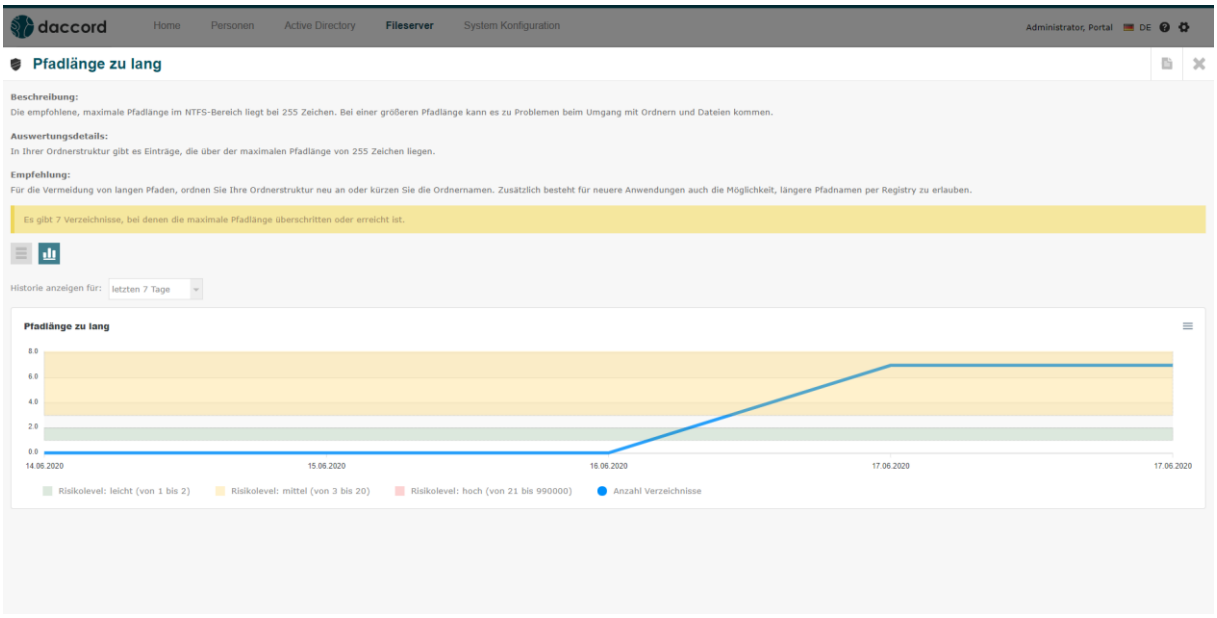


daccord weist nicht nur die potenziellen Sicherheitslücken in der Konfiguration aus, sondern gibt die erforderlichen Hinweise, wie das Problem zu lösen ist. (Bildquelle: G+H Systems GmbH)

Wer als Administrator seine Umgebung mit daccord in der Microsoft Edition prüft, kann binnen kürzester Zeit viele sicherheitsspezifische Anpassungen über die bekannten Windows-Bordmittel vornehmen. Beim nächsten Zyklus wechselt der Report entsprechend, und über die **Historie** sind diese Veränderungen in der daccord-Software dokumentiert.

Beim Abgleich von eingelesenen Personendaten mit dem Active Directory beschränkt sich die Software auf die Nennung des „username“, der in der Import-CSV-Tabelle angegeben ist. Die „Access Governance Edition“ der Software daccord, quasi die größere Variante für den erweiterten Abgleich, bietet hierfür ganze Musterabgleichfunktionen – in der Microsoft Edition ist dies zum jetzigen Zeitpunkt noch nicht umgesetzt. Der Schwerpunkt dieser Edition liegt in der **Visualisierung der Berechtigungen im Active Directory und Filesystem**.

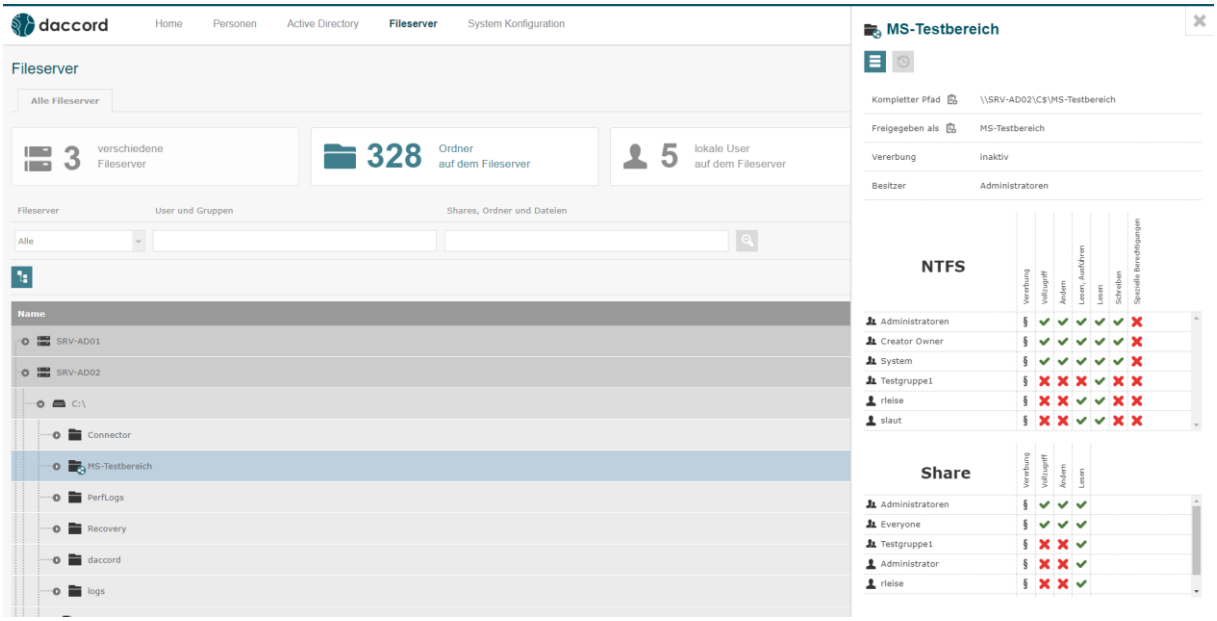
Nur wenige HR-Systeme sind überhaupt in der Lage, einen direkten Abgleich der Personaldaten mit dem Active Directory durchzuführen. Ein Software-Anbieter, der sich auf Personalsysteme spezialisiert hat, kümmert sich in erster Linie um die eigene, spezifische Datenhaltung. Die gern in den Medien propagierten Identity-Management-Verfahren brauchen, um ordnungsgemäß arbeiten zu können, zumindest eine gesicherte Datenquelle und sind somit für die Prüfläufe der IT-Verantwortlichen keine praktische Hilfe. Für die Suche nach verwaisten Benutzerkonten sind die Funktionen der daccord Microsoft Edition ausreichend – das nicht gelöschte Praktikantenkonto dürfte der Vergangenheit angehören.



Die Lösung protokolliert alle Veränderungen mit Zeitstempel, hier exemplarisch die Anzahl zu langer Dateipfade im Windows-Dateisystem. (Bildquelle: G+H Systems GmbH)

Wer sieht und liest was?

Der Dialog „Fileserver“ ist besonders spannend für Administratoren, die sich um die **Prüfung der Zugriffsrechte** Gedanken machen müssen. Letztendlich greift die daccord Microsoft Edition alle Daten ab, die Microsoft Windows in den Dialogen Freigabe und Sicherheit bietet. Wer den in den Tiefen der Microsoft-Fenster zu findenden Abschnitt „Effektive Berechtigung“ kennt, wird sich schon einmal die Frage gestellt haben, warum es dies nicht als Übersichtsfunktion gibt – Benutzername oder Gruppenname eingeben und sich darstellen lassen, welche Dateien oder Ordner mit welchen Rechten sicht- beziehungsweise änderbar sind. Nun – die Suche nach der Funktion hat ein Ende, denn sie steht mit der Microsoft Edition von daccord nun zur Verfügung. Praktischerweise sogar ohne direkten Zugriff auf die Dateiserver selbst, was eine nachträgliche oder dokumentierende Verarbeitung ermöglicht.



Grafische Darstellung der NTFS-Zugriffsrechte im Dateisystem und der Freigabe – bedeutend übersichtlicher als im Windows-Dialog. (Bildquelle: G+H Systems GmbH)

Jedes Element, beispielsweise Ordner oder Datei, wird – nach einem Mausklick – detailliert in einem separaten Fensterbereich dargestellt. Jedoch nicht der Inhalt oder die Größe, sondern die Zugriffsrechte der verschiedenen Personen und Rollen, der Vererbungsstatus und die effektive Berechtigung. Ganz so, wie in den Microsoft-Dialogen – jedoch in „hübsch“ und „übersichtlich“.

Prüfung – das heißt nicht ändern

Die Microsoft Edition von daccord ist ein **Analyse- und Auswertungsprogramm**, das die aus dem AD gesammelten Informationen und die Berechtigungen auf den Fileservern überprüft. Die regelmäßig erzeugten Prüfergebnisse gleicht die Software mit den hinterlegten Compliance-Richtlinien ab und weist die Ergebnisse in der intuitiven Weboberfläche für die IT-Verantwortlichen aus. Etwaige Änderungen indes nehmen Administratoren, Support-Mitarbeiter oder Benutzerdatenverantwortliche mit den ihnen bereits bekannten Programmen oder Microsoft Bordmitteln vor.

Das mag auf den ersten Blick hinderlich wirken, bietet aber auch zwei entscheidende Vorteile. Die daccord-Software greift ausschließlich **lesend** auf die Daten zu und speichert die erfassten Daten in der eigenen Datenbankstruktur ab. Auch ohne einen laufenden Zugriff auf das Netzwerk mit den ADs oder Dateiservern ist eine Abstimmung der Compliance-Regelwerke und eine Auswertung möglich. Faktisch muss der Prüfer über gar keine Berechtigung zur Anpassung verfügen – was wiederum, mit Blick auf die **Compliance-Prüfung**, von Vorteil ist.

Zudem bleiben die etablierten Arbeitsabläufe bei der Benutzeranlage und das Knowhow bezüglich der entsprechenden Werkzeuge unangetastet. Für das Stammpersonal, das Berechtigungen und Zugriffe vergibt, gibt es keine Veränderungen und folglich auch keinen Schulungsaufwand.

Insgesamt können wir der Lösung von daccord bescheinigen, dass die Einarbeitung in das Programm, dank der **Software-Wizards** und der guten Beschriftung der Fensterelemente, wirklich einfach ausfällt. Während viele Programme ein mehrtägiges Training erfordern, um es vollständig einsetzen zu können, ist ein solcher Aufwand bei daccord in der Microsoft Edition nicht erforderlich. Die früheren Fassungen der Software erforderten vom Administrator zumindest einige Installationsschritte unter Linux – das Basissystem von daccord arbeitet mit dem freien Open Source-Betriebssystem.

Fazit

Zur Benutzerkonten- und Rechteprüfung von gewachsenen, großen oder unübersichtlichen Windows-Strukturen ist die Microsoft Edition von daccord bestens gewappnet. Sehr gut gefiel uns die **zügige und unkomplizierte Einrichtung und die klare Gliederung und gute Übersicht**, die die Software dem Administrator bietet. Die laufende Überwachung von Dateiservern und der automatische Abgleich der Active Directories mit Exporten aus Personalwirtschaftssystemen ergeben das erforderliche Werkzeug, um die **Compliance-Einhaltung sicherzustellen**.

Letztendlich sind Nutzer für eine Prüfung mithilfe der Microsoft Edition von daccord nicht mehr auf die Unterstützung eines externen Dienstleisters angewiesen. Dem Auslesen teilweise sehr großer Datenmengen und den damit verbundenen hohen Datenbankanforderungen wird die Software durch die native Nutzung der performanten **Graph-Datenbanken des Herstellers Neo4J** gerecht. Bei Herstellertests konnten hier innerhalb von 12 Minuten 15 Millionen Datensätze ausgelesen, analysiert und verarbeitet werden.

Insbesondere dank der modernen Docker-Container-Struktur ist die daccord Microsoft Edition innerhalb kürzester Zeit installiert, ohne dass an den bestehenden Systemen irgendeine Änderung durchzuführen wäre. Ausgestattet mit der **kostenfreien 7-Tage-Nutzungslizenz** kann sich jeder Interessent problemlos ein eigenes Bild von der Lösung machen. Als Basissystem nutzten wir in unserer Betrachtung, der Empfehlung des Herstellers folgend, ein Windows 10-System mit mehr als 8 GByte RAM und eine aktuelle CPU mit mehr als zwei Cores. Ansonsten steht lediglich Microsoft .Net Framework mindestens Version 4.6.2 auf der Voraussetzungsliste. Setzt die Software auf Linux auf, benötigt der Server 100 GByte Plattenspeicherplatz, zwei CPU-Kerne, 8 GByte RAM und SuSE Linux Enterprise Server 12 SP2, SP3 oder SP4, OpenSuse 15.1 Textversion/Gnome Desktop oder CentOS Linux Release 8.1.1911. Preislich veranschlagt der Hersteller 19,20 Euro einmalig pro aktivem AD-Benutzer und eine 20-prozentige, jährliche Software-Wartung.

In absehbarer Zukunft erweitert der Hersteller die Microsoft Edition noch um weitere Integrationspakete, die den Leistungsumfang noch einmal deutlich erweitern. Aktuell in Planung, so der Anbieter, sind Pakete für das Azure AD mit Office 365, Microsoft Exchange Teams und OneDrive.