Rollen und Rechteverwaltung

Für optimale Arbeitsabläufe in der Apotheke ist eine klare Aufgabenverteilung innerhalb des Teams von großer Bedeutung. Neben persönlichen Vorlieben und Fähigkeiten der Mitarbeiter können auch gesetzliche Vorgaben, wie in Bezug auf Betäubungsmittel oder Datenschutz, eine feste Zuweisung von Rollen und Aufgaben erforderlich machen.
IXOS ermöglicht es Ihnen, jedem Mitarbeiter im Modul **Kontakte** sowohl vordefinierte oder eigens angelegte Rollen, als auch zusätzlich bestimmte Aufgabengebiete zuzuweisen, damit sich die in Ihrer Apotheke gelebte Arbeitsteilung im EDV-System wiederspiegelt. Um sicherzustellen, dass geschützte Funktionen nur von den vorgesehenen Mitarbeitern bedient werden, können Sie dann im Modul **Arbeitsplatzschutz** jeden Arbeitsplatz nach Wunsch individuell gegen unberechtigte Zugriffe sichern.

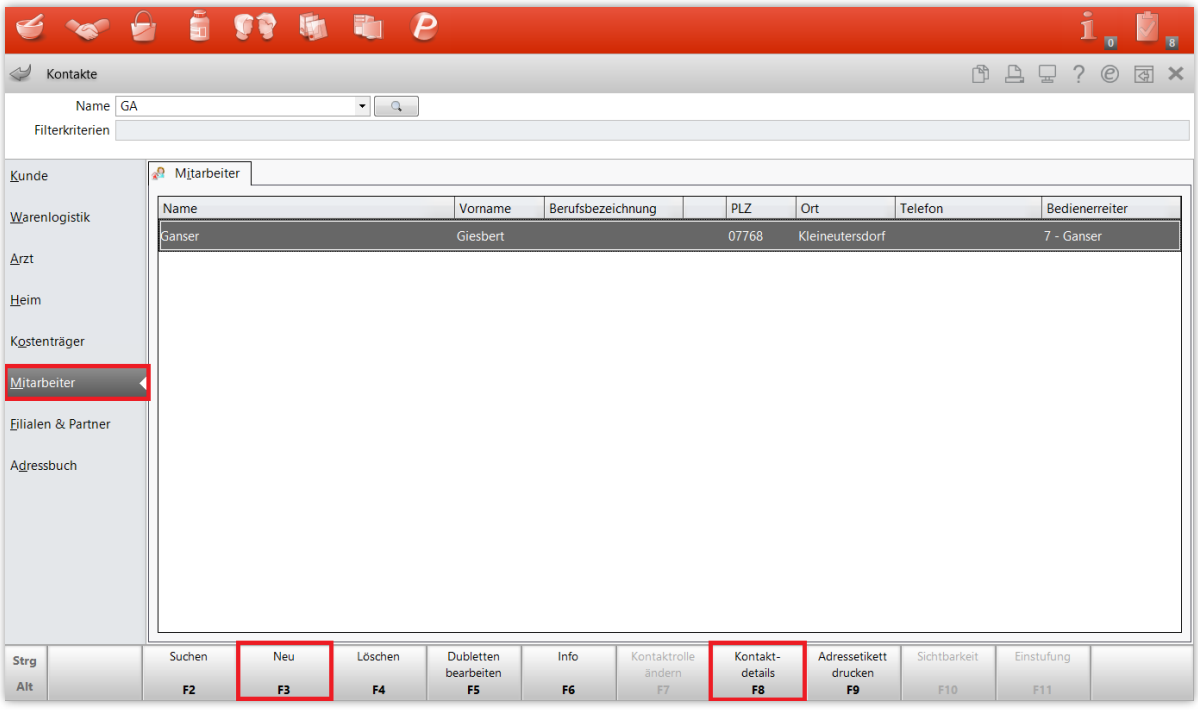
Wie Sie dazu vorgehen können, zeigen wir Ihnen hier.

Zuweisen von Rollen und Berechtigungen

Um das Berechtigungssystem in IXOS sinnvoll zu nutzen, müssen allen aktiven Mitarbeitern (das heißt, allen, die prinzipiell Zugriff auf IXOS haben) geeignete Rollen und / oder Rechte zugeteilt werden.

Um die Benutzerkonten der Mitarbeiter bearbeiten zu können, benötigen Sie die Rolle „Leiter“ oder die Rechte „Benutzerkonto bearbeiten“, „Benutzerkonto bearbeiten und nur Rollen zuweisen“ bzw. „Benutzerkonto bearbeiten und Rechte zuweisen“.

Suchen Sie in den **Kontakten** auf der Seite **Mitarbeiter** den betreffenden Mitarbeiter heraus und öffnen Sie die **Kontaktdetails – F8** – oder legen Sie ihn dort mit **Neu – F3** an, falls es sich um einen neuen Mitarbeiter handelt.

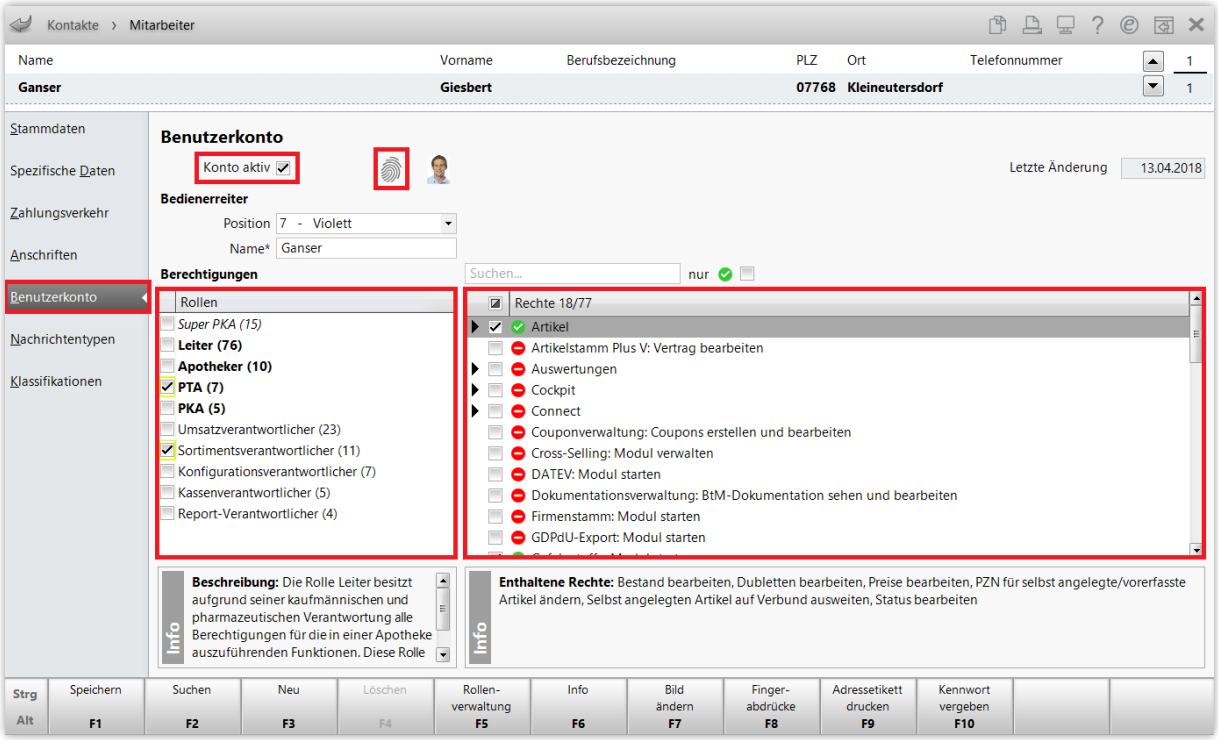


Auf der Seite **Benutzerkonto** können Sie nun das Konto auf aktiv setzen, falls noch nicht geschehen, sowie einen Bedienerreiter zuweisen und die **Rollen** und **Rechte** festlegen.

Wenn Sie das optionale IXOS-Modul **Fingerprint Benutzererkennung** verwenden, können Sie hier über das Fingerabdruck-Symbol auch die Fingerabdrücke des Kollegen hinterlegen. Mit **Fingerprint** lässt sich eine unkomplizierte Benutzerauthentifizierung ganz ohne Kennwörter ermöglichen.

In unserem Beispiel bekommt unser Mitarbeiter Herr Ganser die Rollen **PTA** und **Sortimentsverantwortlicher**. Damit sind dann, wie auf der rechten Seite unter **Rechte** einsehbar, automatisch bestimmte Rechte abgedeckt, die zu den ausgewählten Rollen gehören. Sie können außerdem nach Wunsch weitere Rechte von Hand hinzufügen. Speichern Sie die Einstellungen mit **Speichern – F1**.

Mit **Rollenverwaltung – F5** können Sie die standardmäßig zugehörigen Rechte der einzelnen Rollen nach Wunsch ihren individuellen Arbeitsabläufen anpassen oder auch beliebig neue Rollen definieren.

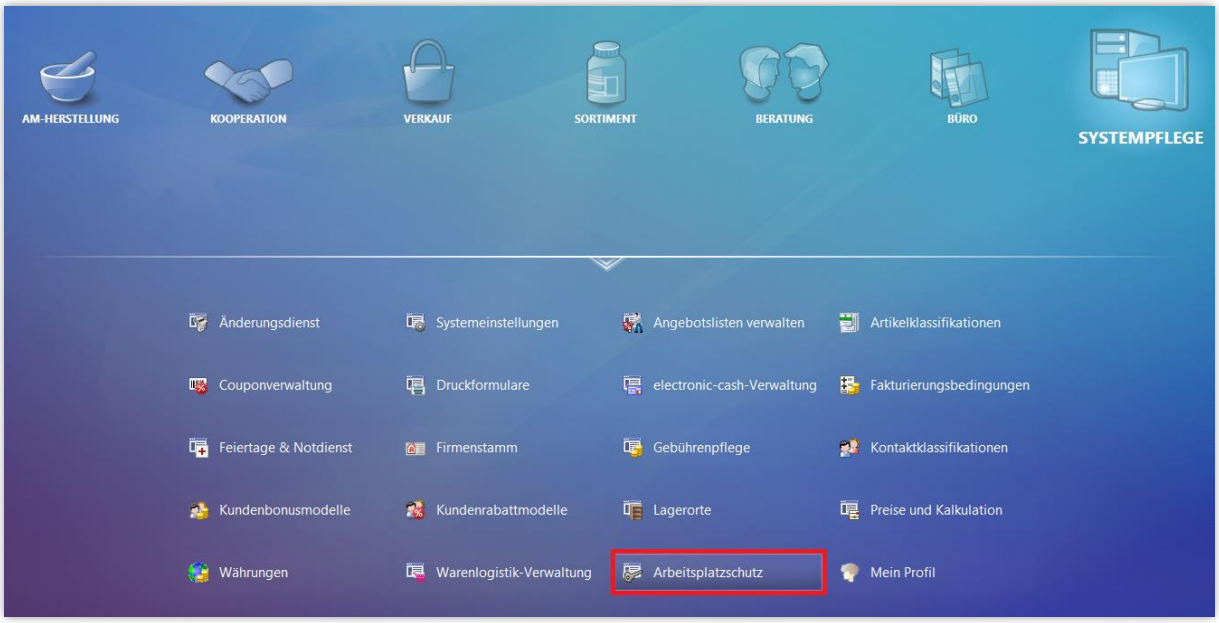


Um nun bestimmte IXOS-Arbeitsplätze vor unerwünschtem Zugriff auf Programmfunktionen zu schützen, müssen Sie ein Berechtigungskonzept im Modul **Arbeitsplatzschutz** auswählen. Erst dann werden die nun zugewiesenen Rollen und Rechte bei der Bedienung von IXOS in Form von Zugriffsbeschränkungen berücksichtigt.

Auswahl und Konfiguration des Berechtigungskonzepts

Sie finden das Modul **Arbeitsplatzschutz** im Menü **Systempflege**.

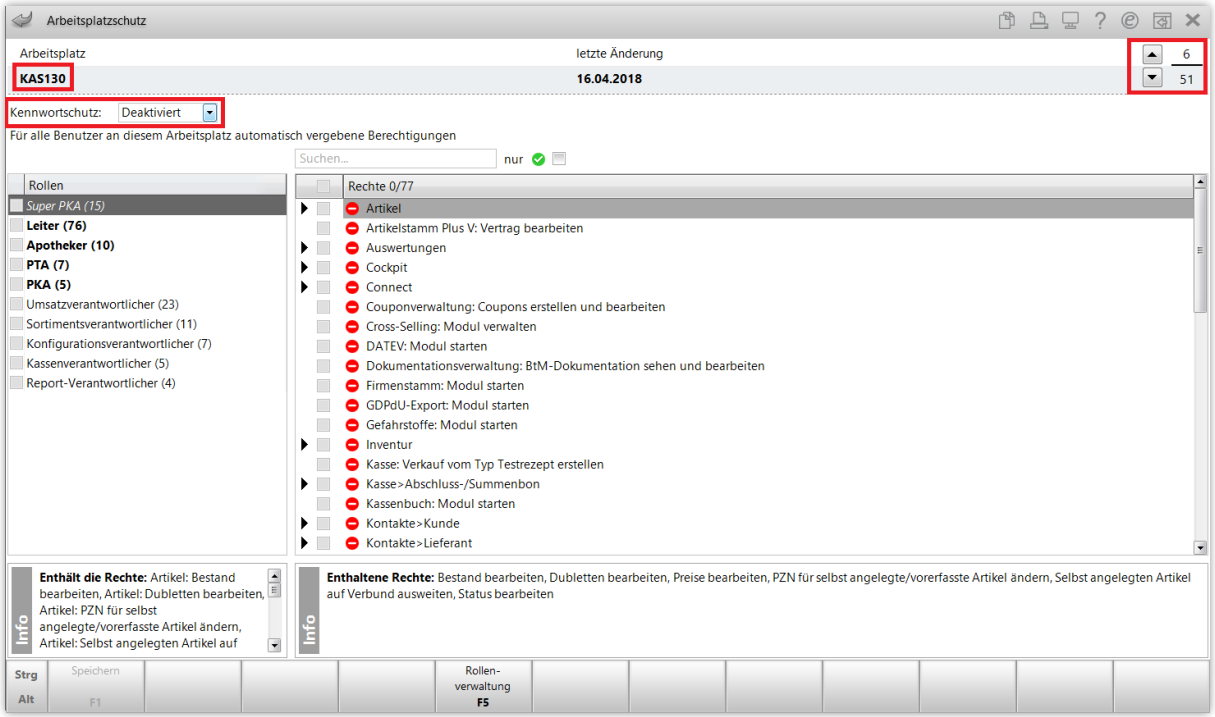
Um das Modul öffnen und bedienen zu können, benötigen Sie die Rolle **Leiter** oder das Recht **Arbeitsplatzschutz**.



Es öffnet sich das Fenster **Arbeitsplatzschutz**. Angezeigt werden zunächst die Einstellungen für den aktuellen Arbeitsplatz (hier KAS130). Mit den Pfeil-Icons ▲ und ▼ oben rechts können Sie die Einstellungen auch für andere Arbeitsplätze tätigen.
Der **Kennwortschutz** ist standardmäßig deaktiviert. Sie können diesen auf „eingeschränkt“ oder „aktiviert“ umschalten.

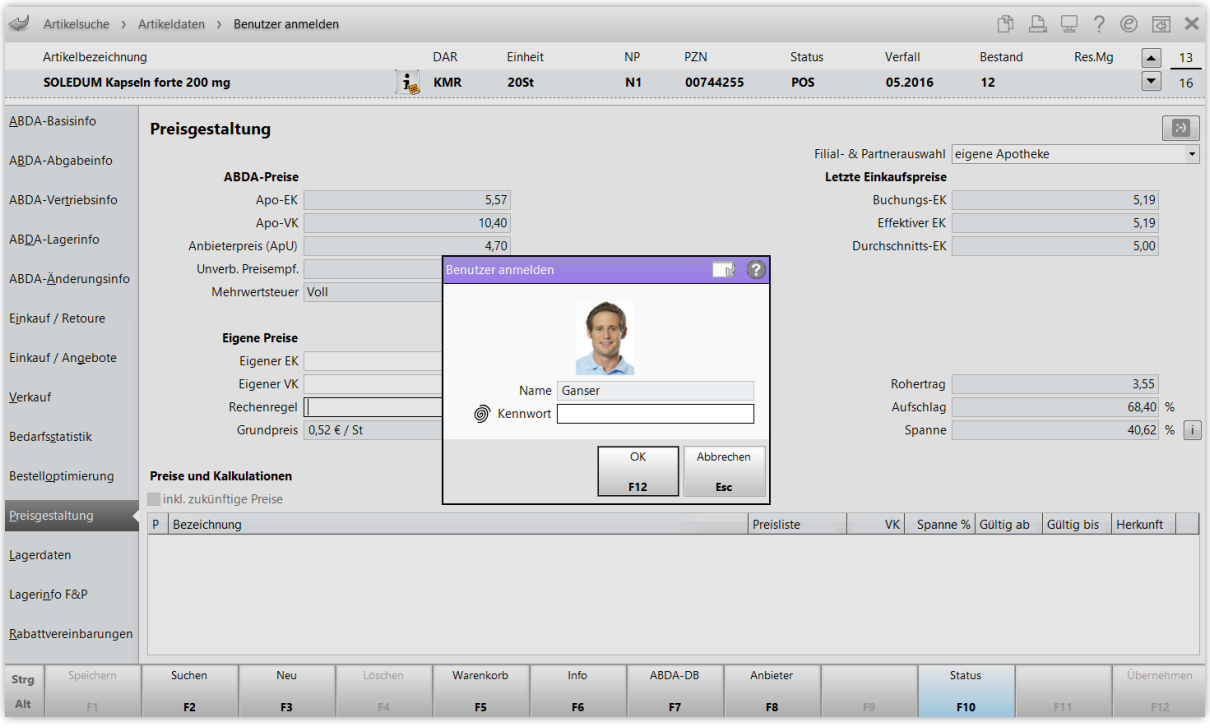
- **Deaktiviert**: An diesem Arbeitsplatz ist jedem Mitarbeiter der Zugriff auf alle Funktionen möglich, mit Ausnahme der Benutzerkonten der Mitarbeiter und des Arbeitsplatzschutzes.
- **Eingeschränkt**: An diesem Arbeitsplatz kann jeder Mitarbeiter auf jeden Bedienerreiter frei zugreifen, aber geschützte Module und Funktionen sind berechtigungsgeschützt. Beim Aufruf solcher Funktionen muss sich der Benutzer mit Kennwort oder Fingerabdruck authentifizieren.
- **Aktiviert**: An diesem Arbeitsplatz muss sich jeder Mitarbeiter an seinem Bedienerreiter authentifizieren, bevor er mit den für ihn zugelassenen Funktionen und Modulen arbeiten kann. Bei einem Bedienerwechsel wird der bisherige Benutzer automatisch gesperrt.

Im mittleren Teil des Fensters können Sie – unabhängig vom Kennwortschutz – Berechtigungen einzeln oder in Form von Rollen **arbeitsplatzspezifisch** erteilen. Diese Rechte gelten dann nur für den betreffenden Arbeitsplatz, aber für alle Benutzer unabhängig von ihren zugewiesenen Rollen und Rechten. So kann man zum Beispiel durch einen Kennwortschutz Zugriff auf umsatzrelevante Daten in der Offizin für nicht berechtigte Personen verhindern, aber gleichzeitig die Rolle „Leiter“ oder „Umsatzverantwortlicher“ für den Bürocomputer freischalten, um die häufige Kennwort- oder Fingerabdruck-Nachfrage zu vermeiden.

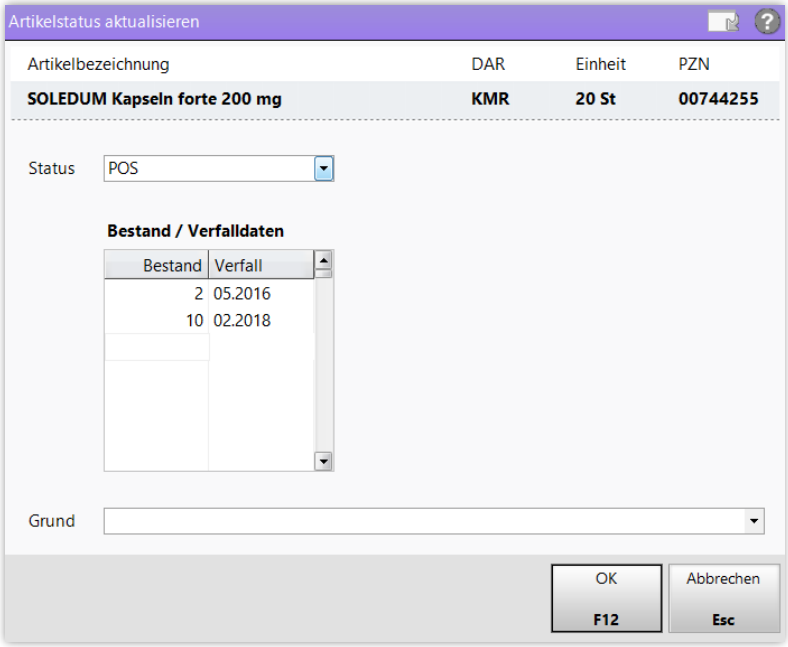


In unserem Beispiel setzen wir den Kennwortschutz auf **Eingeschränkt** und übernehmen die Einstellung mit **Speichern – F1**.

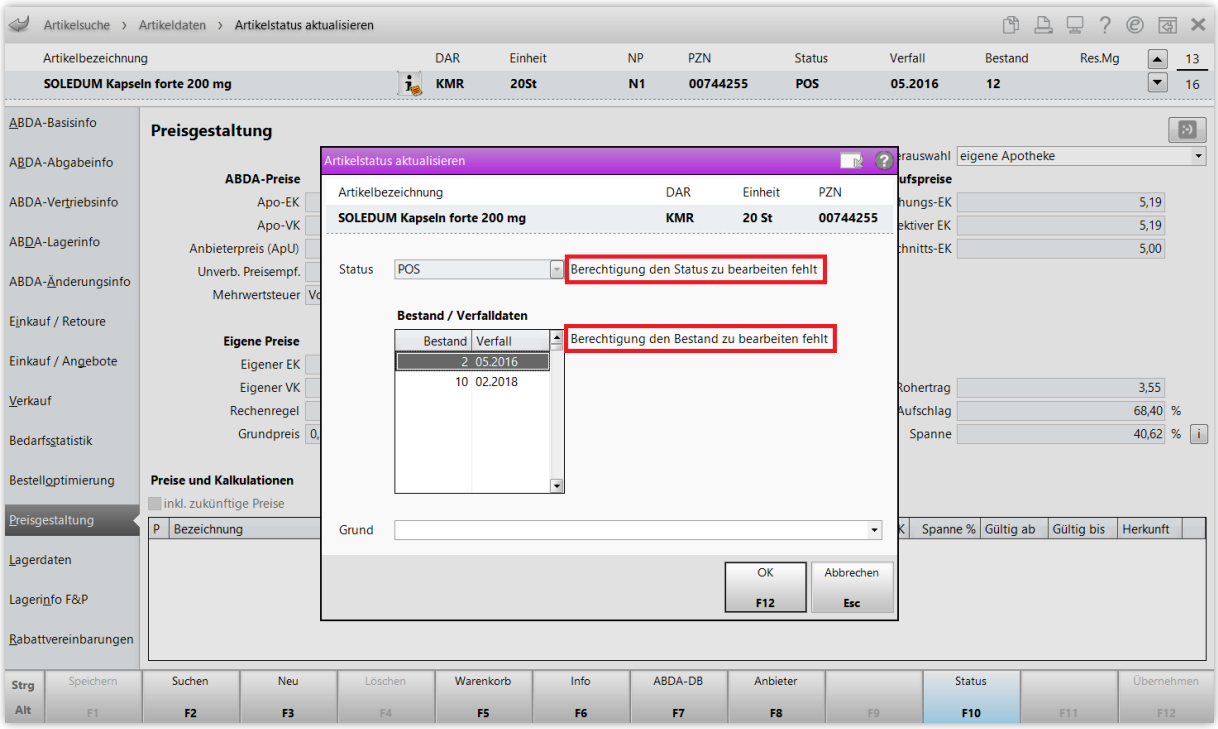
Nun kann neben dem Apothekenleiter nur noch unser Sortimentsverantwortlicher Herr Ganser in den Artikeldaten mit **Status – F10** einen Bestand eines Artikels ändern. Da diese Funktion eine geschützte Funktion ist (also aufgrund der Rollen- und Rechteverwaltung nicht allen Mitarbeitern offensteht), erscheint an dieser Stelle nun eine Kennwortabfrage.



Nach Eingabe seines Kennworts oder Abscannen des Fingerabdrucks kann Herr Ganser nun als berechtigte Person Änderungen am Artikelstatus vornehmen.



Wenn nun ein anderer Kollege in den Artikeldaten **Status – F10** aufruft, wird ihm zwar der Status und Bestand des Artikels angezeigt, aber anders als Herr Ganser kann er den Bestand nicht bearbeiten, weil ihm das Recht „Status bearbeiten“ fehlt.



So können Sie sensible Daten und Funktionen Ihres IXOS-Systems vor versehentlichen Fehlbedienungen und unerwünschten Zugriffen – auch von Nicht-Mitarbeitern – schützen und für mehr Sicherheit im Arbeitsalltag sorgen.