05 | 24 Sonderdruck für tenfold Software

IT Administrator
Das Magazin für professionelle System- und Netzwerkadministration

tenfold 2024 (24.0)

www.it-administrator.de

tenfold 2024 (24.0)

Trau, schau, wem!

von Dr. Christian Knermann

Mit tenfold bietet der gleichnamige österreichische Hersteller eine IAM-Plattform zur Verwaltung von Benutzerkonten und Berechtigungen. Die Software automatisiert Arbeitsabläufe und reduziert manuelle Tätigkeiten in lokalen Microsoft-Umgebungen wie auch in Microsoft 365 und zahlreichen Systemen von Drittanbietern. IT-Administrator hat die neueste Version in der Praxis erprobt und war von der Funktionsvielfalt begeistert.

Der Titel dieses Tests, die Schlussworte einer Fabel des antiken Dichters Aesop, hat bis heute im allgemeinen Sprachgebrauch überdauert. Frei übersetzt rät das Sprichwort dazu, niemandem leichtfertig Vertrauen zu schenken. Es trifft damit bestens auf den Anspruch an ein modernes Identity- und Access-Management (IAM) zu, der sich aus Gesetzen, Verordnungen und regulatorischen Anforderungen ergibt, teils aus Complianceregeln, die Organisationen sich selbst auferlegen.

Nicht nur Unternehmen, die ihren IT-Betrieb an Normen wie der ISO/IEC-27000-Reihe oder dem TISAX-Standard ausrichten, stehen vor den Herausforderungen, Least-Privilege- und Need-to-know-Prinzipien umzusetzen. Sie müssen also ihre Anwender mit den minimal nötigen Berechtigungen ausstatten und den Zugriff auf Informationen nur gewähren, wenn und solange es nötig ist. IAM kümmert sich hier um die zentrale Verwaltung von Benutzerkonten mit ihren Zugriffsrechten und hat dabei im Optimalfall sämtliche Systeme und Anwendungen des Unternehmens sowohl lokal als auch in der Cloud im Blick. Dieser Herausforderung hat sich tenfold aus Wien mit seiner IAM-Plattform gestellt.

Kompletter Lebenszyklus im Fokus

tenfold zielt mit der hauseigenen Software auf eine umfassende Verwaltung von Benutzern und ihren Zugriffsrechten über den kompletten Lebenszyklus der Konten, begonnen beim Eintritt ins Unternehmen über eine Karriere mit beliebig vielen Wechseln von Positionen und Abteilungen bis hin zum Austritt aus der Organisation. Verbreitet ist hier das Meme eines Azubis, der im Laufe seiner Ausbildung alle Abteilungen durchläuft und schließlich die weitreichendsten Zugriffsrechte besitzt, da beim Wechsel in die nächste Abteilung niemand daran denkt, nicht mehr benötigte Berechtigungen zu widerrufen. Dem möchte der Anbieter mit mehreren Ansätzen entgegenwirken.

So stellt tenfold das Self-Service-Prinzip in den Mittelpunkt. Ziel ist dabei, die IT-Abteilung zu entlasten und den Fachabteilungen selbst die Verwaltung zu ermöglichen, Aufgaben also an die inhaltlich für die Daten zuständigen Stellen zu verlagern, die am ehesten beurteilen können, wer welche Berechtigungen benötigt. Zudem setzen die Österreicher auf flexibel konfigurierbare Workflows, die Genehmigungsprozesse auch über mehrere Hierarchieebenen hinweg automatisieren. Das System folgt dabei einem No-Code-Ansatz für die Workflows, ohne tiefgreifende Kenntnisse in Skript- oder Programmiersprachen vorauszusetzen.

Im Hinblick auf Compliance-Anforderungen und interne wie externe Audits hilft das integrierte Reporting Admins und Datenverantwortlichen dabei, die Vergabe von Zugriffsrechten in allen verbundenen Systemen nachvollziehbar zu dokumentieren. tenfold vergibt Berechtigungen nicht nur einmalig, sondern kümmert sich auch um eine regelmäßige Rezertifizierung, also die Überprüfung, ob vergebene Zugriffsrechte noch passen und tatsächlich nur autorisierte Nutzer auf sensible Daten zugreifen dürfen.

Gut verzahnt mit Microsoft und Drittanbietern

tenfold legt den Fokus auf hybride Microsoft-Infrastrukturen lokal wie auch in der Cloud. Die Software arbeitet mit Active-Directory-Umgebungen einschließlich Dateiservern, klassischen Exchange- und SharePoint-Servern sowie mit Microsoft 365 zusammen.

Darüber hinaus bringt der Anbieter über einen eigenen Marketplace Plug-ins mit, die zahlreiche Systeme von Drittanbietern integrieren. Ohne Anspruch auf Vollständigkeit seien hier das ERP-System von SAP, Groupware wie HCL Notes, Groupwise und Zimbra, Ticketsysteme wie OTRS, ServiceDesk Plus und TOPdesk oder Jira sowie die Softwareverteilung Matrix42 Empirum erwähnt. Weitere Systeme, für die sich kein herstellerspezifisches Plug-in findet, integriert tenfold mithilfe eines generischen Connectors,

per REST-API sowie über Java-, PowerShell-, SSH- und LDAP-Schnittstellen.

Wahl zwischen drei Editionen

tenfold vertreibt seine Software über Partner, die auch bei der Inbetriebnahme unterstützen. Ausschlaggebend sind dabei die gewünschte Edition sowie die Anzahl an Benutzern im Unternehmen. Letztere berechnet der Anbieter nur anhand natürlicher Personen und deren aktiven Konten. Deaktivierte Konten zählen ebenso wenig wie Accounts von Funktionsbenutzern.

Der Hersteller bietet sein Produkt in den drei Editionen Essentials, Essentials 365 und Enterprise mit aufsteigendem Funktionsumfang an. Alle drei umfassen den gleichen Kern an grundlegenden Funktionen von der automatischen Verwaltung der Identitäten über ihren gesamten Lebenszyklus, das Management von Zugriffsrechten im Self-Service bis hin zu zentralem Reporting und regelmäßigen Rezertifizierungen.

Die Essentials-Edition bindet lokale AD-Infrastrukturen und daran angeschlossene Dateiserver sowie Exchange Server an. Sie bringt zudem die REST-API, Schnittstellen für PowerShell und Java-basierte Skripte sowie ein Plug-in für E-Mail-Benachrichtigungen mit. Die höheren Editionen erlauben darüber hinaus die Anbindung zusätzlicher Systeme.

Die Variante Essentials 365 erweitert die Verwaltung auf hybride Bereitstellungen in Verbindung mit Entra ID, Microsofts ehemals als Azure AD bekanntem Verzeichnisdienst in der Cloud. Hier kümmert sich tenfold vor allem um die Dienste Exchange Online, SharePoint Online, Teams und OneDrive.

Erst die Enterprise-Edition dehnt den Funktionsumfang auf Microsoft Dynamics NAV, Microsoft SQL Server sowie die Groupware-, Helpdesk-Systeme und weitere Anwendungen von Drittanbietern aus. Auch die SSH-Schnittstelle sowie den generischen Connector und herstellerunabhängige Import- und Export-Plug-ins gibt tenfold nur der Enterprise Edition mit. Im Fokus unseres Interesses stand vor allem die Essentials-365-Edition im Hinblick auf die Verwaltung eines lokalen AD mit angeschlossenem Dateiserver sowie von Ressourcen in Microsoft 365.

IAM auf drei Säulen

Das IAM-System basiert auf drei Serverrollen: dem eigentlichen Applikationsserver, einer Datenbank zur Speicherung aller Einstellungen sowie der Benutzer- und Berechtigungsdaten und mindestens einem Agenten. In kleineren Umgebungen dürfen sich alle Rollen ein und denselben physischen oder virtuellen Server teilen. Die Systemanforderungen sind laut Hersteller moderat. Sowohl der Applikationsserver als auch der Agent verlangen lediglich 8 GByte Haupt- sowie mindestens 10 GByte Massenspeicher. Teilen sich Applikationsserver und Agent einen Server, verdoppeln sich diese Werte. Der Applikationsserver benötigt eine Java-Laufzeitumgebung und bringt diese bei der Installation automatisch mit. Die Datenbank darf sich auf demselben System wie der Applikationsserver befinden, muss dies jedoch nicht. Alternativ kann ein bestehender Datenbankserver, wahlweise Microsoft SQL Server oder Oracle Database, eine separate Datenbank bereitstellen. Für kleinere Umgebungen unterstützt tenfold die Express-Edition beider Datenbanksysteme, bittet aufgrund der Performance- und Größenbeschränkungen jedoch vor dem Einsatz um Rücksprache mit dem Support.

Der tenfold-Agent kümmert sich um die Verzahnung mit den Zielsystemen, liest und setzt Berechtigungen auf NTFS-Dateiservern sowie lokalen Exchange- und SharePoint-Servern. In geografisch verteilten Umgebungen sieht der Hersteller eine Instanz des Agenten pro Standort vor. Falls die entfernten Standorte mindestens mit 1-GBit/s-Geschwindigkeit verbunden sind, ist jedoch nicht zwingend eine separate Instanz erforderlich.

App-Registrierung für die Cloud

Für den Zugriff auf das AD setzt tenfold aus Sicherheitsgründen zwingend auf verschlüsseltes LDAPS. Zudem benötigt der Applikationsserver dauerhaft eine ausgehende HTTPS-Verbindung zum Marketplace des Herstellers, da das System selbsttätig die genutzten Plug-ins aktualisiert. Weitere notwendige Port-Freischaltungen im internen Netz erläutert die umfangreiche Dokumentation, die auch die Einrichtung der Dienstkonten und ihrer Berechtigungen beschreibt.

So setzt tenfold auf mehrere Konten, ein Dienstkonto für den Betrieb des Applikationsservers sowie jeweils separate Konten für das Management von Benutzern und ihren Zugriffsrechten im AD, auf Dateiservern sowie in lokalen Exchange- und SharePoint-Umgebungen. Für die Verwaltung von Berechtigungen in Microsoft 365 benötigt tenfold eine App-Registrierung in Entra ID mit Zugriff auf das Microsoft Graph-API. Auch diesen Zugriff mit den nötigen Berechtigungen in Microsofts Cloudinfrastruktur erläutert die Dokumentation detailliert.

Im Rahmen unseres Tests installierten wir den Applikationsserver mitsamt Da-

tenfold 2024 (24.0)

Produkt
Software für das Identity- und Access-Management (IAM).

Hersteller
tenfold
www.tenfold-security.com

Preis
Die Essentials-Edition als kleinstmögliche Variante kostet für ein exemplarisches Unternehmen mit 100 Benutzern als Kauflizenz inklusive einem Jahr Wartung 4320 Euro. Die Essentials-365-Edition für ein Unternehmen mit 500 Benutzern schlägt als Kauflizenz mit einem Jahr Wartung mit 24.950 Euro zu Buche; weitere Preise sind abhängig von Edition und Unternehmensgröße.

Systemanforderungen
Applikationsserver: Microsoft Windows Server 2012 (R2) / 2016 / 2019 / 2022 mit der Java-Laufzeit-Umgebung Amazon Coretto.

Datenbank: Microsoft SQL Server 2014 SP3 / 2016 SP2 / 2017 / 2019 / 2022 mit Microsoft SQL Server Management Studio oder Oracle Database 12.1 / 12.2 / 18c / 19c mit Oracle SQL Developer.

Agent: Microsoft Windows Server 2012 (R2) / 2016 / 2019 / 2022 mit .NET-Framework 4.8 (64-Bit).

Technische Daten
www.it-administrator.de/downloads/datenblaetter

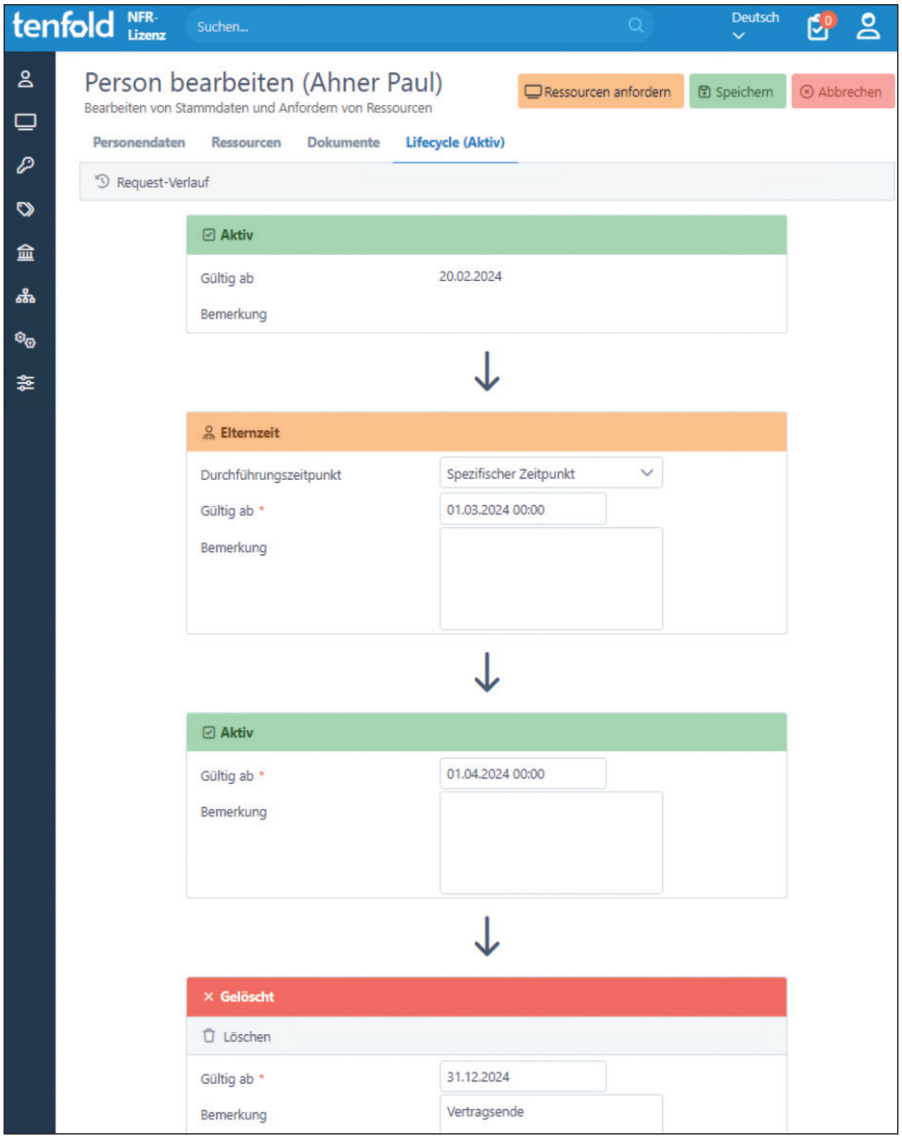

Bild 1: tenfold erlaubt das Planen des Lebenszyklus von Benutzerkonten im Voraus und setzt die Phasen automatisch um.

tenbank und den Agenten auf einer VM unter Windows Server 2019 mit Microsoft SQL Server 2019. Die begleitende Dokumentation gibt hierbei keine Rätsel auf und führt kleinschrittig zur betriebsbereiten Umgebung, deren weitere Verwaltung grundsätzlich per Weboberfläche im Browser erfolgt. Mit der aktuellen Version 24.0 hat tenfold die HTML-Benutzeroberfläche gegenüber früheren Versionen grundlegend renoviert und setzt nun auf ein modernes Layout, in dem sich Admins intuitiv zurechtfinden. Zunächst registrierten wir unter dem Punkt "Provisioning / Schnittstellen / Agents (MSIA)" unsere Agenten.

Anschließend begaben wir uns daran, unter dem Menüpunkt "Organisation" manuell die Struktur unseres exemplarischen Unternehmens abzubilden. Alternativ ist bei der Einführung in einer bestehenden Infrastruktur auch der umgekehrte Weg möglich und tenfold kann vorhandene Informationen wie Abteilungsnamen und Hierarchien sowie Standorte aus den AD-Konten von existierenden Benutzern importieren.

Unternehmensstruktur als Grundlage

tenfold eröffnet umfangreiche Möglichkeiten, sowohl die logische als auch die geografische Struktur einer Organisation zu erfassen. Dies vereinfacht im laufenden Betrieb die Pflege von Stammdaten, da tenfold Attribute, wie etwa Standort oder Abteilung eines Benutzers, anstelle von Freitext mit strukturierten Informationen aus Dropdown-Listen füllt.

Im Hinblick auf die Aufbauorganisation hinterlegten wir hier Unternehmen und Unternehmensteile, Abteilungen mit ihrer Hierarchie sowie Kostenstellen. Die physische Struktur konnten wir mithilfe von Niederlassungen und Gebäuden abbilden. An dieser Stelle verwendet die Software auch den Begriff der Organisationseinheiten, versteht darunter jedoch etwas anderes als OUs im AD. Eine Organisationseinheit fasst hier mehrere Niederlassungen zusammen. Laut Hersteller reichen den meisten Unternehmen die logischen Objekte der Abteilungen und Niederlassungen, tenfold ist aber in der Lage, auch sehr große, international aufgestellte Organisationen mit komplexen Strukturen abzubilden.

Unter einer Person als primärem Objekt versteht tenfold zunächst eine natürliche Person, die das System auf einem oder mehreren Benutzerkonten in verbundenen Systemen abbildet. Dies führte uns zur grundlegenden Konfiguration, wo wir zunächst unter dem Punkt "Einstellungen / E-Mail / SMTP-Server" das System für den Versand von Mail-Benachrichtigungen ertüchtigten. Hier bietet tenfold zwei Optionen, wahlweise die Konfiguration für den Mailserver in Form einer YAML-Datei oder direkte Eingabe im Webfrontend. In letzterem Fall versteht sich tenfold auf die üblichen Optionen, nämlich Verschlüsselung per TLS/SSL oder StartTLS sowie authentifizierten Versand.

An dieser Stelle sei eine Besonderheit erwähnt: tenfold speichert sämtliche Anmeldeinformationen zu verbundenen Systemen verschlüsselt und verwaltet diese an einer zentralen Stelle unter dem Punkt "Provisioning / Zugangsdaten". Dort konfigurierten wir auch gleich den Funktionsbenutzer für den Zugriff auf unser lokales AD sowie die App-Registrierung in Entra ID.

AD schnell eingerichtet

Die Verbindung zum AD richteten wir unter "Einstellungen / Active Directory Domänen" ein. Die Konfiguration erstreckt sich dabei über mehrere Register im Hauptbereich des Fensters. Neben den Koordinaten eines Domain Controllers konnten wir in der Sektion "Domänenobjekte" den Basis-DN definieren, unter

dem tenfold nach Objekten sucht. Alternativ zu allen Objekten unterhalb der Suchbasis bietet tenfold flexible Regeln für zu berücksichtigende Organisationseinheiten (Organizational Unit, OU) und Gruppen wie auch Ausschlüsse.

Drei weitere Register kümmern sich um die zu verwaltenden lokalen Ressourcen "Fileserver" sowie "Exchange" und "SharePoint". Hier hinterlegten wir die OU für die Gruppen zur Vergabe von Berechtigungen auf Dateifreigaben und fügten dann im unteren Bereich des Fensters unsere Freigaben hinzu. Dabei erwiesen sich die vielfältigen Optionen als besonders praktisch. Neben dem Anzeigenamen und Pfad zur Freigabe sowie dem zuständigen Agenten konnten wir pro Freigabe die Scan- und Bearbeitungstiefe für die Dateisystemberechtigungen festlegen.

Standard ist hier keine Einschränkung, alternativ beschränkt tenfold Scans und Bearbeitung von Berechtigungen sowie den Self-Service jeweils auf eine oder mehrere Verzeichnisebenen, maximal bis zu 15. Eine Beschränkung kann hier die Performance steigern und ein Ausufern an unterschiedlichen Berechtigungen sowie zugehörigen Gruppen verhindern. Das System identifiziert zudem explizit vergebene Berechtigungen und aufgebrochene Vererbung etwa aufgrund versehentlich verschobener Verzeichnisse. Die automatisch generierten Fileservergruppen zur Vergabe von Berechtigungen folgen einem anpassbaren Namensschema.

Dazu hatten wir bereits vor der Anbindung unserer Domäne im Bereich "Berechtigungen / Berechtigungsgruppen / Fileserver / Einstellungen" eine Konfiguration angelegt, nach der tenfold die Rechte verwaltet. Das System unterstützt unterschiedliche RBAC-Modi (Role-Based Access Control), unter anderen das von Microsoft empfohlene Prinzip AGDLP (Account, Global Group, Domain Local Group, Permission). Hier abstrahiert die Software weitestgehend vom Hantieren mit AD-Gruppen, um die zugehörigen Gruppen und ihre Hierarchie kümmert sich das System selbständig. Admins können sich somit ganz auf die logische Modellierung von Berechtigungen konzentrieren.

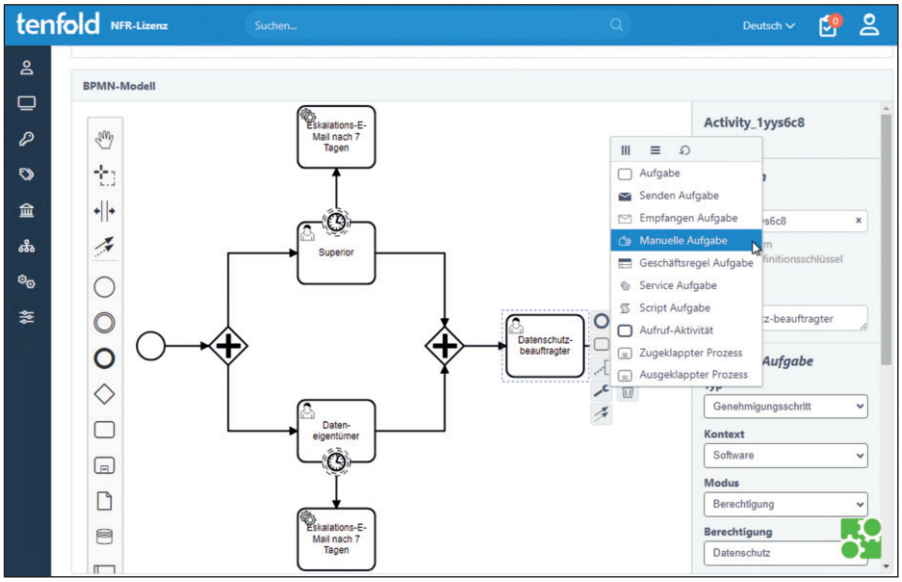

Bild 2: Der integrierte BPMN-Editor unterstützt auch komplexe Workflows mit mehreren Genehmigungsschritten.

Flexible Automatik für Benutzerkonten

Bei der Verwaltung von Personen unterscheidet tenfold grundsätzlich zwischen Mitarbeitern und externen Benutzern. Auch hier regelt das System so viel wie möglich automatisch, wobei uns die vielfältigen Möglichkeiten der Regeln für Benutzernamen überzeugten. Die konnten wir unter "Provisioning / Regelwerke / Benutzernamen" beeinflussen und etwa separate Regeln für Mitarbeiter und Externe verwalten. Eine Entscheidungstabelle steuert dabei, welche Regel wann greift.

Der Generator für Benutzernamen kann auf Wunsch in den Feldern für Vor- und Nachnamen Sonderzeichen ersetzen oder mithilfe frei definierbarer Code-Snippets darauf reagieren. Die Benutzernamen, etwa zur Anmeldung am AD und weiteren angeschlossenen Systemen, stattet die Plattform optional mit Präfix oder Suffix aus und behandelt Fälle von Namensgleichheit nach verschiedenen Eskalationsschemata durch Anhängen einer laufenden Nummer oder Variation der Anteile von Vor- und Nachnamen.

Darüber hinaus regelt der Bereich "Provisioning / Feldmappings" detailliert, welche Felder der Stammdaten tenfold in welche AD-Attribute überträgt und umgekehrt. Im Bereich "Provisioning / Plugins / Active Directory User Lifecycle" fanden wir weiterhin eine Fülle an Möglichkeiten zur Automatisierung der Benutzerverwaltung. So sortiert tenfold Benutzer anhand einer Entscheidungstabelle basierend auf einer Feldregel in eine bestimmte OU im AD ein und setzt beim Anlegen den User Principal Name (UPN) sowie das initiale Passwort. Letzteres verschickt tenfold entweder per E-Mail oder sorgt mithilfe eines One-Time-Secret-Verfahrens für zusätzliche Sicherheit. Ein solches One-Time-Secret teilt das System, optional gesichert mit einer zusätzlichen Authentifizierung am AD, wahlweise dem Anforderer, dem Vorgesetzten oder direkt der betroffenen Person, für die das Benutzerkonto bestimmt ist, mit.

Zur Abbildung von rollenbasierten Berechtigungen aufgrund von Zugehörigkeit zu einem Standort oder einer Abteilung verwendet tenfold Profile, die wir unter "Governance / Profile / Verwaltung" konfigurierten. Profile weisen automatisch die für eine bestimmte Rolle benötigten Ressourcen und Berechtigungen zu. Dabei konnten wir optional auch eine Übergangszeit definieren, die beim Entfernen einer Profilzuweisung greift. So gewährleistet die Software, dass ein Mitarbeiter beim Wechsel in eine neue Abteilung den Zugriff auf Ressourcen seiner vorherigen Abteilung nicht unmittelbar verliert, sondern erst nach einer wählbaren Frist von Tagen. Individuelle Zuweisungen abseits der jeweiligen Rolle entzieht tenfold dabei jedoch nicht automatisch.

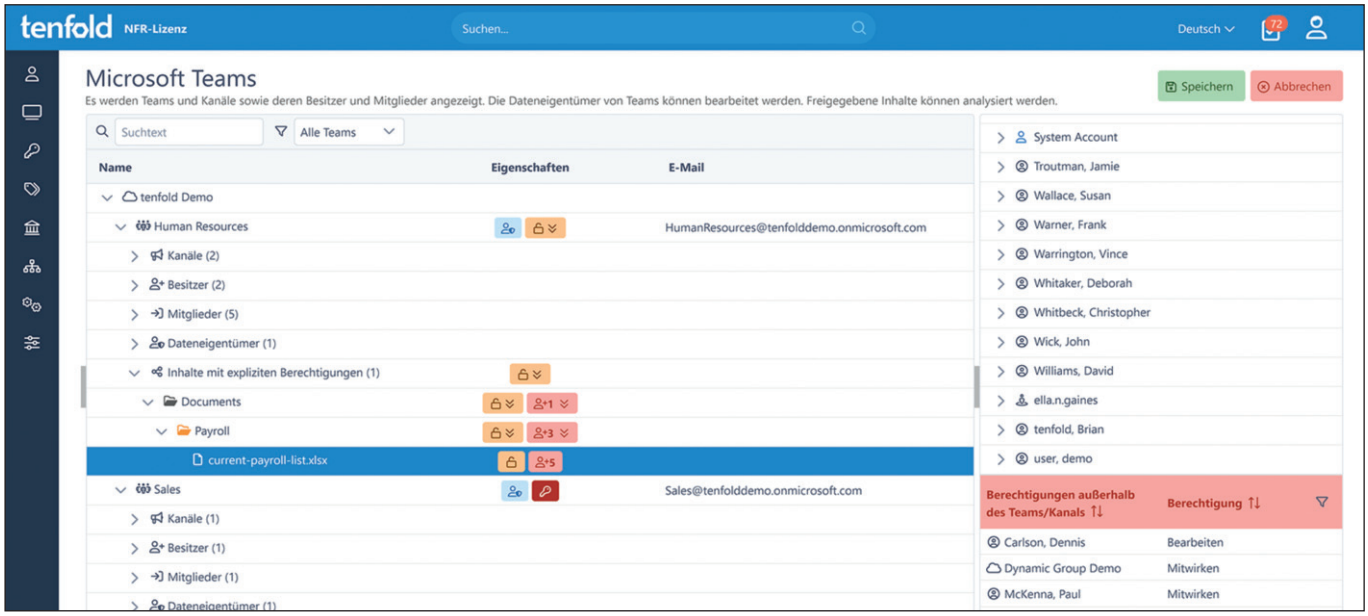

Bild 3: tenfold findet und korrigiert explizit gesetzte Berechtigungen, die von der Vererbung abweichen, auf lokalen Fileservern sowie auch in Microsoft 365.

Im Self-Service zum AD-Benutzer

Sobald wir alle Voraussetzungen und Regeln nach unseren Wünschen konfiguriert hatten, konnten wir uns daran machen, Benutzer anzulegen und Ressourcen zu verwalten. Den einfachsten Zugang ebnet die Startseite des Webfrontends mit farblich nach Kategorien unterschiedenen Kacheln. Mit Einstiegspunkten des Typs "Für mich" fordert jeder Benutzer für den Eigenbedarf Ressourcen an, vollzieht den Status bereits angeforderter und genehmigter Requests nach, richtet Stellvertreter ein oder ändert im Self-Service seine Stammdaten. Je nach Berechtigungen oder erteilten Stellvertretungen legen Kacheln des Typs "Für andere" weitere Benutzer an oder fordern Ressourcen im Namen anderer an. Kacheln des Typs "Verantwortung" ermöglichen je nach Berechtigungen administrative Operationen auf Ressourcen oder Benutzerkonten.

Auf diesem Weg konnten wir nun weitere Benutzer, Mitarbeiter wie auch Externe, mit frei gewählten Werten oder anhand vordefinierter Profile anlegen. Im ersten Schritt prüft das System dabei auf Dubletten und warnt, falls ein Benutzer mit identischem Namen bereits existiert, lässt weitere Konten gleichen Namens aber anhand der Generatorregeln zu. Die Eingabemaske für Personendaten ist frei konfigurierbar, sodass das Frontend sämtliche relevanten Felder abfragt und Benutzer aufgrund der gewählten Werte etwa für die Abteilung und die Niederlassung automatisch in die passende OU sowie AD-Gruppen aufnimmt und auch gleich zugehörige Ressourcen zuweist. tenfold erlaubt granulare Berechtigungen für jedes einzelne Feld der Eingabe, sodass etwa nur die Personalabteilung bestimmte Felder der Personaldaten, wie Personalnummer, Bankverbindung oder Privatadresse, überhaupt sehen und ändern kann.

Lebenszyklus mehrphasig abbildbar

Ebenso einfach gelang es uns, über die Kachel "Für andere anfordern" Änderungen vorzunehmen. Dabei interpretiert tenfold jede Änderung als Request, sowohl Ressourcenanforderungen als auch Änderungen an den Personaldaten, Stellvertretern oder der Abteilungszugehörigkeit. Die Bedienung über das Webfrontend gestaltet sich derart einfach, dass Admins Änderungen, die sich im Hintergrund auf das AD und weitere angeschlossene Systeme auswirken, gefahrlos auch an weniger IT-affine Anwender in anderen Abteilungen delegieren können.

Als besonders praktisch erwies sich der Editor für den Lebenszyklus einer Person. Nach der Auswahl einer Person erreichten wir über die Kachel "Personendaten bearbeiten" deren Stammdaten, zugewiesene Ressourcen und zugeordnete Dokumente. Auf der weiteren Registerkarte "Lifecycle" konnten wir den Lebenszyklus der Person modellieren. Anders als das AD, das nur ein fixes Ablaufdatum pro Benutzerkonto kennt, kann tenfold über mehrere Phasen hinweg ein Konto nach Bedarf sperren, reaktivieren und löschen. So konnten wir eine Person für eine geplante Abwesenheit, wie etwa eine Phase der Elternzeit, deaktivieren, anschließend reaktivieren und schließlich zum voraussichtlichen Vertragsende die Deaktivierung oder Löschung vorsehen (Bild 1).

Einfache Verwaltung auch komplexer Workflows

Die Verwaltung von Dateisystemberechtigungen haben wir aus zwei Perspektiven betrachtet: Zum einen natürlich aus der Sicht des Admins, der im Bereich "Berechtigungen / Active Directory / Fileserver" in einer Explorer-Ansicht Dateifreigaben browsen und für die Verzeichnisse darin die Berechtigungen anzeigen und auch anpassen kann. Dabei verwendet tenfold die unter "Berechtigungen / Berechtigungsgruppen / Fileserver / Berechtigungsstufen" hinterlegten fünf Stufen "Ordnerinhalt anzeigen (LST)", "Lesen und Ausführen (RX)", "Ändern (MD)", "Ändern Plus (MX)" oder "Vollzugriff (FC)".

Damit vereinfacht die Software die typischerweise benötigten Berechtigungen gegenüber den vielfältigen Optionen in Microsofts NTFS-Eigenschaften deutlich. Vorlagen helfen dabei, wiederkehrende Strukturen, etwa für identisch aufgebaute Projektordner, zu erzeugen.

Aus der Sicht eines Endanwenders gestalten Self-Services und Workflows die Verwaltung noch einfacher. Dazu erstellten wir zunächst einige Einträge im Bereich "Governance / Genehmigungen / Kontexte". Ein solcher Kontext ist ähnlich einem Postfach ein logischer Sammelpunkt für Anfragen zum Zugriff auf eine oder mehrere Ressourcen.

Die Workflows konfigurierten wir anschließend im Bereich "Governance / Genehmigungen / Workflows". tenfold bringt hier einige vorgefertigte Workflows mit, die wir anpassen oder als Vorlage für eigene Workflows verwenden konnten. Das System bietet hierzu einen interaktiven Editor, mit dem Admins ihre Workflows grafisch nach Business Process Model and Notation (BPMN) modellieren. Der Editor ermöglicht auch komplexe Workflows mit mehreren Genehmigungsschritten oder Verzweigungen (Bild 2).

Anschließend konnten wir die Workflows mit mehreren Browserfenstern aus der Sicht von verschiedenen Nutzern und Rollen durchspielen. Sobald ein Genehmigungsschritt auf eine Person wartet, erscheint eine Nachricht über die zu erledigende Aufgabe im Webfrontend der jeweiligen Person. Das System informiert zusätzlich per E-Mail darüber.

Abweichungen schnell ermittelt

Analog zu Berechtigungen im Dateisystem verwalteten wir auch Ressourcen in Microsoft 365. tenfold automatisiert hier die Handhabung von Gruppen, Teams, Exchange, SharePoint und generell geteilten Inhalten sowie die grundlegende Zuweisung von Lizenzen. So versahen wir etwa jeden Benutzer automatisch beim Anlegen mit einer Microsoft-365-E3-Lizenz, vergaben eine E5-Lizenz oder spezielle Produkte wie Visio oder Project aber nur nach manueller Anforderung und einem Genehmigungsworkflow.

Überzeugt haben uns anschließend vor allem die umfangreichen Möglichkeiten der Rezertifizierung, der Berichte und des Auditors. Per Schnellsuche nach einer Person konnten wir einen Bericht über sämtliche ihrer effektiven Berechtigungen erzeugen. Mit dem Fokus auf ein Verzeichnis oder eine Ressource in Microsoft 365 liefert das System detaillierte Informationen dazu, welche Benutzer und Gruppen zugreifen dürfen. Aus Sicht von Compliance und Informationssicherheit erweist sich dabei als äußerst nützlich, dass tenfold Berechtigungen außerhalb der Vererbungshierarchie anzeigt (Bild 3).

Insbesondere in Microsoft 365 erlauben Benutzer oftmals versehentlich mittels Linkfreigaben freizügigeren Zugriff, als sie eigentlich beabsichtigen. tenfold hilft dabei, solche Freigaben zu ermitteln und zu korrigieren. Compliance- und Informationssicherheitsbeauftragte dürfen sich weiterhin darüber freuen, dass die Plattform alle über das System veranlassten Änderungen in Form von "Requests" nachvollziehbar dokumentiert und der "Auditor" zudem eventuell am System vorbei durchgeführte Änderungen ermittelt.

Fazit

Wer darf worauf zugreifen und wer hat dies veranlasst? tenfold positioniert sich als umfassendes Werkzeug für das Access Management sowohl in lokalen AD-Infrastrukturen als auch in Microsoft 365. Die Plattform bringt derart viele Funktionen mit, dass wir im Rahmen unseres Tests längst nicht alle Bereiche betrachten konnten. Hervorgehoben seien die Möglichkeiten der Steuerung von Benutzerkonten und Zugriffsrechten, vor allem im Hinblick auf Microsoft 365. Besonders in Microsofts Cloud geben Endanwender oftmals unbeabsichtigt zu viele Informationen frei. tenfold identifiziert Abweichungen, unterstützt beim Korrigieren der Berechtigungen und stellt so die Compliance sicher. *(ln)*

So urteilt IT-Administrator

Benutzerverwaltung	7
Workflows und BPMN-Editor	8
Fileserver-Integration	7
Microsoft 365-Integration	8
Berichte und Audits	10

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik