Rollen im Fokus: Die Vorteile von Role-Based Access Control (RBAC)

MATESO
PASSWORD SAFE

Vorwort

Rechte zu definieren und zu gewähren, kann IT-Teams vor diverse Herausforderungen stellen. Kommen etwa neue Mitarbeitende ins Unternehmen, sollen sie so schnell wie möglich Zugriff auf alle für ihre Arbeit notwendigen Zugänge erhalten. Auch sollte der fortlaufende Betrieb durch unnötige Einschränkungen nicht gestört werden.

Wiederum dürfen Mitarbeitende nicht zu weit gefasste Rechte oder zu lange Zugriff auf Zugänge erhalten, um das Angriffspotential so gering wie möglich zu halten. Denn in digitalen Zeiten ist es wichtiger denn je, Berechtigungen auf Datenzugriffe so niedrig wie möglich zu halten. Dem Least-Knowledge-Prinzip entsprechend sollte ein Benutzer deshalb nur mit den minimal notwendigen Rechten zur Durchführung seiner Aufgaben ausgestattet werden.

Die rollenbasierte Zugriffskontrolle (RBAC) ist deshalb eine beliebte Methodik zur Berechtigungsvergabe in der IT-Infrastruktur von Unternehmen geworden. Obwohl die Wichtigkeit von RBAC in Unternehmen immer mehr an Bedeutung gewinnt, schrecken viele doch noch vor deren Umsetzung zurück – oft aus Sorge vor einer aufwändigen und komplexen Implementierung.

Dieses Whitepaper klärt deshalb über die verschiedenen Berechtigungsmodelle im Vergleich zu RBAC sowie dessen Vorteile und Anwendungsgebiete im Password Management auf und gibt wertvolle Tipps für die praktische Umsetzung mit Password Safe in Organisationen.

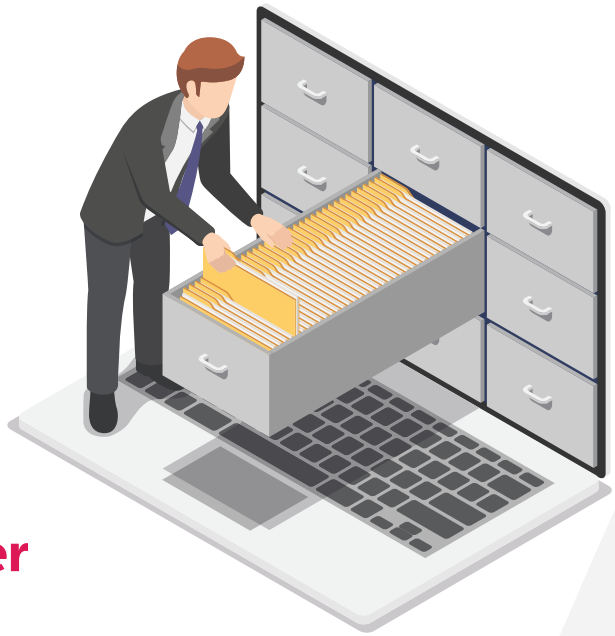
„Welche Rechte soll die Rolle besitzen? Und wem soll diese zugeteilt werden?"

Verliert ein Unternehmen den Überblick über Datenzugriffe, setzt es sich nur unnötigen Gefahren aus, die im Vorfeld durch ein professionelles Berechtigungsmanagement verhindert hätten werden können.

Ausgangssituation

Herrscht in Unternehmen kein ganzheitliches Konzept zum Gewähren von Zugriffsrechten auf Daten und Dienste, entstehen diverse Risiken und Probleme für diese. Jeden Mitarbeitenden einzeln zu berechtigen, ist einerseits enorm zeitaufwendig für die IT. Auch steigt dabei das Risiko von Überberechtigungen oder dass Nutzerrechte nach Gebrauch nicht wieder entzogen werden und somit überflüssige Rechte entstehen, die zu Rechteansammlungen führen.

Fehlen zudem die Möglichkeiten, die Rechtevergabe zu protokollieren und nachverfolgen zu können, entsteht ein zusätzliches Risiko unerlaubter Zugriffe. Bei der Entscheidung für ein professionelles Berechtigungsmanagement können Unternehmen auf diverse Prinzipien zurückgreifen. Die wichtigsten drei Modelle werden im Folgenden vorgestellt und erläutert.



Vorstellung verschiedener Berechtigungsmodelle

Identity Based Access Control (IBAC)

Bei der identitätsbasierten Zugriffskontrolle (Identity Based Access Control: IBAC) werden die Zugriffsrechte direkt auf die Identität des Subjekts bezogen definiert, was diesen Ansatz in der Anwendung sehr leicht verständlich macht. Doch gerade für große und stark vernetzte Unternehmensarchitekturen bietet sich diese Methode eher weniger an, da bei steigenden Benutzerzahlen schwer skaliert werden kann und die Identität des Benutzers nicht mit dessen Position oder Funktionalität zusammenhängt.

Dies führt dazu, dass leicht der Überblick über Berechtigungen verloren werden kann. Im Falle eines Abteilungs- oder Positionswechsels, bei der dem Benutzer neue Tätigkeiten und auch Zugänge zugeteilt werden, müssten auch alle damit verbundenen Zugriffe separat geändert werden, was enorm zeitaufwändig wäre. Hinzu kommt, dass das Risiko von Fehl- und Überberechtigungen steigt, da nicht gewährleistet werden kann, dass der Benutzer auch nur genau die Rechte erhält, die er für seine Arbeit benötigt.

Atribute Based Access Control (ABAC)

Bei der attributbasierten Zugriffskontrolle (Atribute Based Access Control: ABAC) werden Attribute (Merkmale) und nicht Rollen zur Vergabe von Zugriffsrechten verwendet. ABAC ist eine Unterkategorie von RBAC, die dadurch eine noch detailliertere Rechtevergabe ermöglicht. Bei ABAC werden spezifische Merkmale geprüft, um daraufhin eine Zugriffsentscheidung zu treffen. Merkmale können dabei bezogen auf die Person (Benutzername, ID, Alter, ...), Ressourcen (Worauf soll zugegriffen werden?), Aktionen (Lesen, Verschieben, Bearbeiten, Löschen, ...) oder die Umgebung (Ort, Zeit, Gerät, ...) sein.

Aus diesen Merkmalen werden Regeln abgeleitet, die definieren, welche von ihnen erfüllt sein müssen, um einen Zugriff entweder zu genehmigen oder zu verweigern. So könnte etwa der Zugriff auf bestimmte Daten außerhalb der Geschäftszeiten und ohne Firmenstandort unterbunden werden. Im Vergleich zu RBAC ist dieser Ansatz also dynamischer und bietet noch mehr Möglichkeiten zur Rechtevergabe. Andererseits ist die Implementierung und Pflege von ABAC aufgrund dieser auch um einiges aufwendiger: Alle notwendigen Richtlinien zu definieren, kann für die IT die Prüfung und Definition mehrerer Tausende Merkmale bedeuten.

Role Based Access Control (RBAC)

Rollen stellen den Dreh- und Angelpunkt zwischen IT und Business in Unternehmen dar, weshalb die Organisation dieser enge Zusammenarbeit und auch vorhergehende Planung erfordert. Ziel sollte immer sein, Rollen verständlich und transparent zu definieren und ihre Anzahl überschaubar zu halten.

Durch das rollenbasierte Berechtigungsmanagement (Role Based Access Control: RBAC) werden Zugriffsrechte auf Daten und Dienste nicht einzeln direkt auf den Benutzer, sondern anhand der zugewiesenen Rolle gewährt und entzogen – dem Least-Privilege-Prinzip entsprechend. Ein Benutzer kann dabei mehreren Benutzerrollen zugewiesen sein. Häufige Berechtigungen auf Daten nach RBAC sind “Lesen”, “Schreiben” und “Löschen”. Auch Microsoft und Oracle Solaris bauen auf dem RBAC-Prinzip, zum Beispiel für die Berechtigungen über AD-Gruppen auf File Server Ressourcen.

Definition einer Rolle

In Unternehmen hat jeder Mitarbeitende eine spezielle Funktion inne, die durch seine Position widergespiegelt wird und ist einer Abteilung, einem Standort oder auch einer Kostenstelle zugeteilt. Wird der Mitarbeitende nun nach diesen Kriterien einer Rolle zugeteilt, erhält er automatisch auch die jeweiligen Berechtigungen auf Daten, die diese Rolle benötigt. So können Rollen die komplette Hierarchie eines Unternehmens durch das Rollenkonzept detailgetreu abbilden.

“Nach dem Least Knowledge Prinzip haben Mitarbeitende ihrer Rolle entsprechend nur die Berechtigung auf den Datensatz, die sie zum Arbeiten auch benötigen – und das jeweils auch nur für den benötigten Zeitraum.”

Technisch gesehen bildet eine Rolle also nichts anderes als mehrere Benutzer mit denselben Berechtigungen ab. Es kann beispielsweise die Rolle “Administration” mit weitläufigen Berechtigungen oder auch die Rolle “Marketingassistenz” mit auf die Abteilung und Funktion begrenzten Berechtigungen erstellt werden. Durch die Arbeit mit Rollen müssen Mitarbeitende nicht mehr einzeln berechtigt werden, sondern werden einfacher ihrer entsprechenden Rolle zugeteilt.

Bei Berechtigungen nach RBAC werden nicht die direkten Berechtigungen auf jeden einzelnen Datensatz, sondern nur noch über Rollenmitgliedschaften verwaltet.

NIST-Empfehlung zur Rollendefinition: 4 Ebenen

1. **Flach:** Durch die Zuweisung zu einer Rolle erhalten Benutzer direkt die damit verbundenen Rechte. So kann ein Benutzer Mitglied mehrere Rollen sein und eine Rolle kann mehrere Benutzer beinhalten.

   Beispiel: Die Rolle “IT” wird allen Benutzern zugewiesen, die administrative Rechte benötigen.

2. **Hierarchisch:** Durch Einfügen von Ebenen können Rollen in Relation zueinander gesetzt und damit einhergehend Regeln definiert werden, wie Berechtigungen vererbt werden. In Password Safe wird dies anhand von Organisationseinheiten abgebildet.

   Beispiel: Der Gruppe “Inside Sales Manager” werden im Active Directory Rechte aus der Organisationseinheit “Sales” vererbt, der sie untergeordnet ist.

3. **Eingeschränkt:** Je nach zugewiesener Rolle können Aktionen von Benutzern beschränkt werden. In Password Safe wird dies durch restriktive Benutzer oder zusätzliche Schutzmechanismen wie das Mehr-Augen-Prinzip, temporäre Freigabebegrenzungen oder den Sichtschutz abgebildet.

   Beispiel: Ein Benutzer kann durch die ihm zugewiesene Rolle Passwörter nur zum Login nutzen, aber nicht aufdecken.

4. **Symmetrisch:** Unabhängig von weiteren Faktoren bleibt die Berechtigung der Rolle konstant gleich, um den Standard einzuhalten.

   Beispiel: Die Rolle “Regional Sales Manager” hat die gleichen Berechtigungen auf Zugangsdaten unabhängig von ihrem Einsatzort.

Vorteile mit RBAC

Im Weiteren wird darauf eingegangen, welche Vorteile in Bezug auf Sicherheit, Effizienz und Transparenz das RBAC-Modell bietet

Einfache und flexible Verwaltung

Die Zusammenarbeit in Unternehmen wird immer agiler. Über Abteilungen hinweg entstehen flexible Projekt-Teams zur Zusammenarbeit. Mitarbeiter kommen kurzfristig hinzu, treten parallel anderen Teams bei und neue temporäre Gruppen entstehen. Dazu kommt, dass die Mitarbeiterfluktuation zugenommen hat: Mitarbeitende wechseln schneller und häufiger ihre Jobs und Arbeitgeber.

Dies macht es umso wichtiger, einen Überblick darüber zu behalten, wer wann worauf berechtigt ist und auch immer wieder die Berechtigungen auf dem aktuellen Stand zu halten, sodass ehemalige Mitarbeiter effektiv ausgeschlossen werden und keinen Datenzugriff mehr besitzen.

Durch RBAC können Unternehmen flexibler auf Mitarbeiterwechsel und -änderungen nach dem Prozess für Joiner, Mover Leaver (JML) reagieren. Denn gerade, wenn Mitarbeitende hinzukommen, die Abteilung wechseln oder das Unternehmen verlassen, erleichtert RBAC die Arbeit enorm und macht sie sicherer. Dabei können Rechte über Rollenmitgliedschaften jederzeit gewährt und entzogen, von vornherein nur temporär festgelegt oder Zugangsdaten mit Ablaufdatum versehen werden, was RBAC sehr anpassungsfähig und dynamisch gestaltet.

Role-Based Access Control macht zudem die aufwendige Vergabe von Einzelberechtigungen hinfällig, indem einmalig Berechtigungen auf Rollen vordefiniert und in einem Schwung auch auf mehrere Personen ausgerollt oder wieder entzogen werden können. Werden die Rollen leicht verständlich benannt, stärkt dies zudem die Transparenz und Nachvollziehbarkeit auf der Anwenderseite.

Joiner: Mitarbeitende kommen neu hinzu

Ein neuer Mitarbeiter erhält über seine Rolle Berechtigungen auf über 1.000 Passwörter. Mit RBAC müssen nicht mehr die Berechtigungen von 1.000 Passwörtern einzeln berechtigt werden, da nur noch eine Rollenmitgliedschaft bearbeitet wird. Die Berechtigungen sind schon vordefiniert und müssen nur noch dem aktuellen Bedarf angepasst werden.

Mover: Mitarbeitende wechseln die Abteilung

Dem Mitarbeitenden wird einfach die alte Rolle entzogen und er wird der neuen Rolle hinzugefügt. Für eine temporäre Übergangsphase – beispielsweise, wenn er seinen Nachfolger noch einlernt, können beide Rollen auch parallel beibehalten werden, bis der Onboarding-Prozess abgeschlossen ist. Dies sorgt für einen fließenden und sicherer Übergang der Zugangsdaten.

Leaver: Mitarbeitende verlassen das Unternehmen

Verlässt ein Mitarbeitender das Unternehmen, wird er nur aus der Rolle entfernt und hat auf einen Schlag auf keines seiner 1.000 Passwörter mehr Berechtigungen oder Zugriff. Es bleiben also keine unaufgelösten User IDs zurück. Dies betrifft nicht nur ehemalige Mitarbeitende, sondern auch die Zusammenarbeit mit Externen oder Mitarbeitende, die in Elternzeit gehen oder ein Sabbatical einlegen.

Azubi-Effekt auflösen

Als Azubi-Effekt wird das Phänomen beschrieben, dass Auszubildende während ihrer Ausbildung verschiedene Abteilungen im Unternehmen durchlaufen und hierfür die jeweiligen Zugriffsrechte erhalten, die nach einem Abteilungswechsel nicht wieder entzogen werden. Somit verfügen die ausgelernten Mitarbeitenden über immer mehr Zugriffsrechte auf Firmendaten – selbst, wenn sie das Unternehmen schon verlassen haben. Dieser Effekt kann nicht nur bei Auszubildenden, sondern generell bei einem Mitarbeiterwechsel auftreten – etwa bei einer Beförderung oder einem Filialwechsel.

Durch temporäre Mitgliedschaft in einer Rolle und eine generelle temporäre Befristung von Berechtigungen, die nicht von Dauer sind, kann RBAC dafür sorgen, dass dem Azubi-Effekt vorgebeugt und dieser sogar aufgelöst wird.

Gesteigerte Sicherheit und Effizienz

Die Vergabe von Einzelberechtigungen ohne RBAC ist nicht nur zeitaufwendiger. Sie bedeutet auch weniger Kontrolle und Übersicht darüber, wer worauf Zugriff hat. Zudem bietet sie Raum für Fehler und Überberechtigungen. So können Sicherheitslücken entstehen, wenn die Einzelberechtigungen nicht mehr entzogen oder länger als nötig erhalten werden. Erhalten Nutzer zu viele Rechte, können dadurch Fehler entstehen, die im Vorfeld ohne die einzeln gewährten Rechte gar nicht erst entstanden wären.

Bei einem vorab durchdachten und vordefinierten Berechtigungskonzept spart sich das Unternehmen nicht nur Arbeit, sondern ist auch auf der sicheren Seite: Die Zugriffsrechte sind ausschließlich über das Rollenkonzept definiert. Überberechtigungen einzelner Mitarbeiter werden somit nach dem Principle of Least Privilege (PoLP) vermieden, um auch Compliance-Anforderungen gerecht zu werden. Auch Einzelberechtigungen, die fehleranfällig und unübersichtlich sind, werden dadurch bestmöglich ausgeschlossen.

So unterstützt RBAC dabei, die Effizienz und Sicherheit in der IT sowie im gesamten Unternehmen merklich zu steigern. Änderungen erfolgen automatisch, Rechte müssen nicht mehr individuell beantragt und vergeben werden und auch die Wartezeit auf die Genehmigung dieser entfällt. Die Verwaltung von Zugriffsrechten gestaltet sich dadurch nicht nur einfacher, sondern auch und vor allem fehlerresistenter.

Verteilte Verantwortlichkeiten

Um auf der einen Seite Benutzer zu entlasten und auf der anderen Ressourcen zu sparen, können Verantwortlichkeiten durch das RBAC-Konzept umgeschichtet werden, um reale Prozesse aus der Arbeitswelt auch digital abbilden zu können. Die Vorteile dieser verteilten Verantwortlichkeiten werden anhand von Praxisbeispielen verdeutlicht.

Genehmigung von Prozessen

Nach dem Vier-Augen-Prinzip müssen bestimmte Abläufe oder Entscheidungen von mehr als einer Person kontrolliert werden. In der Praxis kann dies im Sinne der Funktionstrennung (Segregation of Duties – SOD) bedeuten, dass Geld etwa nur in Anwesenheit einer zusätzlichen Person gezählt werden darf oder Bestellungen nicht von der gleichen Person genehmigt werden dürfen, die diese eingereicht hat.

Mit RBAC kann dieser Prozess dargestellt werden, indem eine weitere Rolle den Zugriff auf Zugangsdaten genehmigen muss. In Password Safe wird dies durch die Funktion “Mehr-Augen-Prinzip durch Siegel” abgebildet, durch das genau festgelegt werden kann, wie viele und welche Rolle/n zur Genehmigung erforderlich sind und welche Rolle eine Genehmigung überhaupt beantragen darf.

Delegation von Rechten

Ein Kassierer sollte nicht seine eigene Kasse prüfen. Durch RBAC wird dieses Prinzip dadurch abgebildet, dass die Rolle “Administrator” beispielsweise andere Benutzer auf Datensätze berechtigen kann, ohne diese aber selbst einsehen zu können. Dies entlastet auch die IT durch Unkenntnis bei einem potentiellen Verdachtsfall.

Weitergabe von Rechten

Im Fall von Krankheit oder Urlaub wird eine Vertretung für den Mitarbeitenden genannt, die stellvertretend für ihn Prozesse genehmigen und auf Daten zugreifen kann. Dadurch, dass bei RBAC mehrere Personen Mitglied einer Rolle sein können, ist der Zugriff auf Daten unabhängig von der Abwesenheit einer Person gegeben und der weitere Betrieb wird nicht durch fehlende Rechte aufgehalten. Zudem können Rechte nur temporär fur einen bestimmten Zeitraum gewährt werden.

Alle Vorteile auf einen Blick: IT und Unternehmensstruktur clever kombiniert

- granularer Zugriff auf Daten ohne Erhöhung der Komplexität
- bessere Organisation und Übersicht aller Zugriffsprofile mit weniger Verwaltungsaufwand und Fehleranfälligkeit
- einfacheres On- und Offboarding von Mitarbeitenden sowie Abteilungswechsel
- keine Betriebsunterbrechungen: Mitarbeitende verfügen schon im Vorfeld über alle erforderlichen Rechte
- weniger Angriffspotential von innen und außen durch Ausschluss von Überberechtigungen
- mehr Transparenz und Nachvollziehbarkeit zur Bedienung sowie für Auditssogar aufgelöst wird.

Implementierung

Um das Berechtigungsprinzip nach RBAC bestmöglich anzuwenden und den Aufwand auch langfristig so gering wie möglich zu halten, sind im Vorfeld sicherheitstechnische Vorkehrungen zu treffen. Deshalb wird für die effektive Umsetzung von RBAC am Beispiel von Password Safe geraten, in den folgenden drei Schritten vorzugehen:

1. IST-Abgleich: Anforderungseinschätzung

Zunächst sollte eine Liste aller Zugangsdaten (Konten, Websites, Anwendungen, Tools, Programme) erstellt werden. Daraufhin wird sich ein Überblick darüber verschafft, welche Personen welche Zugriffsrechte darauf besitzen. So erfolgt ein IST-Abgleich, wer gegenwärtig Zugriff zu diesen Zugangsdaten hat, um sich einen aktuellen Stand über die Sicherheitslage zu verschaffen.

Berechtigungsanalyse

- Worauf haben einzelne Mitarbeitende Zugriff?
- Wie sind diese Berechtigungen zustande gekommen?
- Wie sind die Berechtigungen für einen einzelnen Benutzer aufgebaut?

2. SOLL-Abgleich: Rollen und Organisationseinheiten anlegen

Nun erfolgt der SOLL-Abgleich, wer im Unternehmen auf diese Zugangsdaten Zugriff haben sollte. Dazu werden Organisationseinheiten definiert, die die Struktur und Hierarchie des Unternehmens wie ein Organigramm widerspiegeln. Nun können AD-Benutzer und Gruppen importiert werden und diese auf Objekte berechtigt werden. Die Gruppen werden dabei zu Rollen. Existiert noch kein derartiger Verzeichnisdienst, müssen die Rollen manuell festgelegt werden.

Rollen können dabei global gedacht oder auf spezifische Organisationseinheiten angewandt werden. Dieses vorab durchdachte und vordefinierte Berechtigungskonzept spart nicht nur enorm Zeit, sondern ist auch viel sicherer: Es kommt zu keinen Überberechtigungen einzelner Mitarbeiter, weil das Berechtigungskonzept nach dem Principle of Least Knowledge aufgebaut ist.

Damit RBAC auch wirklich alle Funktionen in Organisationen korrekt abbilden kann, sollten alle Abteilungen darin eingebunden werden. Für ein nachhaltiges Berechtigungsmanagement, das auch in der Zukunft im Unternehmen Bestand hat, können Rollen schon “vorgedacht” werden, die noch nicht existieren wie etwa Auszubildende mit eingeschränkten Rechten oder Audit-Beauftragte mit umfassenden Leserechten.

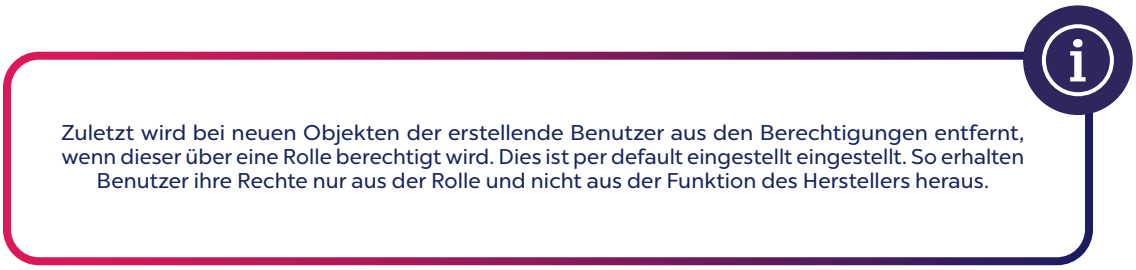
Berechtigungen anlegen

Abschließend wird jeder Benutzer, seiner Funktion entsprechend, mindestens einer Rolle zugeteilt. Die Zuordnung erfolgt nach dem Least-Privilege-Prinzip. Dazu wird bestimmt, auf welche Ressourcen diese zugreifen müssen, um ihre tägliche Arbeit erledigen zu können.

1. Rechte vordefinieren

Da es sehr zeitintensiv ist, jeden Datensatz einzeln zu berechtigen, empfiehlt es sich, im Vorfeld möglichst alle Rechte vorzudefinieren. Dazu wird definiert, welche Arten von Zugriffsrechten benötigt werden – sei es “Lesen”, “Schreiben”, “Verschieben” oder selbst das “Berechtigen” von Zugangsdaten.

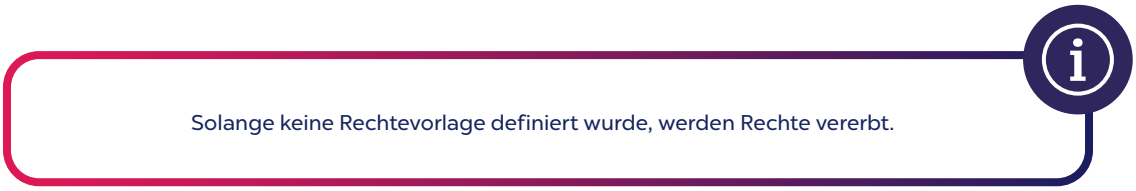
Durch diverse Automatismen wird die Vergabe von Berechtigungen dabei immens erleichtert. Auch sollten die Berechtigungen schon im Vorfeld so schmal wie möglich gehalten werden. Ein Abteilungsleiter sollte etwa nur die Rechte “Lesen” und “Hinzufügen” auf eine Organisationseinheit erhalten, aber keine Unterorganisationseinheiten oder Benutzer hinzufügen können.



Zuletzt wird bei neuen Objekten der erstellende Benutzer aus den Berechtigungen entfernt, wenn dieser über eine Rolle berechtigt wird. Dies ist per default eingestellt eingestellt. So erhalten Benutzer ihre Rechte nur aus der Rolle und nicht aus der Funktion des Herstellers heraus.

2. Rechte vererben

Rechtesets können auch aus Organisationsstrukturen vererbt werden: Wird ein neuer Datensatz in einer Organisationseinheit erstellt, erhält dieser auch automatisch die darin definierten Berechtigungen. Hier besteht jedoch die Gefahr, dass ein Mitarbeitender auch die Organisationseinheit löschen könnte, wollte man das Löschen-Recht vererben wollen. Deshalb bietet sich eher die Nutzung von Rechtevorlagen an.

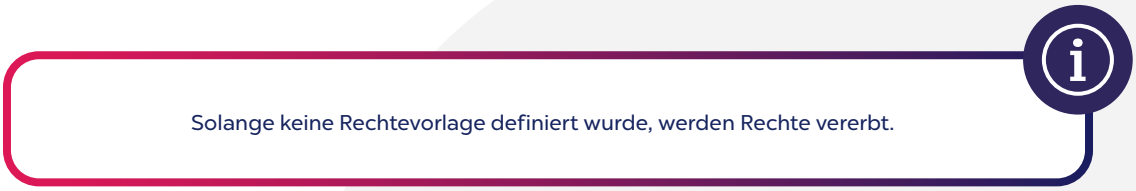


Solange keine Rechtevorlage definiert wurde, werden Rechte vererbt.

3. Rechtevorlagen nutzen

Um die Arbeit mit RBAC effizient zu gestalten, empfiehlt es sich, auf Vorlagen zur Rechtevergabe zurückzugreifen. Eine Rechtevorlage bildet die typischen Aufgaben einer Rolle in einer Organisationseinheit durch ein vorab zusammengestelltes Berechtigungsset ab. So können Rollen auch konzeptionell berechtigt werden, beispielsweise die Rolle “Auszubildender” oder “Infrastrukturmanagement”. Wichtig ist, dass die Rechtevorlage nur auf Rollen- und nicht Benutzerebene angewandt wird.

Rechtevorlagen können auch als Standard gesetzt werden: So wird automatisch die richtige Rechtevorlage vorab ausgewählt, wenn in der jeweiligen Organisationseinheit ein neues Passwort angelegt wird.



Solange keine Rechtevorlage definiert wurde, werden Rechte vererbt.

3. Sicherheit & Audits

Zunächst sollte eine Liste aller Zugangsdaten (Konten, Websites, Anwendungen, Tools, Programme) erstellt werden. Daraufhin wird sich ein Überblick darüber verschafft, welche Personen welche Zugriffsrechte darauf besitzen. So erfolgt ein IST-Abgleich, wer gegenwärtig Zugriff zu diesen Zugangsdaten hat, um sich einen aktuellen Stand über die Sicherheitslage zu verschaffen.

Änderungen sollten niemals einmalig für einzelne Mitarbeitende vorgenommen werden. Bei erforderlichen Änderungen sollte die Berechtigung für die gesamte Rolle angepasst oder bei Bedarf eine neue Rolle erstellt werden.

Fazit

RBAC ermöglicht es Unternehmen, Zugriffsberechtigungen ganz nach ihren individuellen Anforderungen und Bedürfnissen flexibel zu gestalten. So können durch die rollenbasierte Zugriffskontrolle diverse IT-Administrationsaufgaben erleichtert werden wie das Hinzufügen und Entfernen von Benutzern bei Mitarbeiterfluktutation oder das Angleichen von Rechten bei einem Positions- oder Abteilungswechsel.

Dazu kommt, dass sich rein aus sicherheitstechnischen Aspekten RBAC anbietet, um Zugriffe so gering wie möglich zu halten und überflüssige Berechtigungen zu vermeiden. Nur so kann effektiv möglichen Sicherheitsvorfällen und Cyberangriffen vorgebeugt werden. Und sollte es tatsächlich zu einem Vorfall kommen, kann schnell gehandelt und ein größeres Ausmaß verhindert werden, indem der Zugriff auf Daten sofort entzogen wird und im Falle von Password Safe auch die Passwörter automatisch ausgetauscht werden.

Das Berechtigungsmanagement in Password Safe ist der Schlüssel zu einer sicheren Verwaltung von Passwörtern im gesamten Unternehmen. Es bedeutet weniger Auf-wand, weniger Fehleranfälligkeit, mehr Sicherheit und Effizienz in der IT und damit auch bei allen anderen Mitarbeitern. Manuelle Änderungen, Fehlerbehandlungen, Warte-zeiten oder die individuelle Beantragung von Rechten: Dies alles entfällt und macht es zum idealen Konzept für jedes Unternehmen.

Autor:

Kristina Kaya
Product Marketing Managerin

MATESO
PASSWORD SAFE

Die MATESO GmbH ist ein führendes deutsches IT-Unternehmen, das sich seit der Firmengründung in 2006 erfolgreich im DACH-Raum etabliert hat. Die entwickelte Passwort-Sicherheitslösung Password Safe wird durch ihr weltweites Partnernetzwerk international vertrieben. Namhafte Referenzen bezeugen den Technologie- und Know-how-Vorsprung der IT-Software.

Heute verzeichnet das stetig wachsende Unternehmen branchenübergreifend über 10.000 Firmenkunden mit mehreren Millionen Anwendern weltweit – darunter 21 Firmen der Dax 40.

Pioneer im Enterprise Password Management

Password Safe dient Unternehmen als zentraler digitaler Tresor zur Sicherung, Verwaltung und Überwachung von sensiblen Daten wie Passwörtern, Dokumenten und Geheimnissen.

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.com
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE