

Access Rights Management. Only much Smarter.



## **Whitepaper DSGVO**

Wie Sie mit 8MAN Ihr Unternehmen absichern

8.0

© 2017 Protected Networks GmbH



## **Management Summary**

Die Datenschutzgrundverordnung (DSGVO) kommt und damit eine Reihe von neuen Anforderungen an Ihr Unternehmen. Neben den zentralen Informationen zur eigentlichen Regulatorik zeigt Ihnen das vorliegende Whitepaper, wie Sie mit 8MAN die zentralen Punkte der DSGVO umsetzen und damit Ihr Unternehmen sicher in die Zukunft führen. Die DSGVO dient dem Schutz personenbezogener Daten. Damit vertritt sie einerseits die Rechte von Verbrauchern und setzt andererseits Maßstäbe für den Schutz von Unternehmen.

Konkret schützt die Umsetzung Ihr Unternehmen vor Daten-, Informations- und Wissensdiebstahl. So wie Sie vertrauliche Papiere im Safe aufbewahren, sollten Sie auch mit Ihren digitalen Daten umgehen. Ohne Schutzvorkehrungen werden diese unerkannt kopiert und im schlimmsten Fall verkauft. Statt nur vom Datenschutz, sprechen Experten von einem Datenschatz. Diesen abzusichern, bedeutet gleichzeitig Ihr Unternehmen zu schützen.

Im Kapitel sechs dieses Whitepapers sind einige Prüffragen aufgeführt. Machen Sie den Test in Ihrem Unternehmen und prüfen Sie, wie schnell Ihre IT und die Geschäftsbereiche zufriedenstellende Antworten finden. Sollten Sie noch keine Lösung für ein professionelles Access Rights Management im Einsatz haben, freuen wir uns, Ihnen kostenfrei eine Teststellung von 8MAN anzubieten.

Kontaktieren Sie uns! Wir sind jederzeit bereit, 8MAN in Ihrem Unternehmen vorzuführen.

### Berlin im Juni 2017

### Herausgeber

Protected Networks GmbH

Alt-Moabit 73 10555 Berlin

+49 30 390 63 45 - 0

Protected-Networks.com 8MAN.com

### Support

+49 30 390 63 45 - 99

helpdesk@8man.com Knowledge Base

### **Knowledge Management**

Fabian Fischer

T: +49 30 390 63 45-41 T: +49 30 390 63 45-81

Sie haben Feedback?







**CEO Protected Networks** 



**Matthias Schulte-Huxel** 

Challes duly

**CSO Protected Networks** 

## Haftungsausschluss

Die in diesem Dokument gemachten Angaben können sich jederzeit ohne vorherige Ankündigung ändern und gelten als nicht rechtsverbindlich.

Die beschriebene Software 8MAN wird von Protected Networks im Rahmen einer Nutzungsvereinbarung zur Verfügung gestellt und darf nur in Übereinstimmung mit dieser Vereinbarung eingesetzt werden.

Dieses Dokument darf ohne die vorherige schriftliche Erlaubnis von Protected Networks weder ganz noch teilweise in irgendeiner Form reproduziert, übermittelt oder übersetzt werden, sei es elektronisch, mechanisch, manuell oder optisch.

Dieses Dokument ist in einer Einheit zu denen auf der Website von Protected Networks veröffentlichten rechtlichen Hinweisen AGB, EULA und der Datenschutzerklärung zu sehen.

### Urheberrecht

8MAN ist eine geschützte Bezeichnung für ein Programm und die entsprechenden Dokumente, dessen Urheberrechte bei Protected Networks GmbH liegen.

Marken und geschäftliche Bezeichnungen sind – auch ohne besondere Kennzeichnung – Eigentum des jeweiligen Markeninhabers.

Protected Networks GmbH Alt-Moabit 73 10555 Berlin

Berlin im Juni 2017

## Inhalt

1	Die DS	GGVO im Überblick	6
1.1	Zentra	le Anforderungen aus der DSGVO	8
1.2	Anforderungen an Ihr Access Rights Management		
1.3	Mit 8N	1AN zentrale DSGVO Anforderungen umsetzen	10
1.4	Die 8MAN Disziplinen im Detail		
2	Schritt	e für die Implementierung	. 13
2.1	Data O	wners nominieren und ihnen Ressourcen zuweisen	14
2.2	Person	enbezogene Daten lokalisieren und schützen	16
2.3	Zugriff	srechte auf die personenbezogenen Daten reduzieren	17
2.4	Verzeichnisse und Gruppen mit Hilfe des Security Monitorings überwachen		
2.5	Die Sic	herheitsrollen im Unternehmen automatisiert mit Reporten involvieren	18
2.6	Die Berechtigungssituation für Verzeichnisse mit personenbezogenen Daten im Blick behalten		18
2.7		chnisberechtigungen vor dem Abteilungswechsel oder Unternehmensaustritt nen	19
3	Anhang		. 21
3.1	Dokum	entation benötigter Services	22
	3.1.1	Einen Data Owner nominieren und ihm Ressourcen zuweisen	22
	3.1.1.1	Organisationskategorien erstellen	22
	3.1.1.2	Einer Organisationskategorie einen Data Owner zuweisen	23
	3.1.1.3	Einer Organisationskategorie Ressourcen zuweisen	25
	3.1.2	Einen einfachen Leseaccount in 8MAN anlegen	26
	3.1.3	Gruppen anlegen und Benutzer hinzufügen	28
	3.1.4	Mehrfachberechtigungen auf Verzeichnissen entfernen	31
	3.1.5	Wo haben Benutzer/Gruppen Zugriff?	35
	3.1.6	Wer hat wo Zugriff?	36
	3.1.7	Data Owner: Bestehende Zugriffsrechte rezertifizieren	39
	3.1.7.1	E-Mail Aufforderungen zur Rezertfizierung	42
	3.1.7.2	Rezertifizierung aktivieren und deaktivieren	43
	3.1.8	Verzeichnisberechtigungen für Mitarbeiter erteilen und entziehen	43
	3.1.9	Die Zugriffe auf sensible Daten überwachen	48
	3.1.10	Alarme für AD Konten und Gruppen anlegen	51
	3.1.11	Reporte automatisch zusenden lassen	54
	3.1.12	Die Zugriffe auf sensible Daten überwachen	57



	3.1.13 Berechtigungen im Webclient entfernen	. 60
4	Über 8MAN	
4.1	Prüffragen an Ihre IT und Geschäftsbereiche	. 66
4.2	Kontakt	. 67
Stich	nwörter	0

# 1. Die DSGVO im Überblick





Mit der DSGVO regelt die Europäische Kommission die Verarbeitung personenbezogener Daten. Die Verordnung trat am 25.05.2016 in Kraft und wird zum 25.05.2018 geltendes Recht. Damit wird die aus dem Jahr 1995 stammende Datenschutz-Richtlinie 95/46/EG vollkommen ersetzt. Als supranationales EU-Recht wirkt die Regulation unmittelbar und bedarf keiner weiteren nationalen Beschlüsse.

Damit verfolgt die Kommission Datenschutzverstöße mit immer mehr Nachdruck. Ausdruck der Ernsthaftigkeit der EU-Initiative sind die neuen Bußgelder bei Verstoß gegen die Regulierung. Rangierten die Strafzahlungen vor der Novelle zwischen 50.000 und 300.000 Euro, erhebt die EU mit der DSGVO bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes (DSGVO Art. 83 Abs. 4 und Abs. 5).

Das Datenschutzrecht bietet jeder in der EU sich aufhaltenden, natürlichen Person Schutz vor der Verarbeitung ihrer Daten und reguliert Unternehmen und Institutionen weltweit bei der Handhabung personenbezogener Daten.

Personenbezogene Daten zeichnen sich durch einen Bezug zwischen der Person und einer anderen Person, Sache oder einem Ereignis aus. Konstitutiv für personenbezogene

Daten ist die Möglichkeit die Daten einer bestimmten Person zuzuordnen. Beispiele für personenbezogene Daten sind Kfz-Kennzeichen, Kontonummern, Rentenversicherungsnummern,

Matrikelnummern, E-Mail- und IP Adressen. Maßgeblich für die Gültigkeit der Novelle ist nicht der Standort des Unternehmens, sondern der Aufenthaltsort der Person, deren Daten erfasst wurden.

### 1.1 Zentrale Anforderungen aus der DSGVO

Die DSGVO ist komplex. Sie verfügt über insgesamt elf Kapitel, die wiederum in 99 Artikel aufgegliedert sind. Experten diskutieren vor allem die Artikel 5 und 32. Diese repräsentieren die zentralen Neuanforderungen der DSGVO im Vergleich zu vorherigen Datenschutzrichtlinien.

\_\_\_\_\_

## Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten



- (1) Abschnitt e) Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("Integrität und Vertraulichkeit");
- (2) Der Verantwortliche ist für die Einhaltung des § 1 verantwortlich und muss dessen Einhaltung nachweisen können ("Rechenschaftspflicht").

### Artikel 32: Sicherheit der Verarbeitung

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.



## 1.2 Anforderungen an Ihr Access Rights Management

Die Artikel 5 und 32 implizieren eine Reihe von Anforderungen an das Access Rights Management in Ihrem Unternehmen.

\_\_\_\_\_

### **Artikel 5: Implizite Anforderungen**

- **1. Datensicherheit und Integrität herstellen:** Ressourcen, die personenbezogene Daten erhalten, dürfen nur vertrauenswürdigen Personen zugänglich sein. Ferner müssen die Verzeichnisse einem kontinuierlichen Monitoring unterliegen. Damit ist gewährleistet, dass Kopiervorgänge und Modifikationen an den Dateien jederzeit nachvollziehbar sind. Im Falle eines Sicherheitsvorfalls sind sowohl die Geschäftsbereiche als auch die IT auskunftsfähig und in der Lage den Vorfall aufzuklären.
- **2. Dokumentation von Zugriffsrechten:** Insbesondere die im Artikel 5 Absatz 2 festgehaltene Rechenschaftspflicht fordert von datenverarbeitenden Institutionen jederzeit verzeichnisgenau die Zugriffsrechtehistorie und das tatsächliche Zugriffsverhalten aus der Vergangenheit nachweisen zu können.
- **3. Pflege der Berechtigungssituation**: Insbesondere im Joiner, Mover und Leaver Prozess (also dem Lebenszyklus eines Nutzerkontos im Firmennetzwerk) müssen die IT und die Fachabteilungen die Berechtigungen des Mitarbeiters im Blick behalten und sehr schnell ändern können. Datendiebstahl erfolgt meist in der Leaver-Phase. Zu diesem Zeitpunkt muss die Fachabteilung dem Mitarbeiter alle Zugriffsrechte auf sicherheitskritische Verzeichnisse entzogen haben.

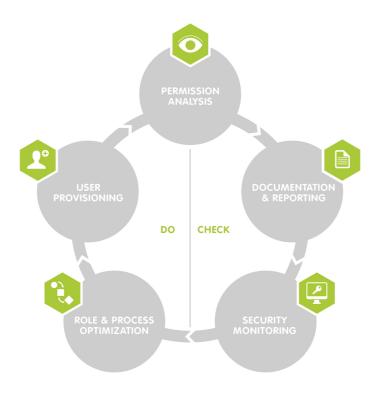
### **Artikel 32: Implizite Anforderungen**

**4. Data Owners einführen:** Die DSVGO fordert klare Verantwortlichkeiten im Umgang mit personenbezogenen Daten. Dazu ist die Einführung der Rolle "Data Owner" zentral. Data Owners sind Führungskräfte, die innerhalb ihrer Abteilung über Daten wachen. Sie wissen welche Verzeichnisse geschützt werden müssen und welche Mitarbeiter vertrauenswürdig sind. Die Einführung von neuen Rollen, wie die des Data Owners, verlangt gleichzeitig nach neuen Prozessen der Zusammenarbeit und der Dokumentation vorgenommener Aktivitäten.

© 2017 Protected Networks GmbH

### 1.3 Mit 8MAN zentrale DSGVO Anforderungen umsetzen

8MAN verfügt über fünf zentrale Disziplinen. Diese bilden in ihrer Gesamtheit ein klares und schnell zu implementierendes System für ein DSGVO konformes Access Rights Management.



### **PERMISSION ANALYSIS**

Zeigt ressourcenübergreifend die Berechtigungssituation in Ihrem Unternehmen.

### **DOCUMENTATION & REPORTING**

Erfasst Access Rights Aktivitäten im Logbuch und erstellt revisionssichere Reporte.

### **SECURITY MONITORING**

Überwacht sicherheitsrelevante Aktionen im Active Directory und auf Ihren Fileservern.

### **ROLE & PROCESS OPTIMIZATION**

Verkürzt Ihren Access Rights Management Prozess und involviert nur die notwendigen Akteure.

### **USER PROVISIONING**

Regelt die Anlage neuer Nutzerkonten, die Rechteverwaltung und die Bearbeitung von Kontodetails.



#### Die 8MAN Disziplinen im Detail 1.4



Zentral für die Erfüllung der zentralen DSGVO-Anforderungen ist Permission Analysis. 8MAN zeigt die Berechtigungssituation in Ihrem Netzwerk bidirektional: Entweder wählen Sie eine Ressource mit personenbezogenen Daten und lassen sich anzeigen, wer darauf Zugriff hat oder Sie lassen sich die Zugriffsrechte eines Nutzers auf sämtliche Ressourcen anzeigen. Mit diesem Wissen ist die Anforderung (1) "Datensicherheit und Integrität herstellen" schnell umsetzbar.



Die Zugriffsrechtesituation, die Aktivitäten in den geschützten Verzeichnissen und die Praxis der Berechtigungsvergabe bereitet Documentation & Reporting für Sie in einfach lesbaren und strukturierten Reporten auf. Diese lassen sich automatisiert und verzeichnisspezifisch an die beteiligten Rollen im Unternehmen versenden. Die Anforderung (2) "Dokumentation von Zugriffsrechten" ist damit automatisch erfüllt.



Neben der Zugriffsrechtesituation sind vor allem die tatsächlichen Vorgänge mit den personenbezogenen Daten relevant. Mit dem Security Monitoring vertiefen Sie das Sicherheitsniveau und erfassen Aktivitäten innerhalb der Verzeichnisse, in denen die personenbezogenen Daten gespeichert sind. Darüber hinaus erfasst die AD Analyse auch außerhalb von 8MAN vorgenommene Änderungen an der Berechtigungssituation. Damit sind temporäre Gruppenmitgliedschaften und daraus resultierende unkontrollierte Berechtigungsvergaben sofort nachvollziehbar. 8MAN informiert Sie proaktiv über die Alerts Funktion, sollte jemand versuchen, die Sicherheitsgruppe zu manipulieren.



8MAN bietet mit Role & Process Optimization eine Reihe von Best Practice Prozessen, deren Implementierung für ein DSGVO-konformes Access Rights Management essentiell ist. Die Kontrolle und Pflege von Zugriffsrechten auf personenbezogene Daten muss prozessual im Unternehmen definiert sein. Role & Process Optimization schafft dafür den geeigneten Rahmen. Zentral ist in der Konzeption die Rolle des Data Owners: Anforderung (4) "Data Owners einführen". Die Führungskraft wacht über die Zugriffsrechtesituation im eigenen Bereich und entscheidet, wer auf die personenbezogenen Daten Zugriff haben soll. Im Rahmen einer periodischen Rezertifizierung kann der Data Owner – auch ohne weitreichende IT Kenntnisse – Berechtigungen entfernen oder bestehen lassen.



Auch bei einer vierteljährlich gesetzten Rezertifizierung bleibt die Adhoc-Pflege der Berechtigungssituation eine wichtige Anforderung. Verlässt ein Mitarbeiter das Unternehmen, müssen frühzeitig seine Zugriffsrechte auf personenbezogene Daten bzw. sonstiges Unternehmenwissen entfernt werden. Dies erfolgt durch den Data Owner oder Administrator via Drag & Drop im **User Provisioning**. Anforderung (3): Pflege der Berechtigungssituation.



# 2. Schritte für die Implementierung



## 14 | Whitepaper DSGVO

Das folgende Kapitel zeigt Ihnen die wichtigsten Schritte auf dem Weg zu einem DSGVO konformen Access Rights Management. Die Dokumentation der genannten Services finden Sie im <u>Anhang dieses Dokumentes</u>.

### 2.1 Data Owners nominieren und ihnen Ressourcen zuweisen

Um die IT-Sicherheit Ihrer personenbezogenen Daten zu erhöhen, ist es notwendig die entsprechenden Strukturen in Ihrem Unternehmen zu verankern. Ziel ist es, die Sicherheitskompetenz im Unternehmen zu dezentralisieren. Nominieren Sie dazu Data Owners in den Bereichen, wo personenbezogene Daten verwendet werden. In der Regel zählt dazu der Einkauf, Vertrieb und natürlich die Personalabteilung.

### DATA OWNERS, DATENSCHUTZBEAUFTRAGTE UND DER AUDITOR

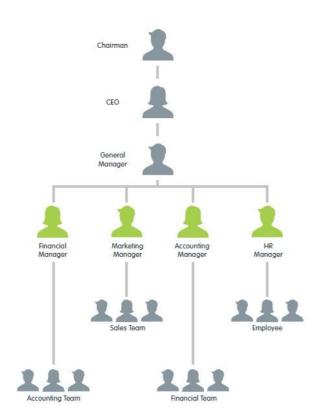
Typischerweise ernennen Geschäftsführer Ihre Abteilungsleiter zu Data Owners. Sie kennen die schützenswerten Daten ihrer Abteilung und wissen, wer darauf Zugriff haben sollte.

Der Data Owner ist die "First Line of Defense". Er reportet an den Datenschutzbeauftragten und wird über weitere Rechte und Pflichten durch ihn beraten ("Second Line of Defense").

Die "Third Line of Defense" ist üblicherweise das interne oder externe Audit. Sowohl der Datenschutzbeauftragte als auch der interne Auditor sollten durch automatisierte Reporte regelmäßig über die Berechtigungssituation informiert werden. Alternativ können Sie den Sicherheitsrollen im Unternehmen auch einen Lese-Account in 8MAN anlegen (D013).



### Data Owners: Sicherheitskompetenz im Unternehmen verteilen





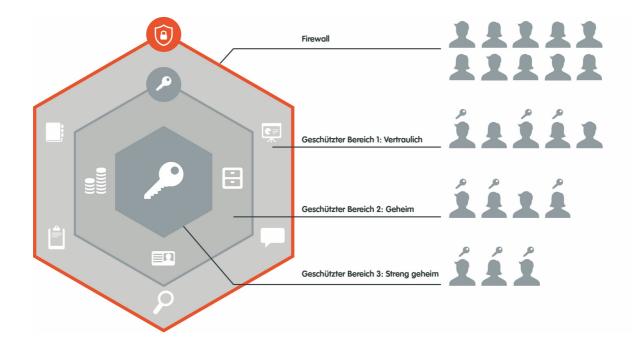
Data Owners sind Führungskräfte in der Organisation. Sie wachen über sicherheitsrelevante Daten.

### Auszuführende(r) Service(s):

D002 Einen Data Owner definieren und ihm Ressourcen zuweisen

D013 Einen 8MAN Account für eine Sicherheitsrolle anlegen

### 2.2 Personenbezogene Daten lokalisieren und schützen



Jeder Data Owner durchsucht im nächsten Schritt seine zugewiesenen Ressourcen nach personenbezogenen Daten. Sollten sich diese in unterschiedlichen Verzeichnisbäumen befinden, empfehlen wir die Daten zentral zu speichern. Personenbezogene Daten gehören zum "Geschützten Bereich 2".

Nur wenige Mitarbeiter sollten darauf zugreifen können.



## 2.3 Zugriffsrechte auf die personenbezogenen Daten reduzieren

Erstellen Sie eine AD Sicherheitsgruppe und berechtigen Sie darüber alle zugriffsberechtigten Personen auf das sicherheitskritische Verzeichnis (E001). Anschließend identifizieren Sie etwaige Mehrfachberechtigungen und entfernen diese, sodass der Zugriff auf das Verzeichnis nur durch die Sicherheitsgruppe erfolgen kann (E017). Entfernen Sie anschließend die Zugriffsrechte von Personen, die nicht zwingend Einblick in die personenbezogenen Daten brauchen (E015). Hierbei gilt das "Principle of least Privilege". Es besagt, dass sicherheitsrelevante Daten nur den Personen zugänglich seien sollte, die auf deren Verarbeitung wirklich angewiesen sind.

### Auszuführende(r) Service(s):

E001 <u>Gruppen anlegen und Benutzer</u> <u>hinzufügen</u>

E017 Mehrfachberechtigungen auf Verzeichnissen entfernen

E015 <u>Verzeichnisberechtigungen für</u> <u>Mitarbeiter erteilen und entziehen</u>

# 2.4 Verzeichnisse und Gruppen mit Hilfe des Security Monitorings überwachen

Im nächsten Schritt wenden Sie das Security Monitoring an. Liegen Ihre personenbezogenen Daten auf dem Fileserver, empfehlen wir die tatsächlichen Zugriffe auf das Verzeichnis regelmäßig zu analysieren (C009). Senden sie den Report mit den Dateizugriffen automatisiert an den Datenschutzbeauftragten und die interne Revision. Damit involvieren Sie ohne weiteres Zutun die weiteren Sicherheitsrollen in ihrem Unternehmen. Ihre AD Gruppe sichern Sie mit der Alerts Funktion ab (C005). Sollte jemand diese Manipulieren, erhält der Data Owner, Datenschutzbeauftragte und Geschäftsführer sofort einen E-Mail Alert.

### Auszuführende(r) Service(s):

C009 <u>Die Zugriffe auf sensible Dateien</u> <u>ermitteln</u>

C005 <u>Alarme für AD Konten und Grup-</u> pen anlegen, bearbeiten und löschen

## 2.5 Die Sicherheitsrollen im Unternehmen automatisiert mit Reporten involvieren

Die Reporte über die Berechtigungssituation oder über die Dateizugriffe auf personenbezogene Daten sollten periodisch dem Datenschutzbeauftragten und dem internen Auditor zur Verfügung gestellt werden. 8MAN erlaubt es, die Reporte verzeichnisspezifisch zu definieren und automatisiert den Beteiligten via E-Mail zu senden (D020). Insbesondere die Services (B034, B014, C009) sind dabei zentral.

### Auszuführende(r) Service(s):

D020 Reporte automatisch zusenden lassen

B034 Wo haben Benutzer / Gruppen Zugriff? (Fokus Verzeichnis)

B014 Wer hat wo Zugriff? (Fokus Mitarbeiter)

C009 <u>Die Zugriffe auf sensible Dateien</u> <u>überwachen</u>

# 2.6 Die Berechtigungssituation für Verzeichnisse mit personenbezogenen Daten im Blick behalten

Die Berechtigungen auf sicherheitskritische Verzeichnisse müssen regelmäßig durch die Data Owners geprüft werden. Die durch den Administrator zu aktivierende 8MAN Rezertifizierungs-funktion (D023) fordert die Data Owners periodisch zur Einhaltung ihrer Prüfpflicht auf. In einer einfachen Ansicht können Sie schnell und verzeichnisspezifisch die Zugriffsrechte entweder bestehen lassen oder entziehen (D024).

### Auszuführende(r) Service(s):

D023<u>Den Rezertifizierungsprozess aktivieren (Administrator)</u>
D024 <u>Bestehende Zugriffsrechte rezertifizieren (Data Owner)</u>



## 2.7 Verzeichnisberechtigungen vor dem Abteilungswechsel oder Unternehmensaustritt entfernen

Sobald ein Mitarbeiter die Abteilung wechselt, bedarf es eines sofortigen Entzugs seiner abteilungsspezifischen Zugriffsrechte. Dies können Data Owners bequem im Webclient erledigen. In der "Leaver-Phase" gilt: Je früher die Berechtigungen auf sicherheitskritische Verzeichnisse entfernt werden (E052), desto besser.

### Auszuführende(r) Service(s):

E052 <u>Berechtigungen im Webclient</u> <u>entfernen</u>



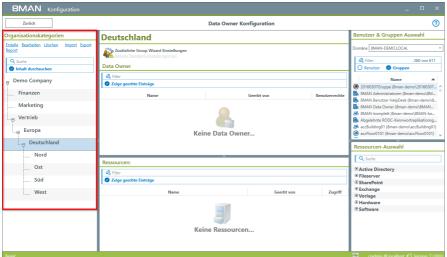
# 3. Anhang



### **Dokumentation benötigter Services** 3.1

#### 3.1.1 Einen Data Owner nominieren und ihm Ressourcen zuweisen

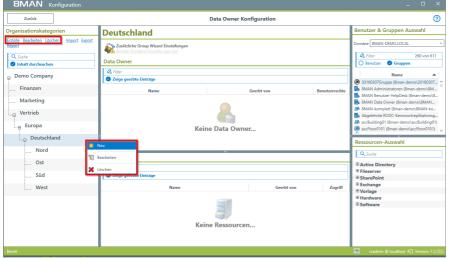
#### 3.1.1.1 Organisationskategorien erstellen



Mit den Organisationskategorien bilden Sie die Einheiten (Container), welche die Data Owner verwalten.

Sie können Strukturen und Hierarchien erstellen, ähnlich dem Organigramm Ihres Unternehmens.

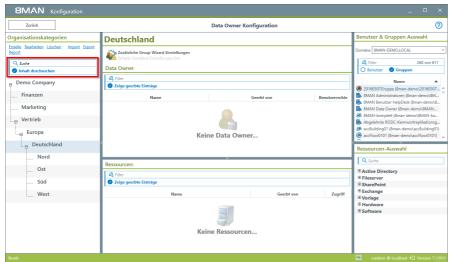
Sie können jeder Organisationskategorie eine Beschreibung hinzufügen.



Erstellen Sie beliebig viele Organisationskategorien. Benutzen Sie dazu die Symbole im oberen Bereich oder das Kontextmenü nach Rechtsklick.

Sie können Organisationskategorien per Drag&Drop verschieben.





Sie können die Organisationskategorien durchsuchen.

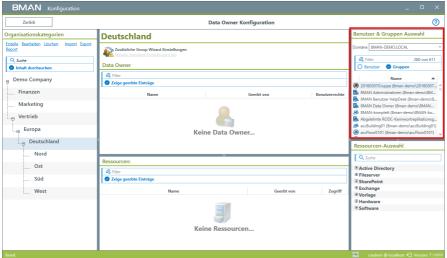
### Option "Inhalt durchsuchen" deaktiviert:

Suchen Sie nur in den Namen und Beschreibungen der Organisationskategorien.

### Option "Inhalt durchsuchen" aktiviert:

Suchen Sie zusätzlich nach Data Ownern und Ressourcen.

### Einer Organisationskategorie einen Data Owner zuweisen 3.1.1.2



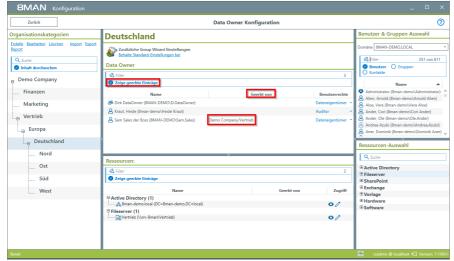
Wählen Sie einen Benutzer oder eine Gruppe mit Doppelklick oder per Drag&Drop.



Data Owner müssen eine "Ändern" oder die "Lesen" Benutzerrolle in der 8MAN Benutzerverwaltung haben. 8MAN-Admins können nicht als Data Owner konfiguriert werden.

Wenn Sie Data Owner zuweisen wollen, welche die erforderliche Rolle nicht besitzen, wird dieser Dialog angezeigt.

Mit einem Klick auf "Anwenden" erhalten die Benutzer die erste "Ändern Zugriff" Rolle.
Sie können die Rolle nachträglich ändern.



Hierarchie-Regel:

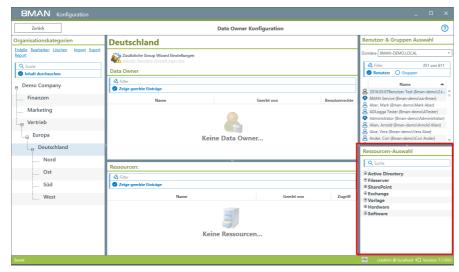
Data Owner können die zugewiesene Organisationskatgeorie und alle **darunter** liegenden verwalten (von oben nach unten).

Aktivieren Sie die Option "Zeige geerbte Einträge", um geerbte Einträge anzuzeigen.

Die Spalte "Geerbt von" zeigt die Herkunft.



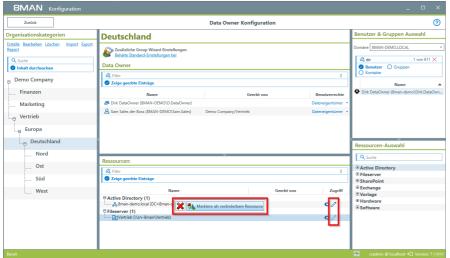
#### Einer Organisationskategorie Ressourcen zuweisen 3.1.1.3



Wählen Sie eine Ressource und fügen Sie mit Doppelklick oder per Drag&Drop zur selektierten Organisationskategorie hinzu. Sie können nur Ressourcen verwenden, für die ein Scan ausgeführt wurde.

Open Order Ressourcen (hier "Vorlage", "Hardware", "Software" können Sie zuweisen, wenn Sie

- eine entsprechende Lizenz eingespielt haben und
- eine Open Order Konfiguration importiert haben.

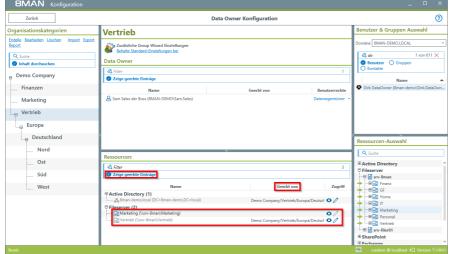


Wenn Sie Ressourcen hinzugefügt haben, sind diese zunächst nur lesend verwaltbar.

Wählen Sie eine Ressource und klicken auf die Ändern- Schaltfläche, um den Data Owners das Ändern zu ermöglichen.

### Beachten Sie:

Wenn der Group Wizard aktiviert ist und Data Owner Änderungen vornehmen sollen, muss auch immer eine entsprechende Active Directory Ressource mit Ändern-Zugriff zugewiesen werden. Andernfalls kann der Group Wizard keine AD-Gruppen erstellen.



Hierarchie-Regel:

Ressourcen sind in der zugewiesenen Organisationskategorie und allen **darüber** liegenden verfügbar (von unten nach oben, entgegengesetzt der Data Owner und NTFS-Rechte-Vererbung).

Aktivieren Sie die Option "Zeige geerbte Einträge", um "geerbte" Einträge ausgegraut anzuzeigen.

Die Spalte "Geerbt von" zeigt die Herkunft.

## 3.1.2 Einen einfachen Leseaccount in 8MAN anlegen

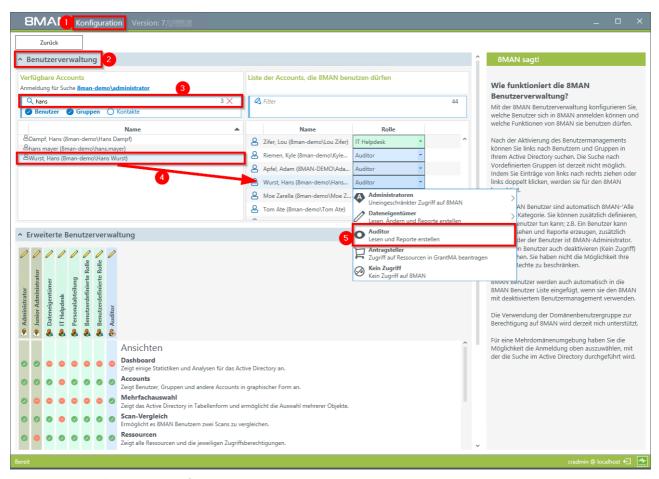
### **Hintergrund / Mehrwert**

Involvieren Sie Sicherheitskräfte in das Access Rights Management, indem Sie einen Zugang mit Leserechten vergeben. Damit kann die jeweilige Person auch ihre eigenen Reporte erstellen.

Die Einstellungen nehmen Sie in der 8MAN Konfigurationsoberfläche vor. Sie finden detaillierte Informationen im Handbuch für Installation und Konfiguration, Kapitel 8MAN Benutzer verwalten ff.



### Der Prozess in einzelnen Schritten



- 1. Starten Sie die 8MAN Konfiguration.
- 2. Wechseln Sie zu "Benutzerverwaltung".
- 3. Nutzen Sie die Suche, um den gewünschten Account zu finden.
- 4. Ziehen Sie den Account per Drag&Drop in die rechte Spalte.
- 5. Wählen Sie in der Spalte Rolle "Auditor".

Die Einstellungen sind sofort wirksam.

#### Gruppen anlegen und Benutzer hinzufügen 3.1.3

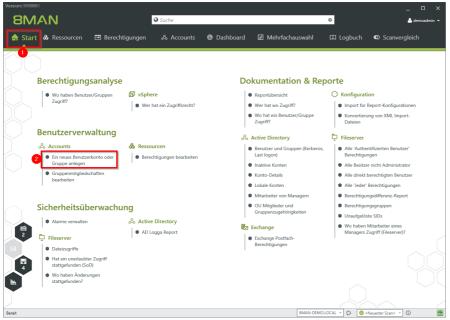
### **Hintergrund / Mehrwert**

Mit 8MAN legen Sie schnell und standardisiert Gruppen an. Der Prozess wird automatisch dokumentiert.

### Weiterführende Services

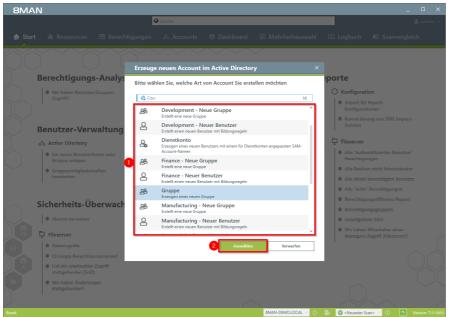
Gruppenmitgliedschaften bearbeiten

### Der Prozess in einzelnen Schritten



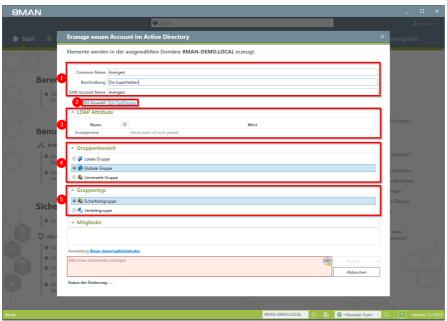
- 1. Wählen Sie "Start".
- 2. Klicken Sie auf "Ein neues Benutzerkonto oder Gruppe anlegen".



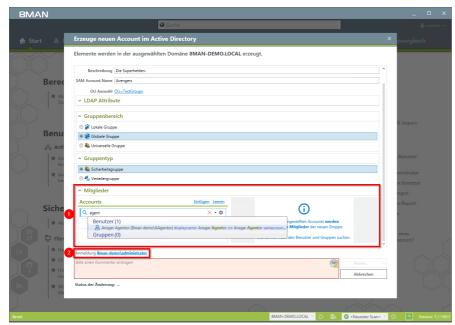


8MAN bietet nach Erstinstallation vier Standardvorlagen. Sie können unbegrenzt viele, an Ihre Bedürfnisse angepasste Vorlagen erstellen. Wir empfehlen, angepasste Vorlagen zu verwenden, da sich dadurch der Anlagevorgang vereinheitlichen und deutlich beschleunigen lässt.

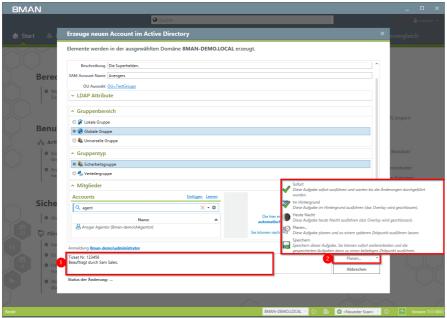
- 1. Wählen Sie eine Gruppen-Vorlage.
- 2. Klicken Sie "Auswählen".



- 1. Geben Sie die Stammdaten ein.
- 2. Ändern Sie ggf. die OU.
- 3. Ergänzen Sie weitere LDAP Attribute.
- 4. Legen Sie den Gruppenbereich (group scope) fest.
- 5. Legen Sie den Gruppentyp fest.



- Sie können bereits bei der Gruppenanlage Mitglieder festlegen.
- 2. Geben Sie an, mit welchen Anmeldeinformationen die neue Gruppe im AD angelegt wird.



1. Sie müssen einen Kommentar eingeben.

Sicherheitsrelevante Ereignisse, wie die Erstellung eines Nutzerkontos sollten vom Ersteller immer begründet werden. Dies dient auch der eigenen Absicherung. Wir empfehlen, eine Ticketnummer und den Beauftrager zu hinterlegen.

2. Führen Sie die Anlage sofort oder später aus, oder speichern Sie die Aufgabe und beenden sie später.



### Mehrfachberechtigungen auf Verzeichnissen entfernen 3.1.4

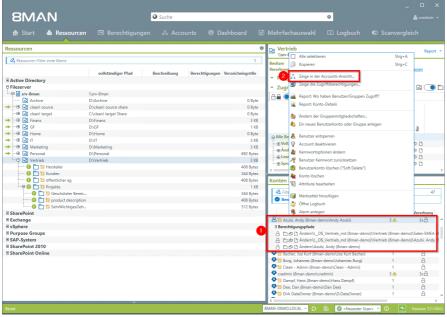
### **Hintergrund / Mehrwert**

Mehrfachberechtigungen kommen über die Mitgliedschaft mit verschachtelten Gruppen im AD zustande. Sie sind Ausdruck einer unsauberen Gruppenstruktur. Denn: Eine Berechtigung sollte sich nur aus einer Gruppenmitgliedschaft ergeben. Mit 8MAN können Sie Mehrfachberechtigungen schnell entfernen.

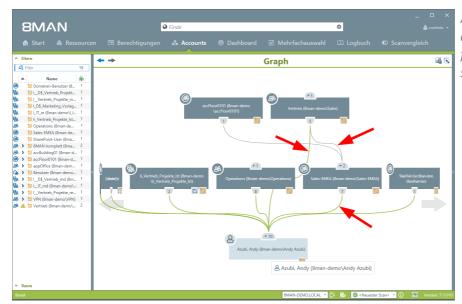
### Weiterführende Services

Mehrfachberechtigungen auf Verzeichnissen identifizieren

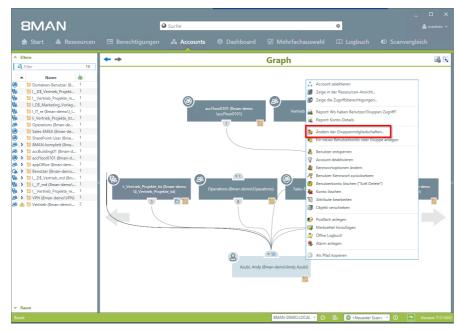
### Der Prozess in einzelnen Schritten



- 1. Sie haben für "Andy Azubi" Mehrfachberechtigungen identifiziert.
- 2. Rechtsklicken Sie auf den Account und wählen "Zeige in der Accounts-Ansicht..." im Kontextmenü.

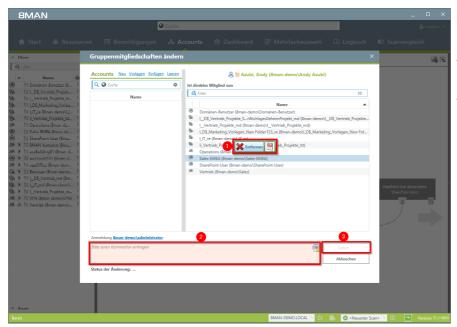


Analysieren Sie mit dem Account-Graphen, wie die Mehrfachberechtigungen aufgebaut

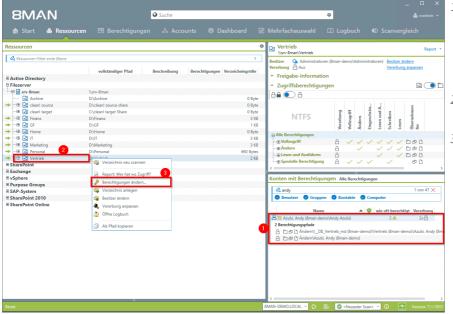


Rechtsklicken Sie den Account und wählen "Ändern der Gruppenmitgliedschaften..." im Kontextmenü.

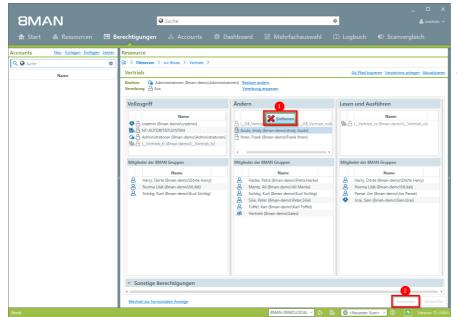




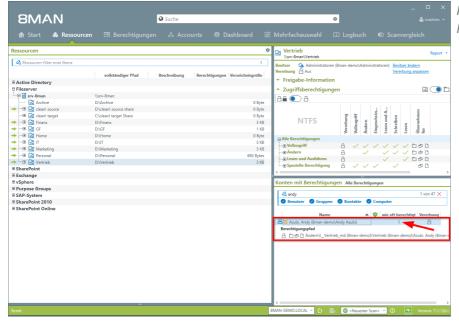
- 1. Entfernen Sie die Gruppenmitgliedschaft.
- 2. Sie müssen einen Kommentar eingeben.
- 3. Starten Sie die Ausführung.



- 1. Nach dem Entfernen der überflüssigen Gruppenmitgliedschaften bleibt noch die zusätzliche Direktberechtigung.
- 2. Selektieren Sie das Verzeichnis mit Rechtsklick.
- 3. Wählen Sie im Kontextmenü "Berechtigungen ändern...".



- 1. Selektieren Sie den betreffenden Benutzer und wählen "Entfernen".
- 2. Starten Sie das Entfernen.



Prüfen Sie das Resultat in der Ressourcenansicht.

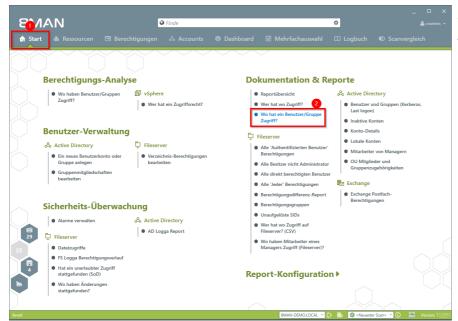


#### Wo haben Benutzer/Gruppen Zugriff? 3.1.5

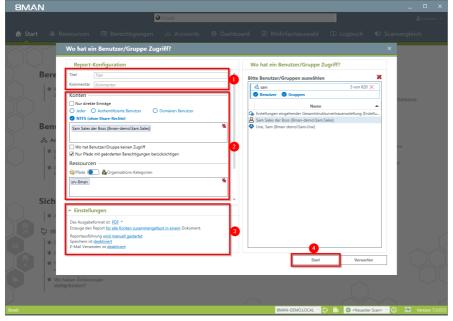
### **Hintergrund / Mehrwert**

Der Report "Wo hat ein Benutzer/Gruppe Zugriff?" listet die Zugriffsrechte von Nutzerkonten und Gruppen auf ausgewählten Fileserver-Verzeichnissen in einem Dokument auf.

### Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Start"
- 2. Klicken Sie auf "Wo hat eine Benutzer/Gruppe" Zugriff?



- 1. Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.
- 2. Definieren Sie den Umfang des Reports.
- 3. Legen Sie verschiedene Ausgabeoptionen fest.
- 4. Starten Sie die Erstellung des Reports.

### 3.1.6 Wer hat wo Zugriff?

### **Hintergrund / Mehrwert**

Führungskräfte wissen am besten, wer worauf Zugriff haben sollte. Insbesondere für sensible Fileserververzeichnisse muss vollständig Transparenz bestehen. Der Report "Wer hat wo Zugriff?" bietet eine vollständige Übersicht über alle Rechte (z. B. "Lesen" und "Schreiben") und Personen, die diese Rechte auf dem Verzeichnis ausüben können.

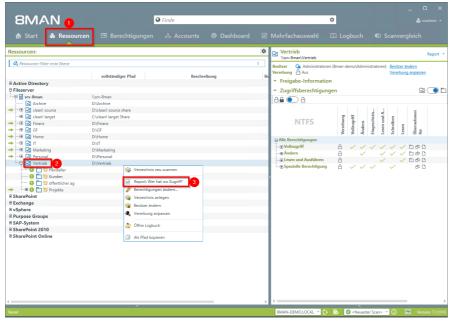
Der Report gibt der verantwortlichen Führungskraft eine Entscheidungsgrundlage, um zwei zentrale Fragen zu beantworten:

- Wer sollte Zugriff haben? (Erhöhung der Datensicherheit)
- Welche Zugriffsrechte sollten bestehen? (Erhöhung von Datenintegrität)

### Weiterführende Services

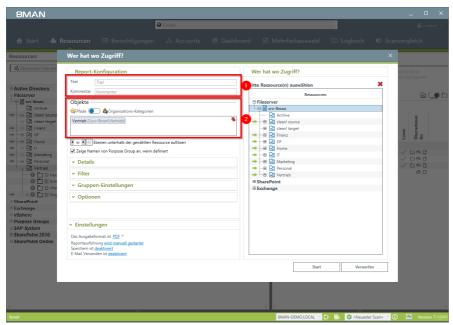
Verzeichnisberechtigungen ändern

### Der Prozess in einzelnen Schritten

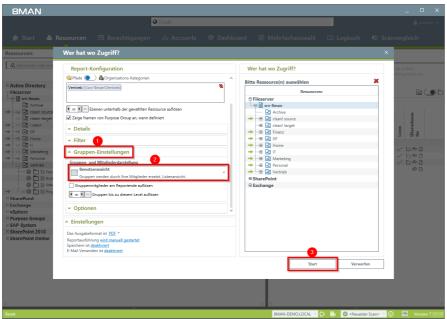


- 1. Wählen Sie "Ressourcen".
- Selektieren Sie mit Rechtsklick ein Verzeichnis, für das Sie verantwortlich sind
- Klicken Sie im Kontextmenü auf "Report: Wer hat wo Zugriff?".

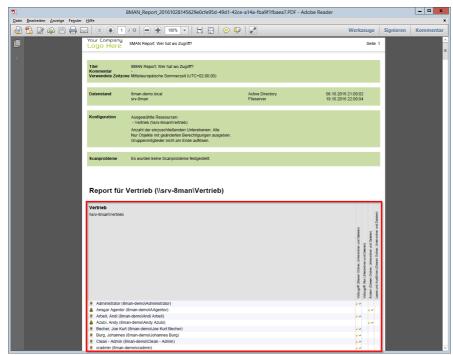




- 1. Geben Sie dem Report einen Titel und fügen Sie einen Kommentar hinzu.
- 2. Das eben gewählte Verzeichnis ist automatisch Teil der Objekte, die untersucht werden sollen. Sie können weitere Ressourcen hinzufügen.



- 1. Klappen Sie "Gruppen-Einstellungen" auf.
- 2. Zur Komplexitätsreduktion empfehlen wir "Benutzeransicht" zu wählen. Die restlichen Einstellungen richten sich an Experten.
- 3. Starten Sie die Reporterstellung.



Prüfen Sie, ob die aufgelisteten Nutzer Zugriff haben sollten. Im zweiten Schritt sollten Sie prüfen, ob es für einige Nutzer nicht reicht, die Rechte von "Vollzugriff" auf "Lesen und Ausführen" herabzusetzen. Damit erreichen Sie eine höhere Datenintegrität.



#### 3.1.7 Data Owner: Bestehende Zugriffsrechte rezertifizieren

## **Hintergrund / Mehrwert**

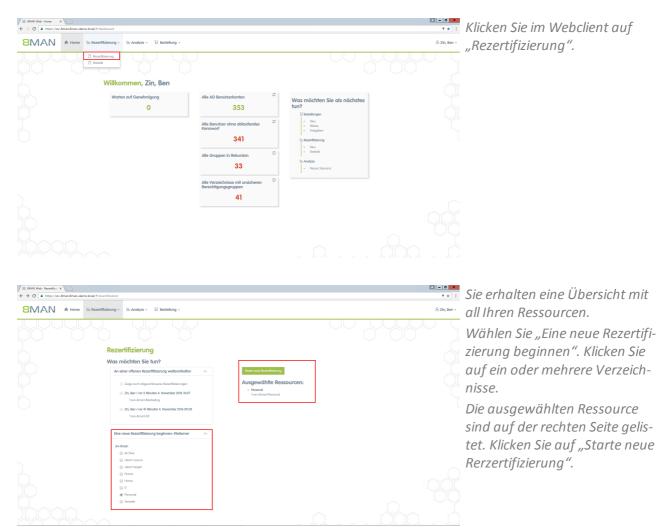
Sicherheitsregularien fordern die Einhaltung des Least-Privilege-Prinzips. Dazu prüfen Sie als Data Owner in regelmäßigen Abständen die Berechtigungssituation auf Ihre Ressourcen. Im Rahmen der 8MAN Rezertifizierung erhalten Sie eine E-Mail und gelangen in eine einfache Ansicht, in der alle Ressourcen und Zugriffsberechtigte aufgelistet sind. Sie müssen dann für jede Ressource entscheiden, ob das Zugriffsrecht belassen oder entfernt werden soll.

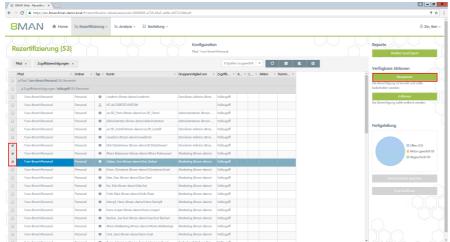
Ihre Änderungswünsche werden nach Abschluss an den zuständigen Administrator übermittelt.

#### Weiterführende Services

Verzeichnisberechtigungen ändern

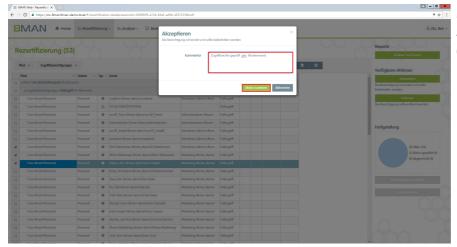
#### Der Prozess in einzelnen Schritten



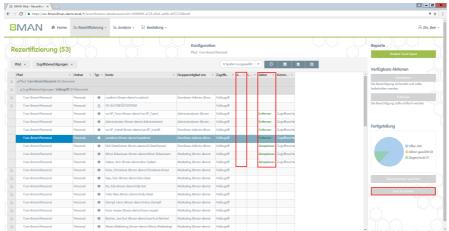


Sie können bestehende Berechtigungen akzeptieren oder entfernen lassen. Aktivieren Sie erst alle Nutzer, die ihren Zugriff behalten sollen. Klicken Sie auf "Akzeptieren".

Unterordner werden nur angezeigt, wenn diese über abweichende Berechtigungen verfügen.



Kommentieren Sie Ihre Entscheidung. Sie wird revisionssicher im System dokumentiert.



Verfahren Sie genauso mit den Zugriffsrechten, die entzogen werden sollen.

Ihre Entscheidung sehen Sie in der Spalte Aktion. Klicken Sie auf "Final Ausführen". Der Administrator erhält nach Finalisierung eine Liste für die Umsetzung.

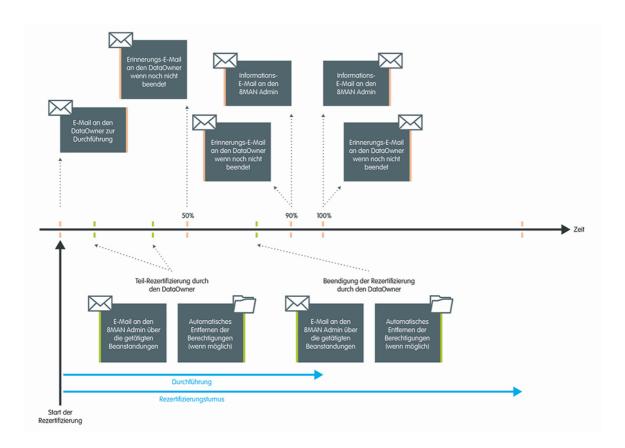
Temporär berechtige Nutzerkonten (siehe eingerückte Spalte in der Abbildung), die gleichzeitig über eine weitere, unbegrenzte Berechtigung auf ein Verzeichnis verfügen, werden unwirksam und entsprechend nicht mehr in der Spalte Ablaufdatum angezeigt.





Wenn Sie "Final Ausführen" klicken, bekommt Ihr Administrator fast jedes Mal eine E-Mail mit den Änderungswünschen. Deshalb empfehlen wir den Rezertifizierungsprozess in einem Rutsch durchzuführen.

#### E-Mail Aufforderungen zur Rezertfizierung 3.1.7.1



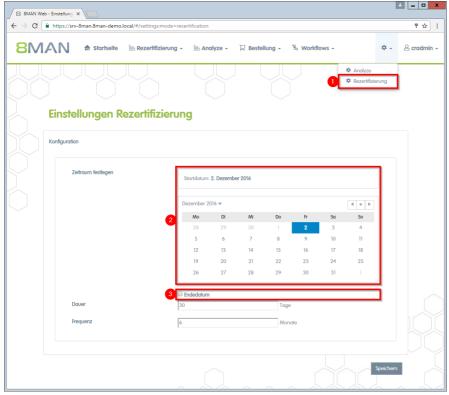
8MAN sendet Ihnen im Rezertifizierungszeitraum automatische Reminder für die Durchführung der Rezertifizierung.



Wenn Sie die Rezertifizierung nicht vor Ende der Periode beenden, stoppt 8MAN den Prozess und Sie und der Administrator erhalten eine Meldung über fehlende Umsetzung.



#### 3.1.7.2 Rezertifizierung aktivieren und deaktivieren



- 1. Loggen Sie sich als 8MAN Administrator in die Weboberfläche ein und wählen Rezertifizierung.
- 2. Wählen Sie ein Start-Datum. Ab diesem Tag ist die Rezertifizierung aktiviert.
- 3. Wählen Sie ein Ende-Datum. Ab diesem Tag ist die Rezertifizierung deaktiviert. Es gibt keine weitere Möglichkeit, die Rezertifizierung zu deaktivieren. Die Data Owner mit offenen Rezertifizierungen werden per E-Mail informiert.

Diese Einstellungen gelten global für alle Data Owner.

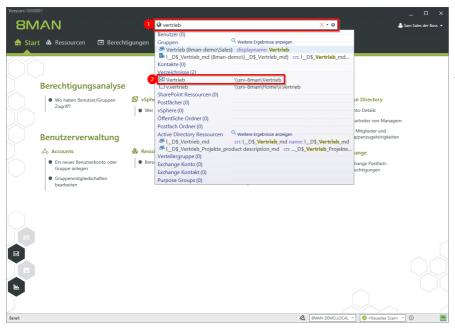
#### 3.1.8 Verzeichnisberechtigungen für Mitarbeiter erteilen und entziehen

# **Hintergrund / Mehrwert**

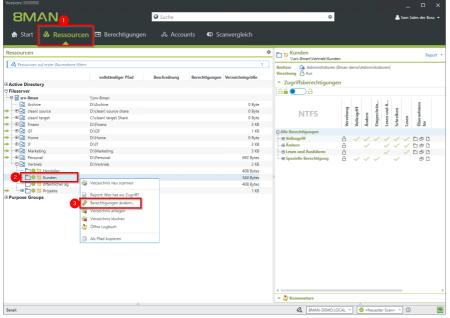
Berechtigungen sollten schnell vergeben und wieder entzogen werden. Deshalb können sie das für Ihre Mitarbeiter selbst erledigen. Sie benötigen keine Fachkenntnisse über Active Directory und Fileserver. Entscheiden Sie einfach, welche Rechte sie vergeben möchten: "Ändern" oder "Lesen und Ausführen".

Für eine bessere Datenintegrität empfehlen wir "Ändern" nur ausgewählten Mitarbeitern zu vergeben.

#### Der Prozess in einzelnen Schritten

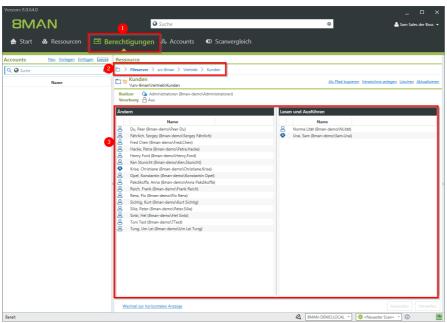


- 1. Verwenden Sie die Suche, um das gewünschte Verzeichnis zu finden.
- 2. Klicken Sie auf das Suchergebnis.

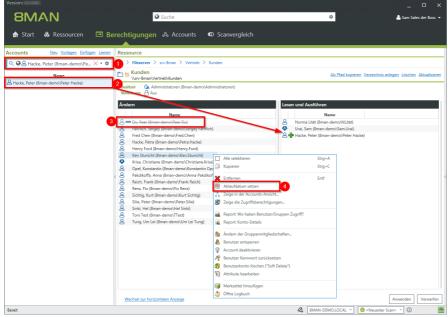


- 1. 8MAN wechselt in die Ansicht "Ressourcen".
- 2. Wählen Sie ggf. in ein Unterverzeichnis. Rechtsklicken Sie das gewünschte Verzeichnis.
- 3. Klicken Sie auf "Berechtigungen ändern...".

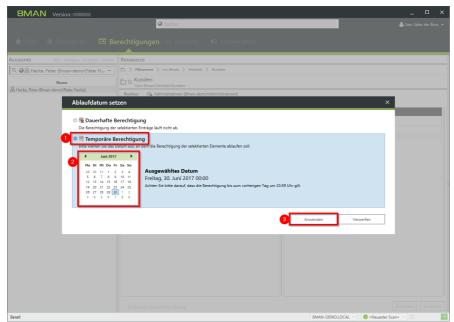




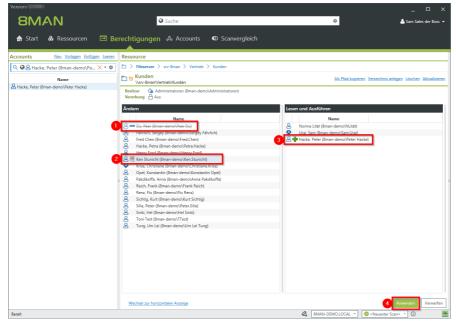
- 1. 8MAN wechselt in die Ansicht "Berechtigungen".
- 2. 8MAN zeigt Ihnen das Verzeichnis, an dem Sie arbeiten. Sie können das Verzeichnis wechseln.
- 3. 8MAN zeigt Ihnen die bestehenden Berechtigungen in den Zugriffskategorien "Ändern" und "Lesen und Ausführen".



- 1. Finden Sie mit der Suche einen Benutzer oder eine Gruppe.
- 2. Ziehen Sie Benutzer per Drag&Drop auf eine Spalte, um eine Berechtigung zuzuweisen.
- 3. Klicken Sie mit der rechten Maustaste auf einen Eintrag, um eine Berechtigung zu entziehen - sofort oder zu einem geplanten Zeitpunkt. Klicken Sie auf "Ablaufdatum setzen".



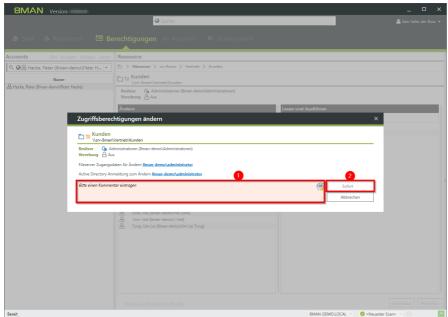
- 1. Aktivieren Sie die Option "Temporäre Berechtigung".
- 2. Setzen Sie ein Ablaufdatum.
- 3. Klicken Sie auf "Anwenden".



8MAN zeigt alle geplanten Berechtigungsänderungen:

- 1. Eine Berechtigung entziehen.
- 2. Ein Ablaufdatum für eine Berechtigung setzen.
- 3. Eine Berechtigung erteilen.
- 4. Klicken Sie auf "Anwenden".





- 1. Sie müssen einen Kommentar eingeben.
  - 2. Starten Sie die Berechtigungsänderung.

#### 3.1.9 Die Zugriffe auf sensible Daten überwachen

# **Hintergrund / Mehrwert**

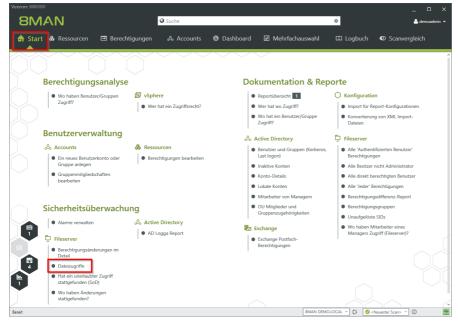
Sie haben im ersten Schritt die Zugriffsrechte für sicherheitsrelevante Verzeichnisse eingeschränkt. Im zweiten Schritt empfehlen wir die permanente Überwachung der Zugriffe und von den Nutzern durchgeführte Aktionen. Dadurch erhalten Sie die vollständige Prozesstransparenz für besonders schützenswerte Daten und Informationen.

#### Weiterführende Services

Prüfen und ändern Sie vorher die Verzeichnisberechtigungen, um die Akteure mit Zugriffsrechten einzuschränken:

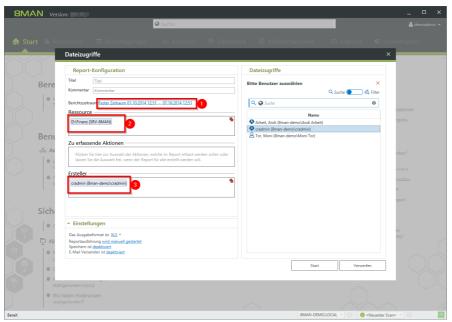
Verzeichnis Berechtigungen ändern

#### Der Prozess in einzelnen Schritten

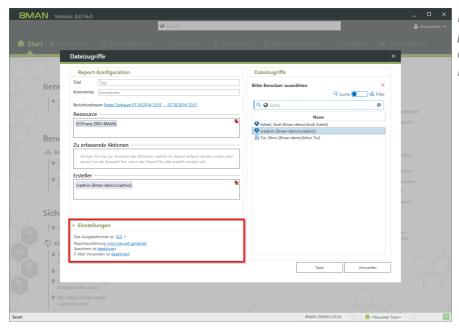


Wählen Sie auf der Startseite "Dateizugriffe".

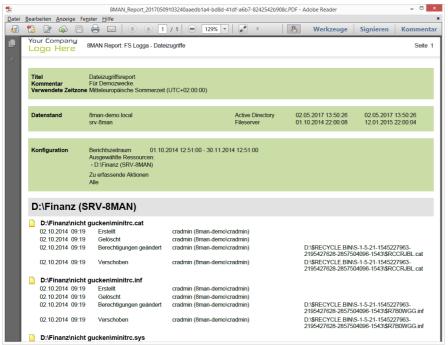




- 1. Legen Sie einen Zeitraum fest.
- 2. Optional: wählen Sie per Drag&Drop eine Ressource.
- 3. Optional: Wählen Sie einen Ersteller (Event-Autor)



Planen Sie den FS Logga Report, versenden ihn per E-Mail oder speichern ihn auf dem Dateisystem.



Sie erhalten eine übersichtliche Auflistung über sämtlicher Dateiaktivitäten im gewählten Zeitfenster.



# 3.1.10 Alarme für AD Konten und Gruppen anlegen

## **Hintergrund / Mehrwert**

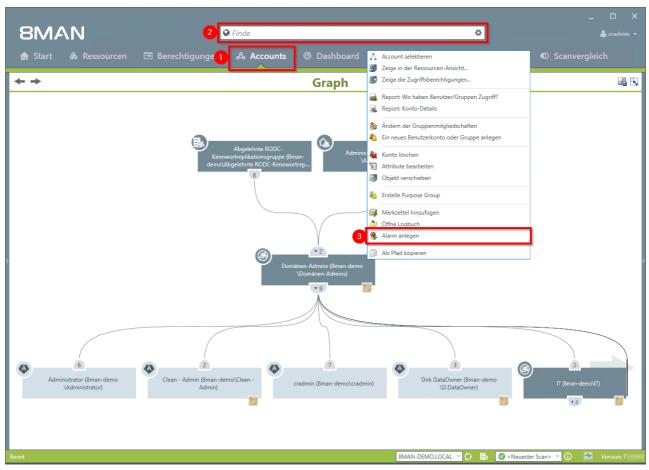
Über Gruppenmitgliedschaften erhalten Mitarbeiter ihre Zugriffsrechte im Firmennetzwerk. Besonders schützenswerte Gruppen verleihen ihren Mitgliedern Rechte auf geheime Ordner und wichtige Ressourcen. Mit dem 8MATE Alerts können Sie AD Gruppen aktiv überwachen und sollten neue Mitglieder hinzugefügt werden, einen Alarm auslösen.

Die Gruppenverschachtelungen im Active Directory machen es notwendig, auch Gruppenmitgliedschaften zu überwachen, die sich aus neuen, indirekten Mitgliedschaften ergeben. Ein Beispiel: Die Gruppe "Geschäftsführer" wird überwacht und hat als Mitglied die Gruppe "geheime Daten". 8MATE Alerts benachrichtigt Sie jetzt auch, wenn der letztgenannten Gruppe neue Mitglieder oder Gruppen hinzugefügt bzw. entfernt werden.

#### Weiterführende Services

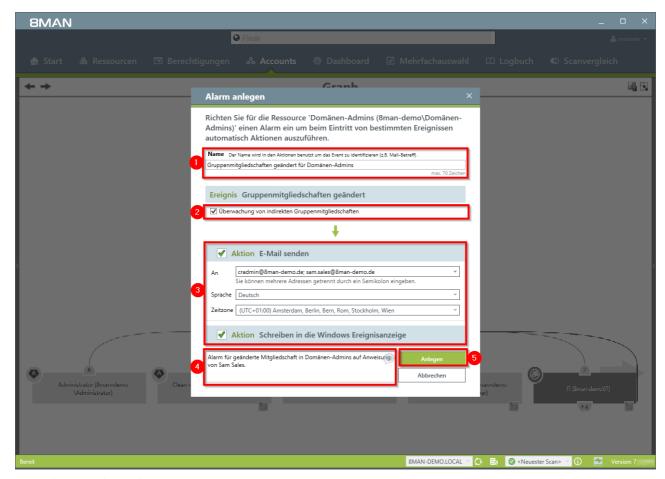
Alarme für Nutzerkonten anlegen Alarme verwalten

#### Der Prozess in einzelnen Schritten



- 1. Wählen Sie "Accounts".
- 2. Finden Sie die gewünschte Gruppe mit der Suchfunktion.
- 3. Rechtsklicken Sie die Gruppe und wählen "Alarm anlegen" im Kontextmenü.





- 1. Geben Sie dem Alarm einen Namen.
- 2. Aktivieren Sie die Checkbox, um auch über indirekte Änderungen an den Gruppenmitgliedschaften informiert zu werden.
- 3. Sie können beliebig viele E-Mail-Empfänger hinterlegen. Darüber hinaus kann der Alarm auch in die Windows Ereignisanzeige geschrieben werden.
- 4. Sie müssen einen Kommentar hinterlegen.
- 5. Aktivieren Sie den Alarm.

## 3.1.11 Reporte automatisch zusenden lassen

## **Hintergrund / Mehrwert**

Involvieren Sie Sicherheitskräfte in das Access Rights Management, indem Sie pragmatisch die relevanten Reporte zuweisen.

8MAN versendet die Reporte im gewünschten Turnus automatisch. Der Vorgang ist für jeden Report derselbe.

Wir empfehlen eine Auswahl unserer Management Reporte an die Sicherheitsrolle zu senden. Sie sind leicht verständlich und auf das wesentlich reduziert.

#### **Die 8MAN Management Reporte:**

#### **Active Directory**

Mitarbeiter von Managern Konto-Details von Nutzern zeigen

#### **Fileserver**

Wer hat wo Zugriff?

Wo haben Mitarbeiter eines Managers Zugriff?

Wo haben Benutzer/Gruppen Zugriff?

## **Exchange**

Wer hat wo Zugriff? Postfach Berechtigungen identifizieren

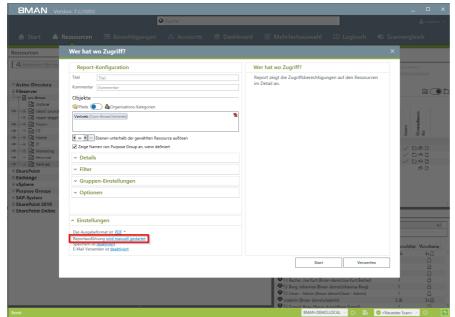
#### **SharePoint**

Wer hat wo Zugriff?

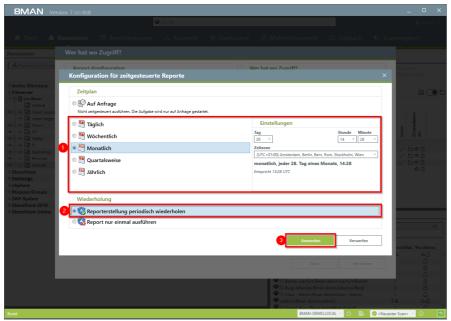
Wo haben Benutzer/Gruppen Zugriff



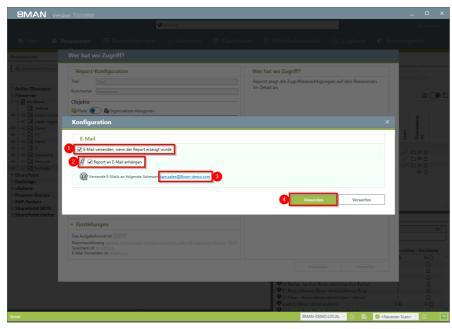
#### Der Prozess in einzelnen Schritten



Wählen Sie einen beliebigen Report. Klicken Sie im Bereich Einstellungen auf "wird manuell gestartet".



- 1. Legen Sie den Zeitplan fest.
- 2. Aktivieren Sie die periodische Wiederholung.
- 3. Klicken Sie auf "Anwenden".



- 1. Aktivieren Sie den E-Mail-Versand.
- 2. Aktivieren Sie die Option "Report an E-Mail anhängen".
- 3. Legen Sie fest, wer die E-Mail erhalten soll. Sie können mehrere Empfänger angeben.
- 4. Klicken Sie auf "Anwenden".



# 3.1.12 Die Zugriffe auf sensible Daten überwachen

## **Hintergrund / Mehrwert**

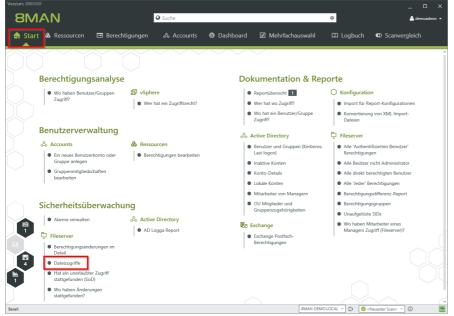
Sie haben im ersten Schritt die Zugriffsrechte für sicherheitsrelevante Verzeichnisse eingeschränkt. Im zweiten Schritt empfehlen wir die permanente Überwachung der Zugriffe und von den Nutzern durchgeführte Aktionen. Dadurch erhalten Sie die vollständige Prozesstransparenz für besonders schützenswerte Daten und Informationen.

#### Weiterführende Services

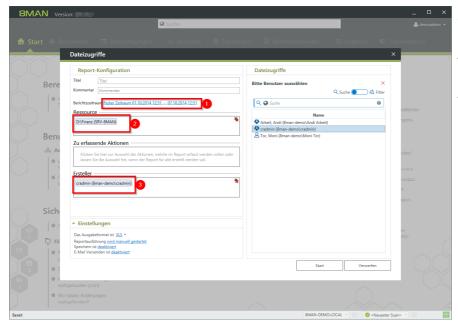
Prüfen und ändern Sie vorher die Verzeichnisberechtigungen, um die Akteure mit Zugriffsrechten einzuschränken:

Verzeichnis Berechtigungen ändern

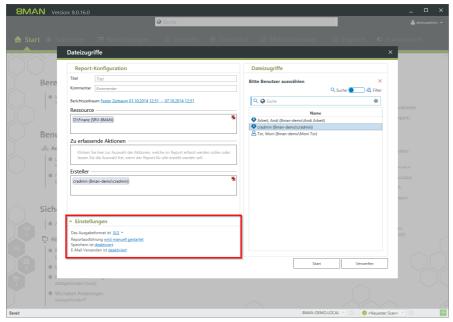
#### Der Prozess in einzelnen Schritten



Wählen Sie auf der Startseite "Dateizugriffe".

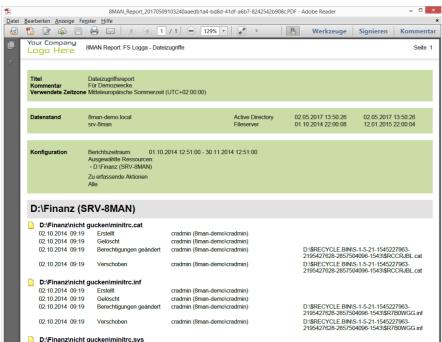


- 1. Legen Sie einen Zeitraum fest.
- 2. Optional: wählen Sie per Drag&Drop eine Ressource.
- 3. Optional: Wählen Sie einen Ersteller (Event-Autor)



Planen Sie den FS Logga Report, versenden ihn per E-Mail oder speichern ihn auf dem Dateisystem.





Sie erhalten eine übersichtliche Auflistung über sämtlicher Dateiaktivitäten im gewählten Zeitfenster.

# 3.1.13 Berechtigungen im Webclient entfernen

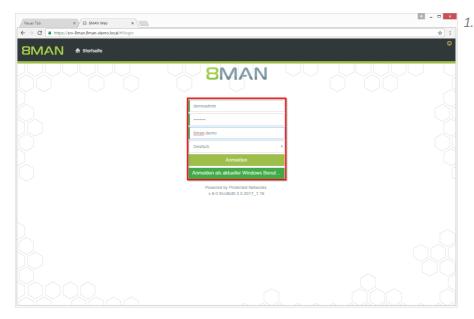
# **Hintergrund / Mehrwert**

Überberechtigungen sind Alltag im Berechtigungsmanagement. Setzen Sie Führungskräfte als Data Owner ein, können diese für ihren Verantwortungsbereich Berechtigungen einfach und gesammelt entfernen. Der Webclient ermöglicht auch technisch weniger versierten Benutzern die Berechtigungssituation zu pflegen.

## Weiterführende Services

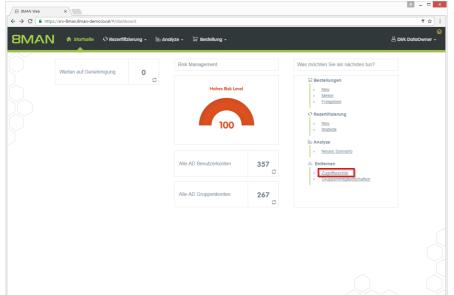
Gruppenmitgliedschaften im Webclient entfernen

### Der Prozess in einzelnen Schritten

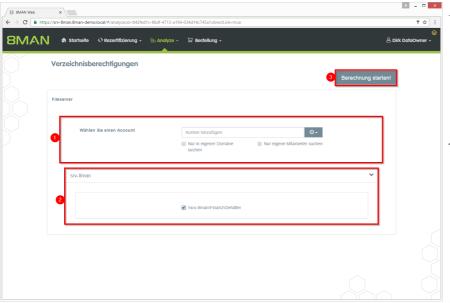


1. Loggen Sie sich in die Weboberfläche ein.

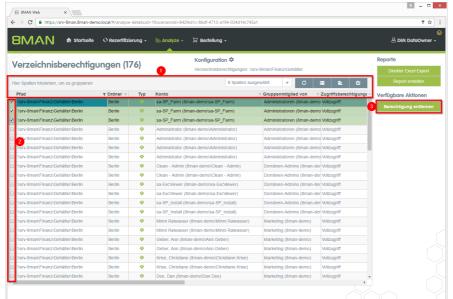




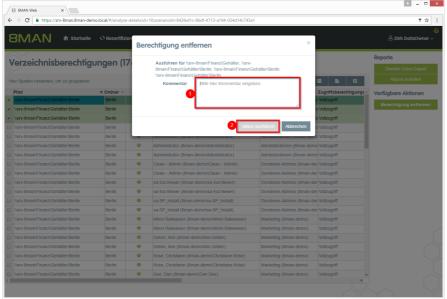
Klicken Sie auf "Zugriffsrechte".



- 1. Wählen Sie optional ein Konto aus, denen Sie die Berechtigungen entziehen wollen.
  - Lassen Sie die Auswahl frei, um alle Konten mit Berechtigungen aufzulisten.
- 2. Wählen Sie mindestens eine Ressource.
  - Welche Ressourcen Data Owner bearbeiten können, legen Sie in der Data Owner Konfiguration fest. 8MAN Administratoren können alle Ressourcen bearbei-
- 3. Klicken Sie auf "Berechnung starten".



- 1. Nutzen Sie die Sortier-, Filter- und Gruppierungsfunktionen sowie die Spaltenauswahl, um Ihre Auswahl einzugrenzen.
- 2. Selektieren Sie die gewünschten Einträge.
- 3. Klicken Sie auf "Berechtigungen entfernen".



- 1. Sie müssen einen Kommentar eingeben.
- 2. Klicken Sie auf "Aktion ausführen".

Der Job wird an den 8MAN Server übergeben und dort ausgeführt. 8MAN zeigt den Status in der Jobübersicht.



# 4. Über 8MAN





8MAN ist eine führende Lösung für Access Rights Management (ARM) in Microsoft- und virtuellen Server-Umgebungen und schützt damit Unternehmen vor unberechtigten Zugriffen auf sensible Daten. Die in Deutschland von Protected Networks entwickelte Software-Lösung setzt Maßstäbe für professionelle Netzwerksicherheit und agile IT-Organisation und bündelt modernste Funktionalität mit der Erfüllung gängiger Sicherheits- und Compliance-Richtlinien. Die 8MAN Kerndisziplinen umfassen: Permission Analysis, Security Monitoring, Documentation & Reporting, Role & Process Optimization und User Provisioning.

#### **WIE SIE IHR UNTERNEHMEN SICHERN**

Die Einführung von 8MAN ist kein Projekt, sondern ein Griff zum Telefon. Vereinbaren Sie einen Termin und ein zertifizierter Techniker wird die Installation und Konfiguration bei Ihnen im Unternehmen vornehmen. Je nach den Möglichkeiten in Ihrem Unternehmen kann die Installation vollständig via Remote Access vorgenommen werden.

Kostenloses Webinar Starten Sie mit einer 30-minütigen Führung und sehen Sie den 8MAN in Aktion. Als Teilnehmer bleiben Sie untereinander anonym. Sie haben die Möglichkeit, am Ende der Präsentation im Chat Fragen zu stellen.

Kostenlose Teststellung Testen Sie 8MAN mit einer 21 Tage gültigen kostenlosen Testlizenz und Sie haben genug Zeit, sich von unserer Lösung in Ruhe zu überzeugen.

#### Prüffragen an Ihre IT und Geschäftsbereiche 4.1

- 1. Wo sind unsere personenbezogenen Daten gespeichert und wer hat darauf Zugriff?
- 2. Wo hat Herr Mustermann überall Zugriff?
- 3. Wer hat im Zeitraum XY was im Verzeichnis XY gemacht?
- 4. Welches sind unsere besonders sicherheitsrelevanten AD- Gruppen, auf welche Daten berechtigen diese und wer ist darin Mitglied?
- 5. Wie bekomme ich Bescheid, wenn eine AD Sicherheitsgruppe oder ein Nutzerkonto manipuliert wurde?
- 6. Wer erstellt mir schnell einen verständlichen Report über die Zugriffsrechtesituation in meinem Unternehmen?
- 7. Wer ist in seinem Fachbereich verantwortlich für die Überwachung sicherheitsrelevanter Verzeichnisse?
- 8. Wann hatten wir unsere letzte Rezertifizierung von Zugriffsrechten?



#### 4.2 Kontakt



Sven Reinhardt Head of Sales Engineering & Professional Services +49 30 390 63 45-66 sven@8man.com

Kostenloses Webinar: Starten Sie mit einer 30-minütigen Führung und sehen Sie den 8MAN in Aktion. Als Teilnehmer bleiben Sie untereinander anonym. Sie haben die Möglichkeit, am Ende der Präsentation im Chat Fragen zu stellen.

Kostenlose Teststellung: Testen Sie 8MAN mit einer 21 Tage gültigen kostenlosen Testlizenz und Sie haben genug Zeit, sich von unserer Lösung in Ruhe zu überzeugen.