One Person – One Identity – The Big Picture

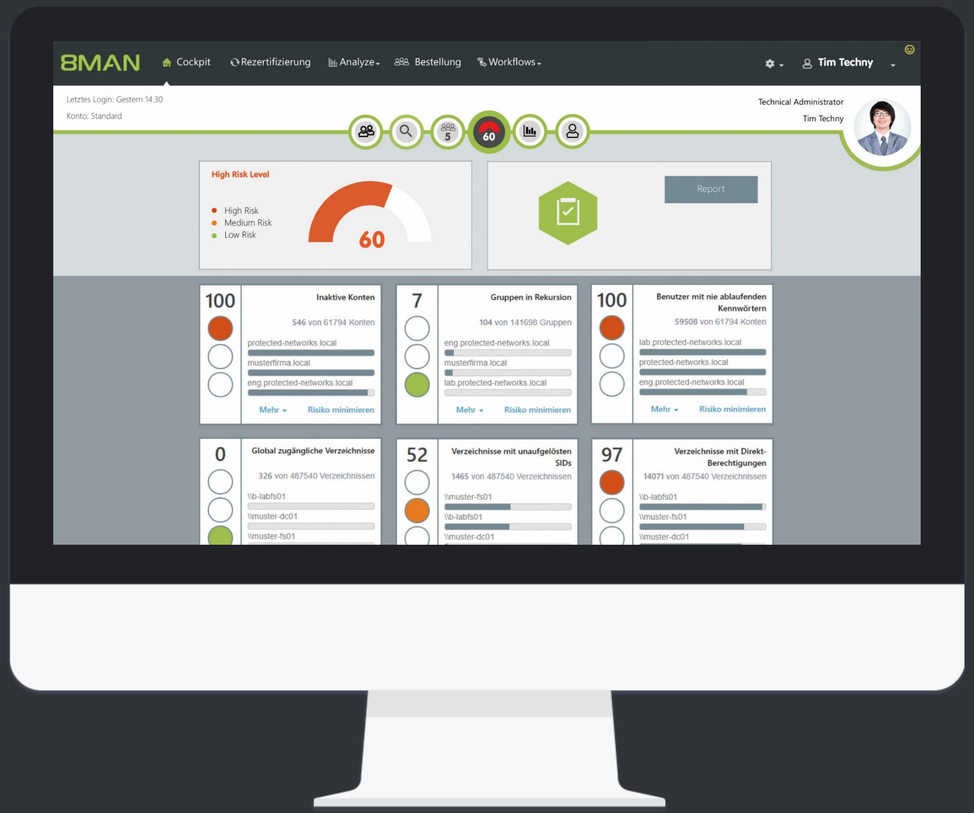
Wie Sie Joiner, Mover und Leaver ganz smart per Berechtigungsmanagement in den Griff bekommen und Standardprozesse automatisieren.

Arnd Rößner | Terrabit GmbH

8MAN

Agenda:
Das erwartet Sie die kommenden 45 Minuten

TERRABIT IT-SOLUTIONS



- Use-Case / Kundenprojekt
- Kundenanforderungen
- Lösungsansätze und Lösungs-Umsetzung
- Ihre Fragen

Die Story:
Es war eine strenge Mutter, die hatte zwei Töchter …

Unternehmens-Merge – nie ohne Risiko, weil:

- Konsolidierung der IT
- Verschiedenen Domänen und Topologien
- Angleichung der gelebten Prozesse

Mutterkonzern:

- Sitz in der EU (nicht DE)
- Zentral-IT, zusammengesetzt aus Personal der Tochterunternehmen Anna und Bella
- Gibt den Töchtern strenge IT-Vorgaben – bis hinunter auf Software- und Hardware-Ebene

Anna: [wurde aufgekauft]

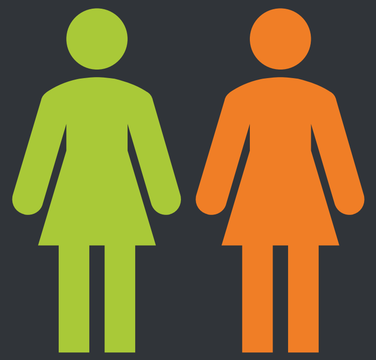
- 10.000 User
- Sitz in DE
- Eigene interne IT nach Vorgaben der Mutter ➔ kaum Freiheiten
- Bereits gut strukturiertes Identity and Access Management

Bella

- 5.000 User
- Sitz in DE
- Eigene interne IT nach Vorgaben der Mutter ➔ kaum Freiheiten
- Chaotisches Identity and Access Management

Zielsetzung des „One Person - One Identity“-Projekts:

- Töchter müssen eine gemeinsame Identität für alle Mitarbeiter schaffen
- Best Practice für gut strukturiertes Unternehmen Anna soll auch für Bella übernommen werden
- Pilotprojekt-Charakter
- Zusage: Bei Erfolg veranlasst Konzernmutter Schritt-für-Schritt konzernweite Übernahme dieses Use Case auf weitere Tochterunternehmen



Aus den eigenständigen Töchtern Anna und Bella wird Anna-Bella

- 15.000 User
- Jeder User hat exakt eine Mitarbeiter-Identität
- Die Identität ist individuell und unverwechselbar, vom Eintritt ins Unternehmen bis zum Austritt
- Die Identität gilt über alle Anwendungen und Zugriffsbereiche hinweg

Die Anforderungen an den Gesamtprozess:
Nur eine Identität

Konkrete Anforderungen, mit denen der Kunde im Rahmen des Projekts auf uns zukam:

- **Eine einzige Mitarbeiteridentität** vom Eintritt ins Unternehmen bis zum Austritt. Keine Ausnahme (z.B. derselbe Mitarbeiter wird unter verschiedener Identität bei Mutter- und Tochterunternehmen gepflegt).
- Die **Identität gilt für alle Anwendungen und Zugriffsbereiche** (z.B. SAP, Windows, Zeiterfassung, Zutrittskontrolle).
- **Beschleunigung des Joiner-, Mover-, Leaver-Prozesses** von aktuell 16 Stunden Aufwand auf Zielwert von 2 Stunden.
- **Auslagerung des Joiner-, Mover-, Leaver-Prozesses** an HR, um in der IT freie Ressourcen zu schaffen.
- **Bereinigung:** Entfernen von sicherheitskritischen, nicht mehr benötigten (Direkt-) Berechtigungen und weiterem Gefahrenpotenzial wie Verzeichnisse mit unaufgelösten SIDs, global zugängige Verzeichnisse und nonkonforme Benutzerkonten.

Die Anforderungen an den Gesamtprozess:
Nur eine Identität

Konkrete Anforderungen, mit denen der Kunde im Rahmen des Projekts auf uns zukam:

- Einführung eines **Personal-Owners** (= Vorgesetzte sind für die Berechtigung der ihnen zugeordneten Mitarbeiter verantwortlich) und **Data-Owner-Konzept** für Daten-Berechtigung.
- Evaluierung eines **Single-Sign-On-Konzepts** (aktuell nur zu SAP möglich).
- **Berechtigungsworkflow** soll **papierlos** umgesetzt werden, idealerweise auf Basis eines **Webtools**. **Automatisierungen und Subprozesse** erleichtern auch dem unregelmäßigen Anwender die effiziente Nutzung der Berechtigungs-Software.
- Einführung einer Möglichkeit zur **lückenlosen Dokumentation**, welche Berechtigungs-Änderungen und Anpassungen wann von wem vorgenommen wurden.

8MAN …und zwei weitere Punkte,
die wir aus den ersten Briefings mitnahmen:

TERRABIT IT-SOLUTIONS

Kunden-Annahme 1:

Ein Identitätsmanagement bildet alle Anforderungen in Sachen Identitätsfrage ab.

Fehlschluss!

Es ist falsch, zwischen User-Identity und Datenzugriffskonzept zu trennen. Berechtigungsmanagement ist elementar!

Beides (Identitäts- und Berechtigungsmanagement) muss unbedingt gemeinsam betrachtet werden!

User-Identity und Datenzugriffskonzept

Kunden-Annahme 2:

Microsoft AD

Microsoft Active Directory deckt mit seinen umfangreichen Funktionalitäten meine Berechtigungs-Anforderungen ab.

Fehlschluss!

Microsoft Active Directory ist zwar ein äußerst mächtiges Tool, berücksichtigt aber nicht das „Warum“: Man erkennt nicht, wer wann und weshalb eine Berechtigung geändert hat.

Außerdem kann das Active Directory folgende simple Fragen nicht beantworten:

- Liste mir alle detaillierten Berechtigungen des Mitarbeiters X auf!
- Liste mir für Dokument Y alle Personen auf, die darauf Zugriff haben!

8MAN 3 potenzielle Gefahren, die wir im Blick behalten mussten

TERRABIT IT-SOLUTIONS

Fluktuation

Statistik: Alle drei Jahre wechselt ein Mitarbeiter das Unternehmen, die Abteilung oder geht in den Ruhestand. Wächst das Unternehmen zusätzlich, erhöht sich der Administrations-Aufwand für User-Berechtigungen entsprechend.

Pensionierungen sogar nur bei 1,3 Prozent.
Jedes Jahr wechselt rechnerisch knapp jeder dritte Arbeitnehmer in Deutschland den Job. Die Fluktuationsquote beträgt damit rund 30 Prozent, Pensionierungen werden grundsätzlich eingerechnet. Die Quote wird erhoben, indem das Mittel der

Süddeutsche Zeitung
30. September 2017

Eisberg Effekt

Statistik: Alle drei Jahre wechselt ein Mitarbeiter das Unternehmen, die Abteilung oder geht in den Ruhestand. Wächst das Unternehmen zusätzlich, erhöht sich der Administrations-Aufwand für User-Berechtigungen entsprechend.

Parallel-Universum

Statistik: Alle drei Jahre wechselt ein Mitarbeiter das Unternehmen, die Abteilung oder geht in den Ruhestand. Wächst das Unternehmen zusätzlich, erhöht sich der Administrations-Aufwand für User-Berechtigungen entsprechend.

User-Identity

VS

Datenzugriffs-konzept

Gesucht:
Ein erfolgversprechender Lösungsansatz für das Projekt

In vier Schritten Joiner, Mover und Leaver smart in den Griff bekommen:

1 **Auslagern**

Diejenigen Personen in den Prozess einbinden,
die wirklich zuständig sind (HR, Fachabteilung). Nicht alles auf die interne IT abwälzen

➔ **Data-Owner-Prinzip**

2 **Automatisieren**

So viele Schritte wie möglich automatisieren:
Standard-Routinen erstellen, automatisch gestartete Prozesse implementieren,
benutzerfreundliche intuitive Gestaltung für Non-IT-Mitarbeiter …

3 **Zusammenlegen**

Verzahnung von User-Identity und Datenzugriffskonzept

4 **Bereinigen**

Bereinigen des File-Systems im Live-Betrieb

Gesucht:
Ein erfolgversprechender Lösungsansatz für das Projekt

In vier Schritten Joiner, Mover und Leaver smart in den Griff bekommen:

1 **Auslagern**

Diejenigen Personen in den Prozess einbinden,
die wirklich zuständig sind (HR, Fachabteilung). Nicht alles auf die interne IT abwälzen

➔ **Data-Owner-Prinzip**

2 **Automatisieren**

So viele Schritte wie möglich automatisieren:
Standard-Routinen erstellen, automatisch gestartete Prozesse implementieren,
benutzerfreundliche intuitive Gestaltung für Non-IT-Mitarbeiter …

3 **Zusammenlegen**

Verzahnung von User-Identity und Datenzugriffskonzept

4 **Bereinigen**

Bereinigen des File-Systems im Live-Betrieb

8MAN Management-Ansicht:
Überblick behalten – auch für Non-ITler

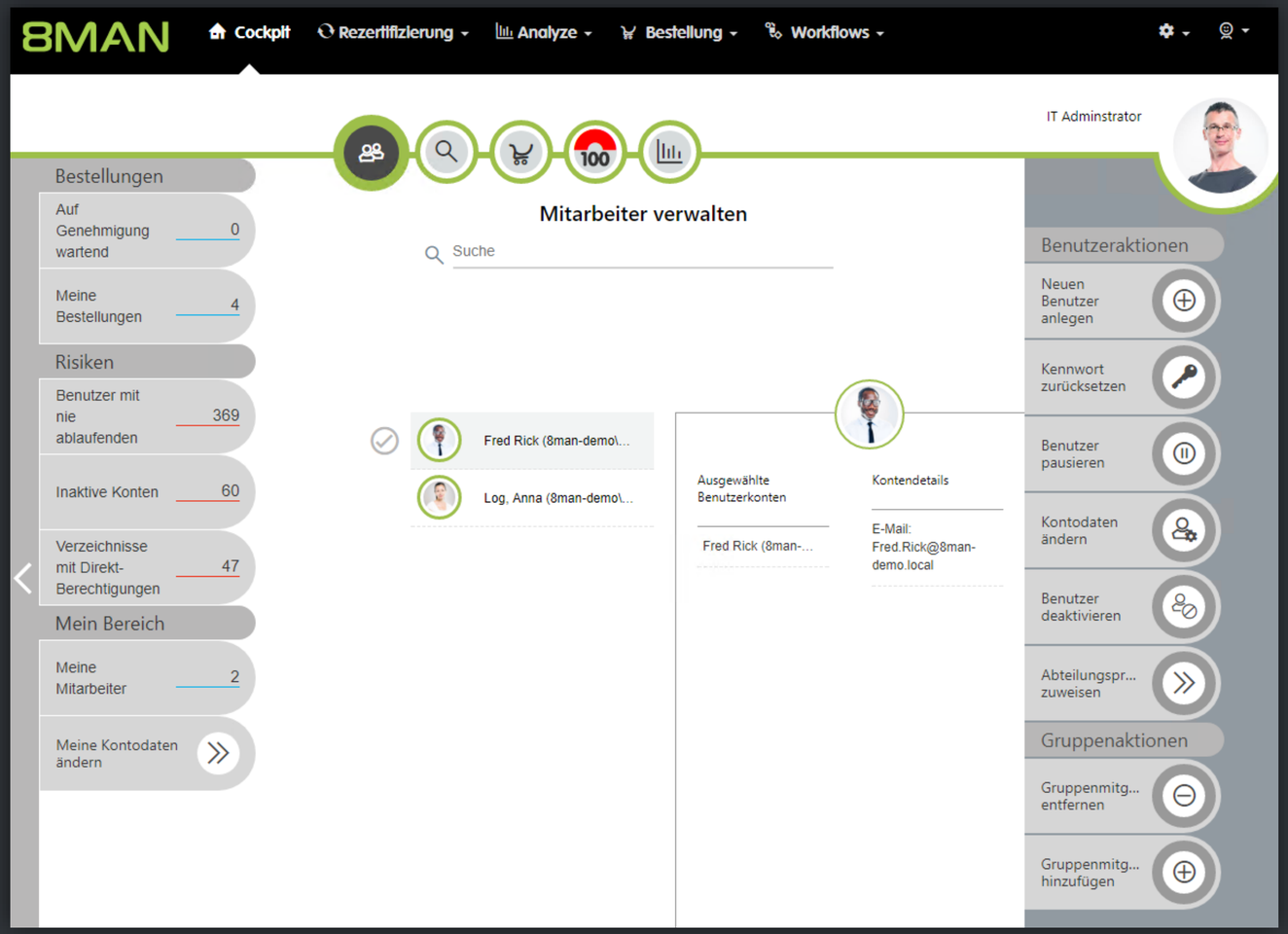
TERRABIT IT-SOLUTIONS

1 Auslagern

2 Automatisieren

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Intuitiv bedienbares Dashboard
- Risiken werden sofort angezeigt
- Gruppen-Berechtigung steht ebenfalls zur Auswahl



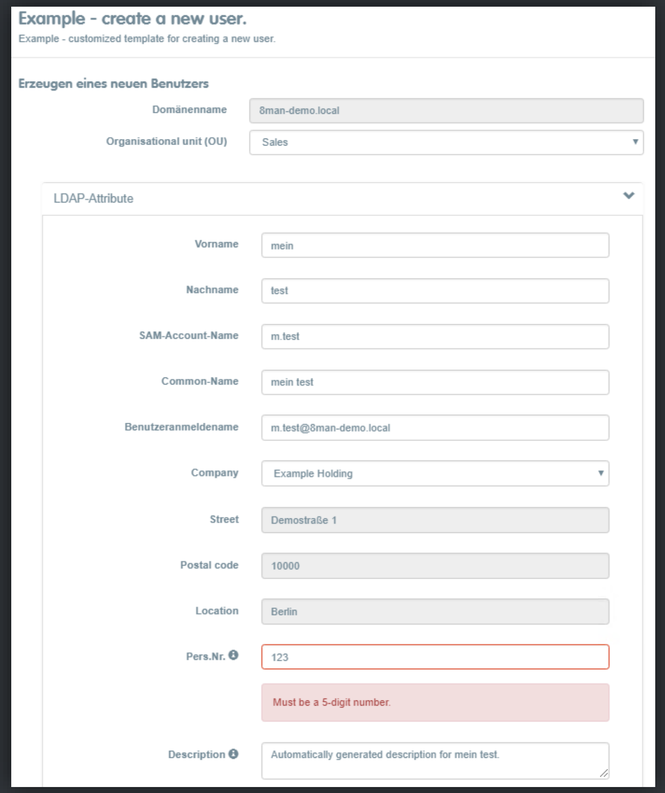
Der Joiner-Prozess im Detail aus HR-Sicht:
Neuen Nutzer anlegen

1 Auslagern

2 Automatisieren

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Individuelles Anlegen von Benutzern mit Kombination beliebiger AD-Attribute und Pull-Down-Menüs
- Einschränkung via RegEx möglich
- Skriptausführung vor und nach Benutzeranlage



8MAN Der Joiner-Prozess im Detail aus HR-Sicht:
Neuen Nutzer anlegen

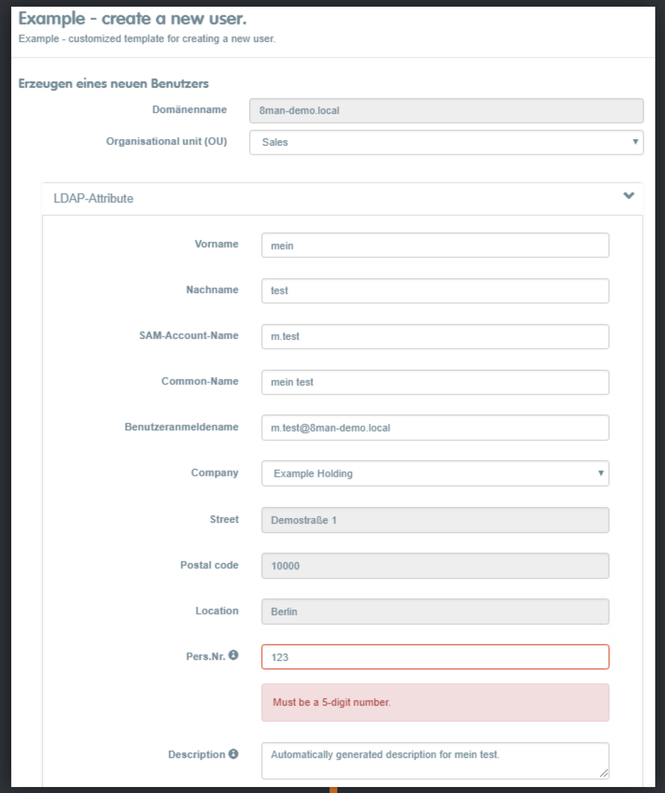
TERRABIT IT-SOLUTIONS

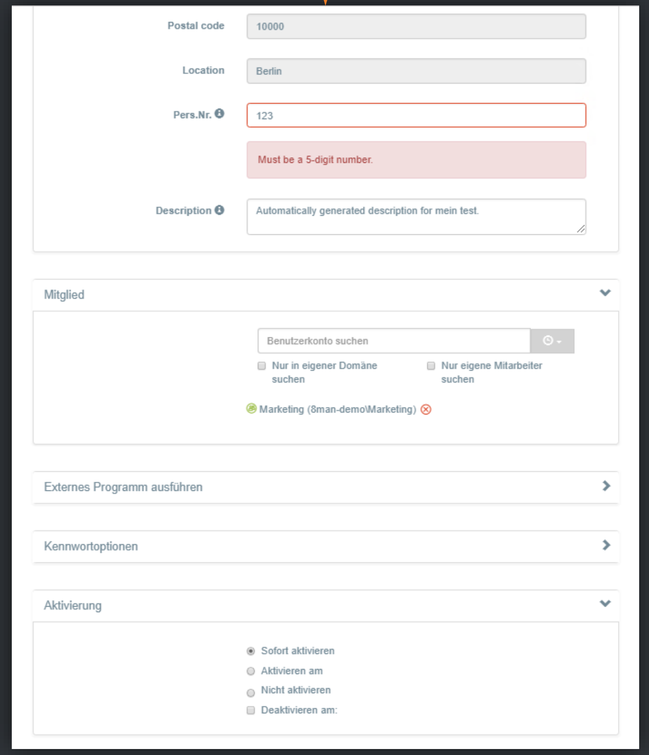
1 Auslagern

2 Automatisieren

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Vorauswahl der Gruppenmitgliedschaften …
- OUs, etc. – Aktivierungsoptionen und Scripting
- Templates sind bestell- und deligierbar





8MAN Der Joiner-Prozess im Detail aus HR-Sicht:
Der Bestellprozess

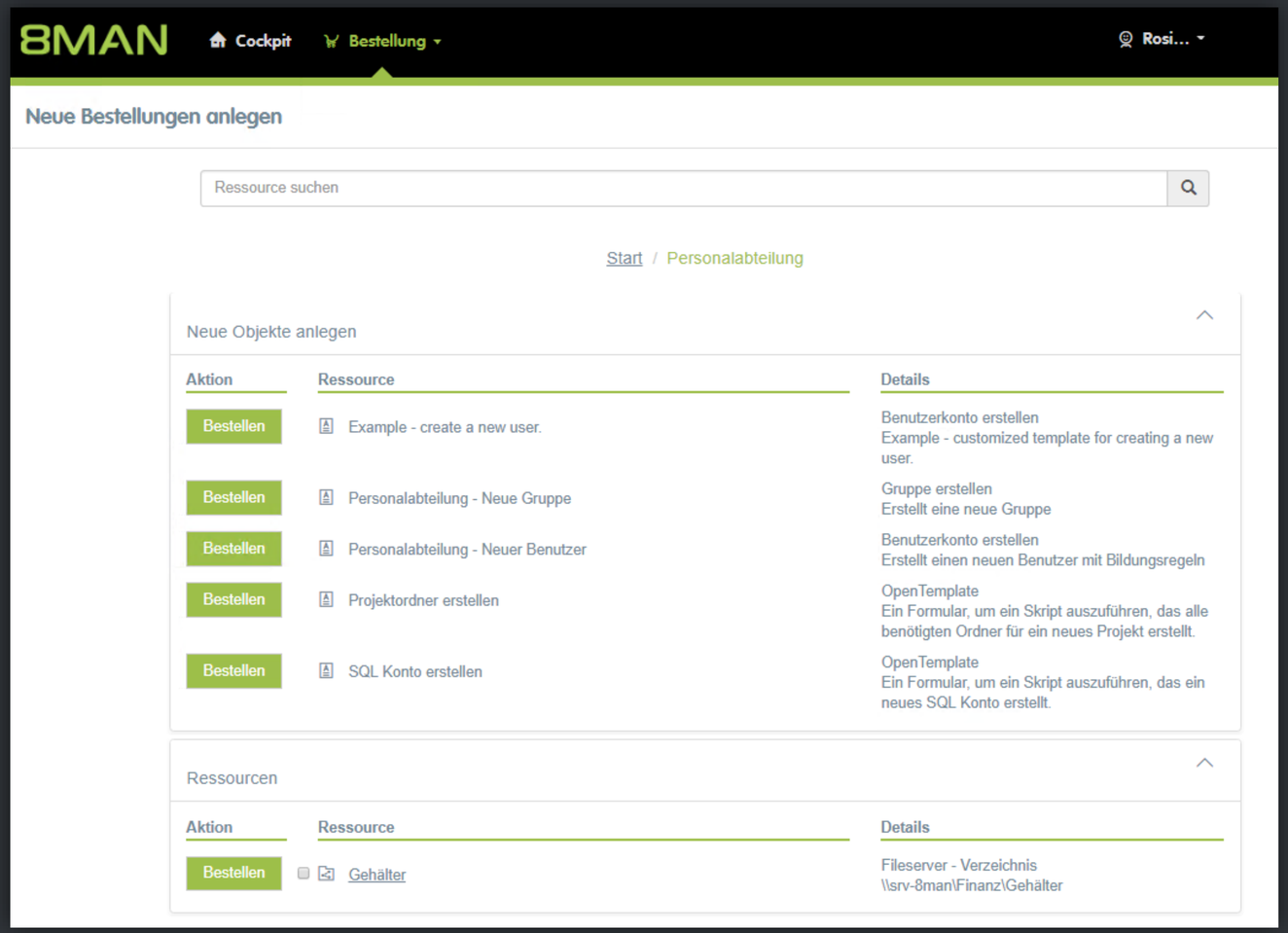
TERRABIT IT-SOLUTIONS

1 Auslagern

2 Automatisieren

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Individuell konfigurierbare Auswahl
- Data-Owner
- Beliebiger und-/oder-Workflow
- Bestellbare Skripte



8MAN Der Joiner-Prozess im Detail aus HR-Sicht:
Data-Owner-Konfiguration

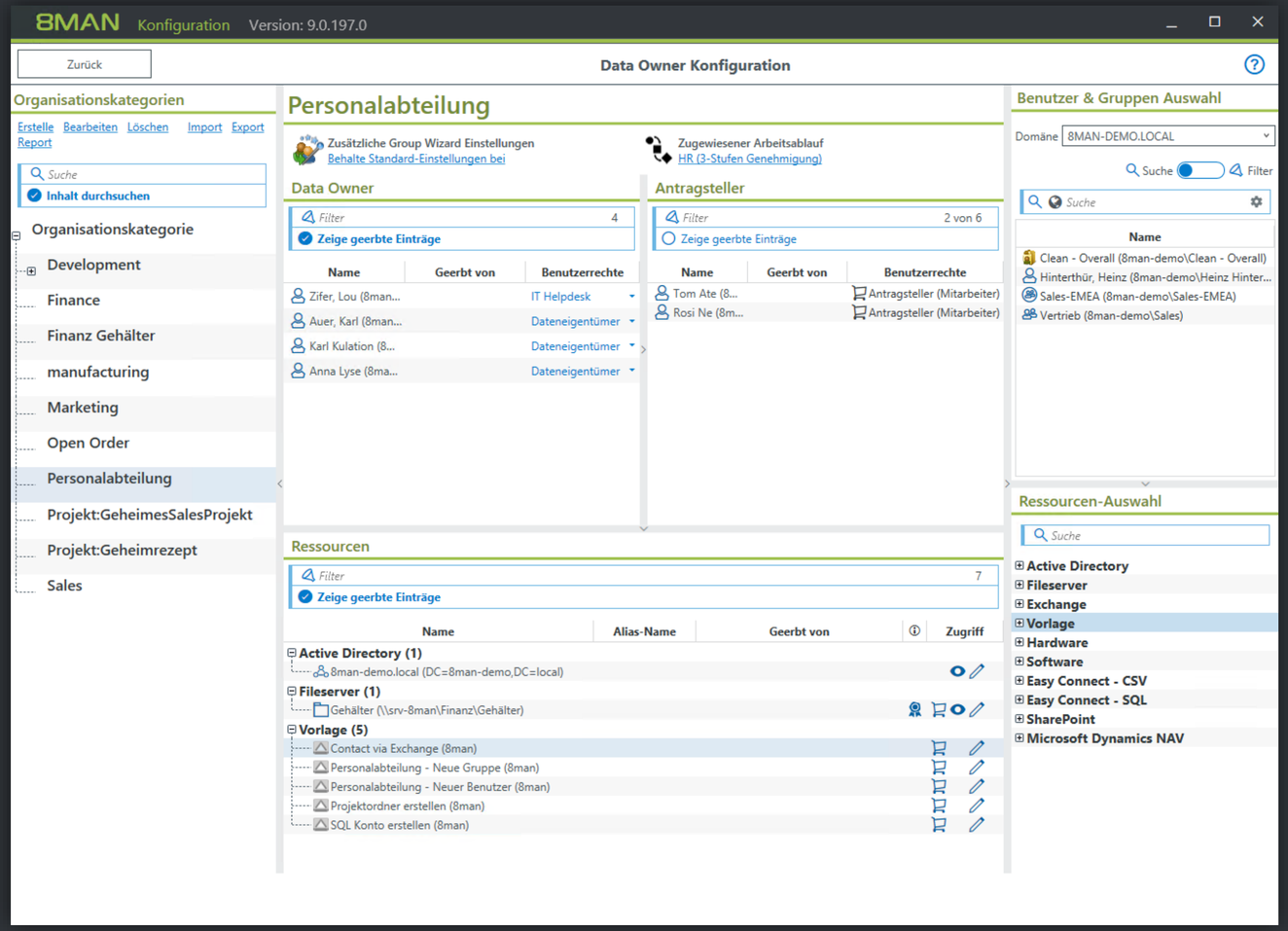
TERRABIT IT-SOLUTIONS

1 Auslagern

2 Automatisieren

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

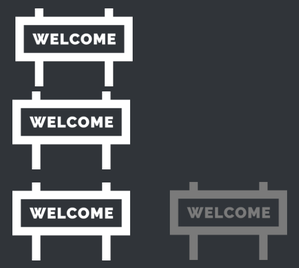
- Einfache Konfiguration (hierarchisch und funktionell)
- Einschränkung auf OUs und einzelne Pfade
- Rezertifizierung, Alias-Namen, individuelle Arbeitsabläufe und Ausblenden von Ressourcen



TERRABIT IT-SOLUTIONS

Enorme Ersparnisse durch optimierte Berechtigungsmanagement-Software.

JOINER-Prozess



MOVER-Prozess

LEAVER-Prozess

NON-IT-Berechtigungsprozess

Enorme Ersparnisse durch optimierte Berechtigungsmanagement-Software.

JOINER-Prozess

Berechtigungs-Aufwand pro neuem Mitarbeiter
von 3 Stunden auf 1 Stunde reduziert

ROI-Berechnung Joiner-Prozess

Bei 50 Neueinstellungen / Monat
bzw. 600 Neueinstellungen / Jahr
x 3 Stunden Arbeitsaufwand

➔ **1.800 Stunden pro Jahr [alt]**

vs. **600 Stunden pro Jahr [neuer Workflow]**

Bei einem internen Verrechnungswert von
40 EUR / Stunde errechnet sich eine
Ersparnis von 48.000 EUR pro Jahr.

Enorme Ersparnisse durch optimierte Berechtigungsmanagement-Software.

MOVER-Prozess

Berechtigungs-Aufwand pro wechselndem Mitarbeiter von 1 Stunde auf 0,25 Stunden reduziert

ROI-Berechnung Mover-Prozess

Bei 500 Mitarbeiter-Anpassungen / Monat
bzw. 6.000 Mitarbeiter-Anpassungen / Jahr
x 1 Stunde Arbeitsaufwand

➔ **6.000 Stunden pro Jahr [alt]**

vs. **1.500 Stunden pro Jahr [neuer Workflow]**

Bei einem internen Verrechnungswert von 40 EUR / Stunde errechnet sich eine **Ersparnis von 180.000 EUR pro Jahr.**

Enorme Ersparnisse durch optimierte Berechtigungsmanagement-Software.

LEAVER-Prozess

Berechtigungs-Aufwand für jeden Mitarbeiter, der das Unternehmen verlässt, von 1 Stunde auf 0,25 Stunden reduziert

ROI-Berechnung Leaver-Prozess

Bei 30 Mitarbeiter-Austritten / Monat
bzw. 360 Mitarbeiter-Austritten / Jahr
x 1 Stunde Arbeitsaufwand

➔ **360 Stunden pro Jahr [alt]**

vs. **90 Stunden pro Jahr [neuer Workflow]**

Bei einem internen Verrechnungswert von 40 EUR / Stunde errechnet sich eine **Ersparnis von 10.800 EUR pro Jahr.**

Enorme Ersparnisse durch optimierte Berechtigungsmanagement-Software.

NON-IT-Berechtigungs-prozess

3h

Jeder Non-IT-Mitarbeiter spart 3 Stunden Arbeitszeit im Jahr durch den optimierten, software-gestützten Berechtigungsprozess

Steigerung der Produktivität

Die Produktivität erhöht sich, weil diverse Anfragen an die IT-Abteilungen schneller (Self-Service) und mit geringerem Benutzer-Impact durchgeführt werden können.
vs. 3 Stunden pro Jahr [neuer Workflow]

Bei einem internen Verrechnungswert von 30 EUR / Stunde und bezogen auf 7.500 Mitarbeiter errechnet sich eine **Ersparnis von 675.000 EUR pro Jahr.**

Der „Azubi-Effekt“
– und was wir daraus lernen können

1 Auslagern

Diejenigen Personen in den Prozess einbinden,
die wirklich zuständig sind (HR, Fachabteilung). Nicht alles auf die interne IT abwälzen

➔ **Data-Owner-Prinzip**

2 Automatisieren

So viele Schritte wie möglich automatisieren:
Standard-Routinen erstellen, automatisch gestartete Prozesse implementieren,
benutzerfreundliche intuitive Gestaltung für Non-IT-Mitarbeiter …

3 Zusammenlegen

Verzahnung von User-Identity und Datenzugriffskonzept

4 Bereinigen

Bereinigen des File-Systems im Live-Betrieb

3 Zusammenlegen

4 Bereinigen

Ausgangssituation: Ein Auszubildender durchläuft mehrere Abteilungen. Damit er arbeitsfähig ist, werden ihm neue, abteilungsspezifische Berechtigungen verliehen.

Problem: Niemand entzieht dem Azubi die nun nicht mehr benötigten bisherigen Berechtigungen. Denn während in Unternehmen das Grundset (Programm-Zugriffe, E-Mail-Konten, VPN-Zugriffe) streng überwacht wird, hakt es oftmals beim Datenberechtigungskonzept gewaltig.

Die Folge: Der Azubi wird zum Super-User und hat mehr Berechtigungen als seine Abteilungskollegen.

8MAN Joiner-, Mover-, Leaver-Prozess in der Praxis:

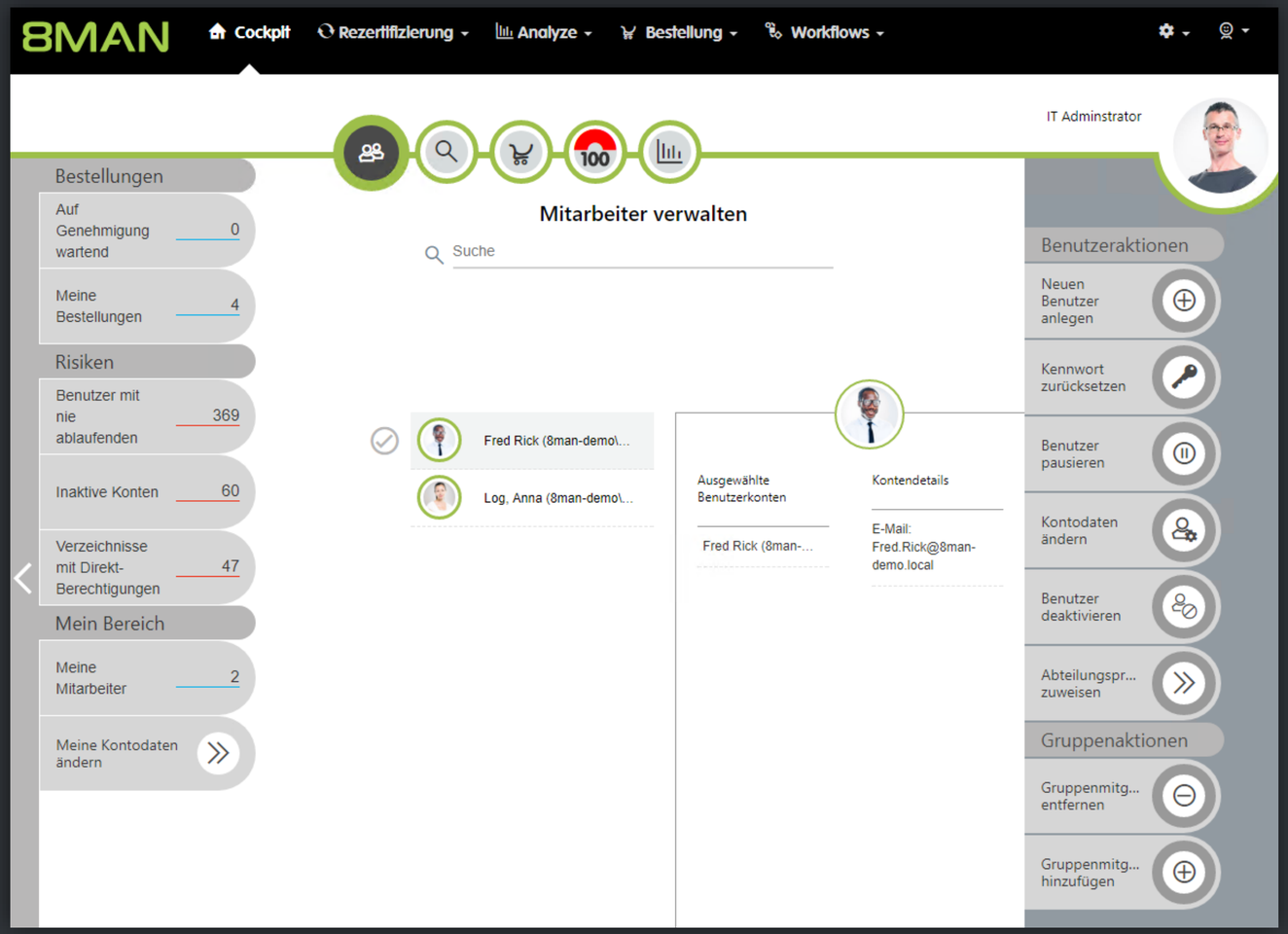
TERRABIT IT-SOLUTIONS

3 Zusammenlegen

4 Bereinigen

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Direkte Darstellung Mitarbeiter (aus Active Directory)
- Individuelle Abteilungsprofile, Passwort-Resets, etc. (individuell deligierbar)
- Bereinigung der Risiken (Report & Action) im jeweiligen Kontext



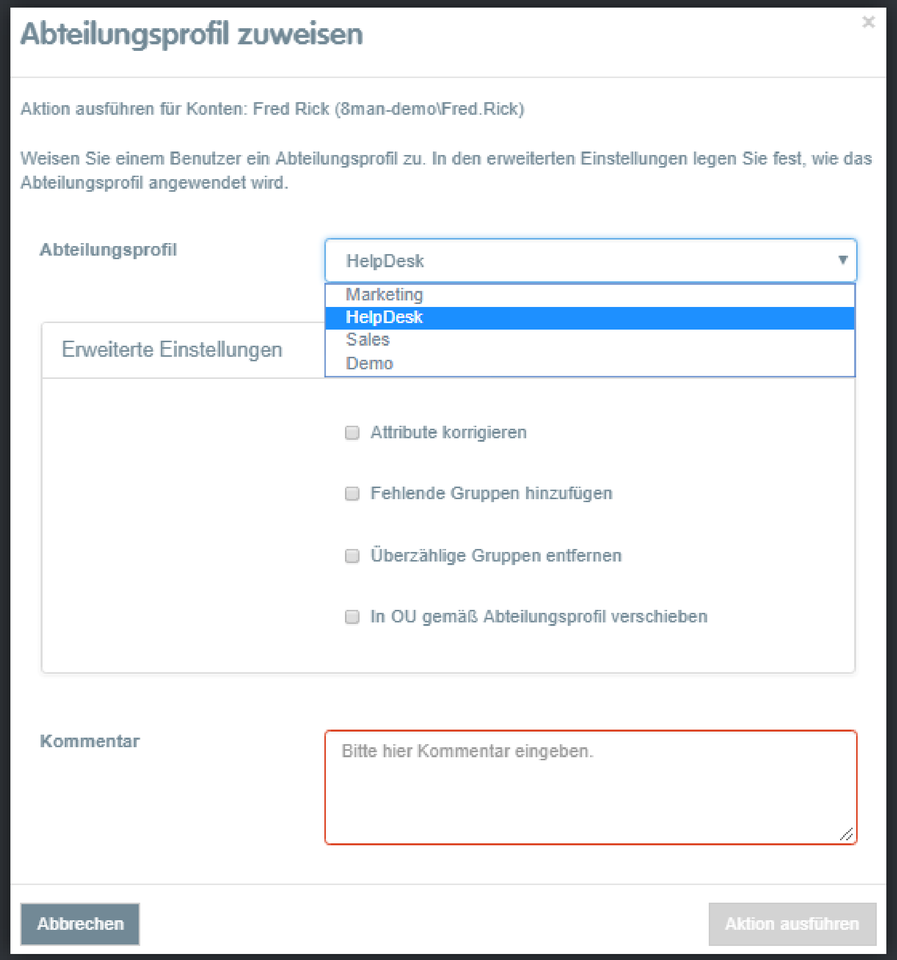
Joiner-, Mover-, Leaver-Prozess in der Praxis:

3 Zusammenlegen

4 Bereinigen

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Leichtes / komfortables Umziehen der Identitäten
- Entzug nicht benötigter Berechtigungen („Azubi-Effekt“)
- Begründung der neuen Rechtezuweisung

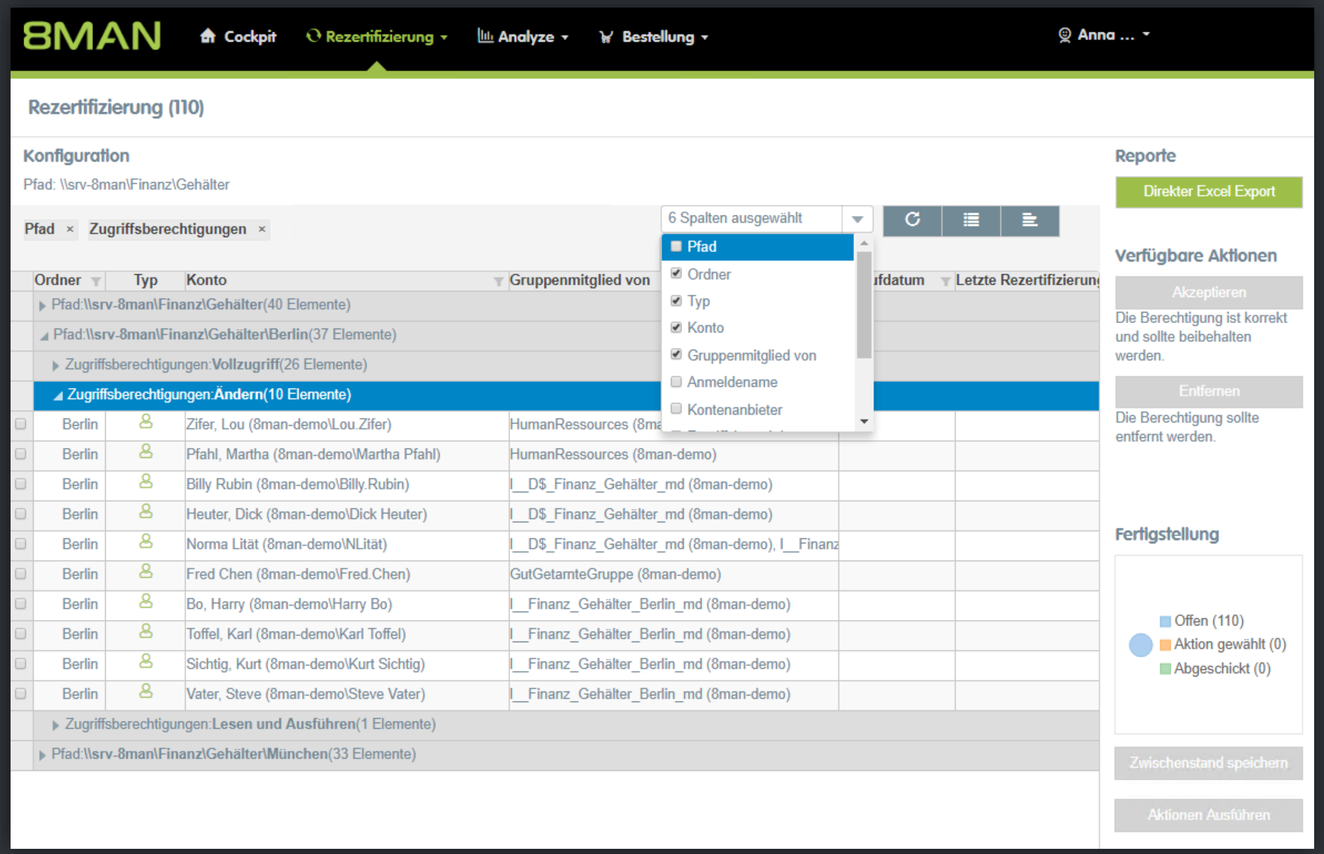


3 Zusammenlegen

4 Bereinigen

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Überprüfung (Bestätigung) / Korrektur (Entzug) direkt durch Data-Owner
- Entzug nicht benötigter Berechtigungen
- Begründung der neuen Rechtezuweisung



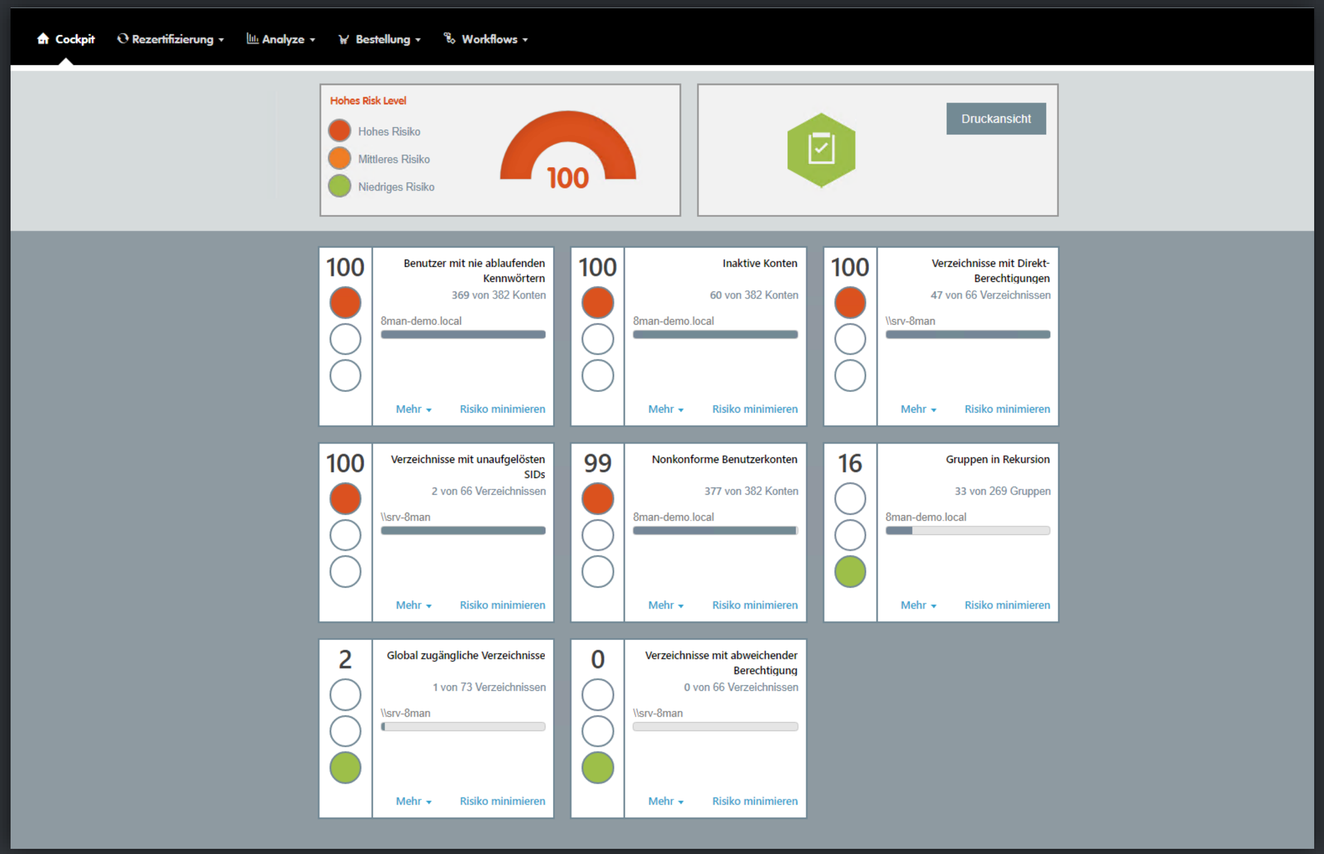
TERRABIT IT-SOLUTIONS

3 Zusammenlegen

4 Bereinigen

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Übersichtliche Risikoanalyse (Risk Assessment)
- Risiken und Lösung im Kontext
- Möglichkeit der Korrektur/Bereinigung einfach (dokumentiert) und delegierbar



Das Microsoft Active Directory ist in seiner aktuellen Ausführung nicht DSGVO-konform:

- Weder Historie noch Logs mit Hinweis, wann einem Mitarbeiter welche Berechtigungen zugeteilt / entzogen wurden.
- Keine Dokumentation und Nachvollziehbarkeit, wer weshalb einem Mitarbeiter Berechtigungen zugewiesen oder entzogen hat.

TERRABIT IT-SOLUTIONS

Features, die eine Software für Berechtigungsmanagement bieten sollte:

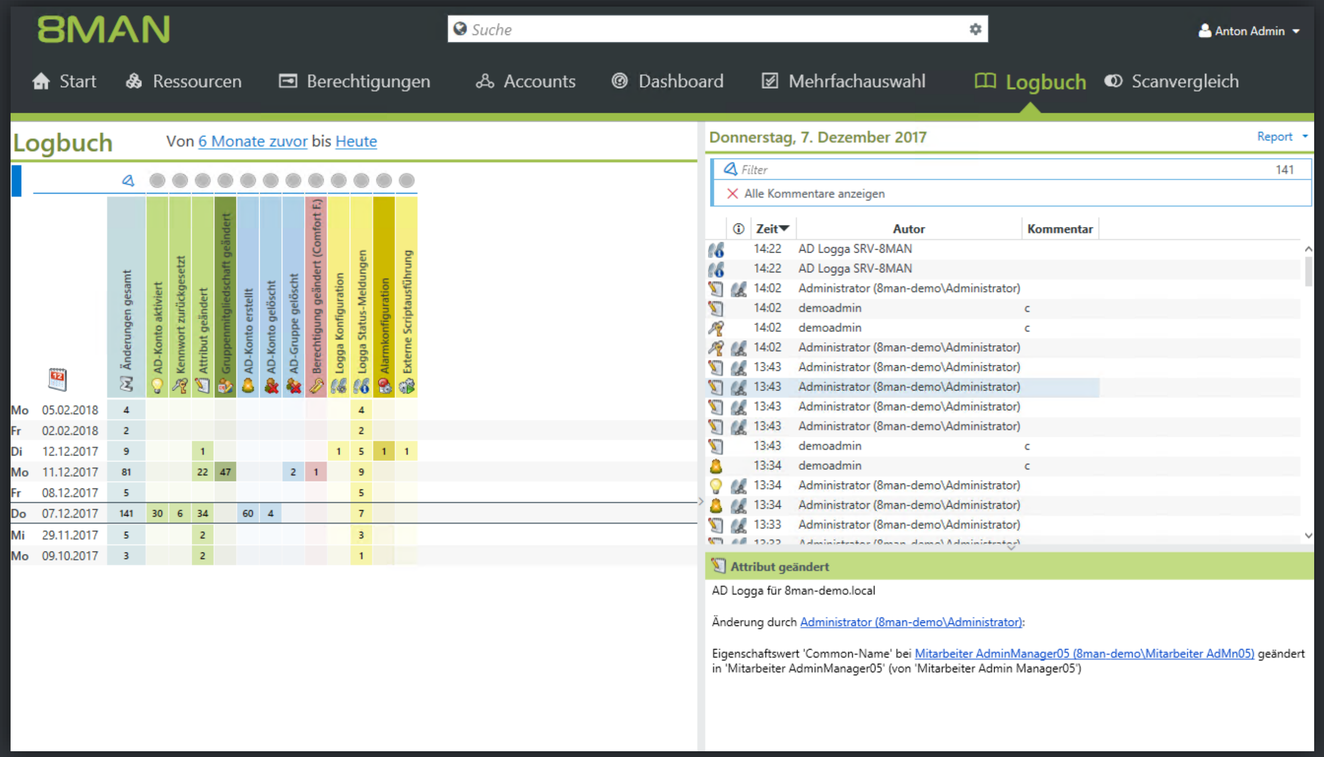
- Einfach in der Handhabung, dokumentiert mit deutschem Support und deutscher EULA
- Intuitiv und „entwickelt mit Kunden für Kunden“
- Konform mit: ISO / BSI / DSGVO
- Leicht konfigurierbar und einfach anzupassen an Kundenumgebungen

8MAN Logging:
Ganz gezieltes Erheben von Daten

TERRABIT IT-SOLUTIONS

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

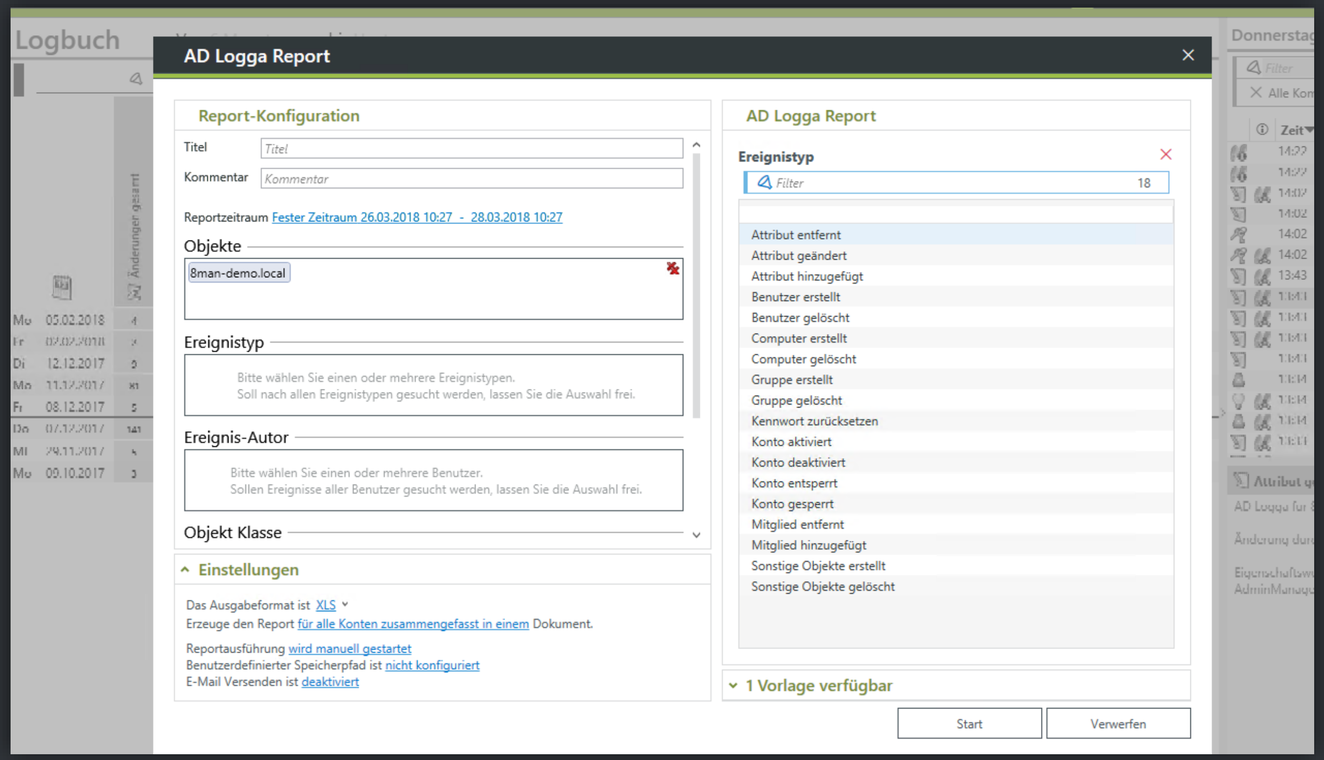
- Integriertes Logging mit Anzeige des Events im Rich Client
- Zurückversetzen / Kontext innerhalb zurückliegender Scans
- Einfaches und übersichtliches Reporting über Topologien
- Einfach einzurichten, übersichtliche Darstellung



TERRABIT IT-SOLUTIONS

Das sagen unsere Kunden – folgende Anforderungen muss eine Software für Berechtigungsmanagement abbilden:

- Direktes Reporting
- Übersicht der Änderungen über verschiedene Topologien
- Individuell konfigurier- und filterbar
- Einfach einzurichten, übersichtliche Darstellung



Fazit.

Learnings aus dem Projekt „One Person – One Identity“

Rückblickend sind folgende die bedeutendsten Learnings, die sich aus dem Projekt herauskristallisiert haben:

- ROI-Betrachtung: Für Auftraggeber überraschend, wie **enorm das zeitliche Einsparpotenzial** im standardisierten, softwarebasierten Joiner-Mover-Leaver-Prozess sowohl in der IT als auch im Non-IT-Bereich ist.

- Obligatorischer Zusammenhang zwischen Identity Management und Access Rights Management bzw. **User-Identity und Zugriffskonzept**

- **Interne IT** wird aus der Verantwortung gezogen, wenn fehlerhafte Berechtigungen vorliegen. Grund: Berechtigungsänderungen sind vollständig dokumentiert ist. Beugt falschen Verdächtigungen vor.

- IT-Mitarbeiter werden nicht unnötig geblockt, da automatisierte Tätigkeiten greifen und von den **Data-Ownern / Personal-Ownern** selbst vorgenommen werden.

Fazit.

Learnings aus dem Projekt „One Person – One Identity“

Rückblickend sind folgende die bedeutendsten Learnings, die sich aus dem Projekt herauskristallisiert haben:

- **Reputation der IT-Abteilung** im Unternehmen steigt: Interne IT stellt verlässliches Framework zur Verfügung, um Sicherheitsanforderungen einzuhalten.
- Deutliches **Plus an Daten-Sicherheit** im Unternehmen durch aktuell gehaltene Berechtigungen.
- Erweiterbarkeit für **3rd-Party-Applikationen.**
- Logging / Dokumentation: Wahrung der **DSGVO-Konformität**, ohne allerdings eine Komplett-Überwachung der User vorzunehmen und damit quasi alle Mitarbeiter unter Generalverdacht stellen.
- Design und Funktionalität der Access-Rights-Management Software sind ein **Schlüsselfaktor** zur erfolgreichen Umsetzung eines durchdachten Berechtigungsmanagements.

Q&A:
Ihre Fragen?

Wir stehen Ihnen gerne auch im Anschluss im Ausstellerbereich für Fragen und Antworten sowie Demos zur Verfügung.

Kontakt:

T: +49 7121 515 393 - 0 E: beratung@terrabit.de W: www.terrabit.de