Kapitel 2

Grundkonfiguration

Im zweiten Kapitel lernen Sie, wie Sie einen Office 365-Mandanten anlegen, Abonnements verwalten, eigene Domänen einrichten, Benutzer anlegen, Ihre Clients konfigurieren, und Sie erhalten erste Hilfestellungen, wenn mal ein Problem auftritt.

Das zweite Kapitel steht ganz im Zeichen der grundlegenden Einrichtung einer Office 365-Umgebung. Bevor Sie beginnen, Ihren Anwendern einen Zugang zu Cloud-Postfächern, Cloud-Speicher etc. zu verschaffen, müssen Sie zunächst einige grundlegende Konfigurationen durchführen. Der Aufwand und die Komplexität werden dabei gerne unterschätzt. Damit Sie beispielsweise Ihre eigenen Domänen mit Office 365 nutzen können, müssen Sie diese zunächst zu Ihrer Umgebung hinzufügen. Anschließend machen Sie sich Gedanken zur Benutzerverwaltung und zur Konfiguration der Anwender-Clients.

2.1 Anlegen eines Office 365-Mandanten

Damit Sie die Funktionen von Office 365 auf die Eignung für Unternehmen hin überprüfen können, bietet sich ein Testzugang an. Diesen erhalten Sie von Microsoft innerhalb weniger Minuten. Dabei müssen Sie nur Kontaktinformationen und keine Zahlungsinformationen wie Kreditkartendaten angeben. Ein solcher Testzugang ist 30 Tage lang uneingeschränkt benutzbar und wird, wenn Sie während dieses Zeitraums keine Abonnements abschließen, anschließend automatisch deaktiviert.

Sollten die 30 Tage für Ihre Tests nicht ausreichen, können Sie beim Office 365-Kundendienst (siehe Abschnitt 2.11, »Problembehebung«) um eine Verlängerung bitten. Die Erfahrung zeigt, dass diese im Regelfall problemlos gewährt wird. [«]

Fügen Sie jedoch zu Ihrem Testzugang Abonnements hinzu, können Sie sofort produktiv mit dem Mandanten arbeiten. Die Konfigurationsschritte, die Sie während des Testzeitraums für den Mandanten angelegt haben, müssen Sie damit nicht erneut durchführen. Andererseits hat ein neuer Mandant auch seine Vorteile: Sie beginnen wieder bei null und schleppen keine unerwünschten Konfigurationen mit, die Sie vielleicht testweise einmal angelegt und dann vergessen haben.

Bei den Testzugängen haben Sie die Auswahl zwischen unterschiedlichen Lizenztypen, von denen Ihnen 25 kostenfrei zur Verfügung gestellt werden:

- Office 365 Business
- Office 365 Business Premium
- Office 365 Enterprise

Ein Testkonto können Sie über folgende URL einrichten: *www.office365.de*

Beim Anlegen des Testkontos entscheiden Sie sich für den vorderen Teil einer Domäne mit der Endung *onmicrosoft.com* (siehe Abbildung 2.1). Diese Domäne wird *Mandantdomäne* genannt. Jeder Office 365-Mandant hat eine solche Domäne, auch wenn Sie später Ihre eigene Domäne einsetzen (beispielsweise *beispielag.de* für Ihre E-Mail-Adresse). Der Name ist dabei frei wählbar, darf aber noch nicht in Benutzung sein.

Abbildung 2.1 Anlegen eines Testmandanten

[»] Achtung: Überlegen Sie sich diesen Namen sehr sorgfältig, denn er ist später nicht mehr änderbar. Er sollte auch nicht zu kryptisch sein, da der Zugriff auf die privaten SharePoint-Websites immer über den selbst gewählten Teil der Mandantdomäne erfolgt. Haben Sie sich beispielsweise für die Mandantdomäne `beispielag.onmicrosoft.com` entschieden, erfolgt der Zugriff auf die privaten SharePoint-Websites über `beispielag.sharepoint.com`, auf die SharePoint Online-Administration über `beispielag-admin.sharepoint.com` und der direkte Zugriff auf OneDrive for Business über `beispielag.onedrive.com`. Merken Sie später, dass Sie das Testkonto nicht weiterverwenden, sondern auf der grünen Wiese mit einem neuen Mandanten anfangen wollen, ist der Name blockiert, und Sie müssen einen anderen wählen.

Mit der *onmicrosoft.com*-Domäne könnten Sie auch gleich losarbeiten, Benutzer anlegen und diese mit E-Mail-Adressen ausstatten, die auf der ausgesuchten Domäne enden. Das wollen Sie in der Praxis höchstwahrscheinlich nicht tun, sondern Ihre eigene Domäne verwenden. Dazu müssen Sie Ihre Domäne zu Ihrem Office 365-Mandanten hinzufügen. Wie das geht, lesen Sie in Abschnitt 2.4, »Domänenverwaltung«.

Mit der Domäne legen Sie ein Administratorkonto an, unter dem Sie sich zukünftig an Office 365 zur Verwaltung Ihres Mandanten anmelden.

Dem Administratorkonto wird automatisch eine Lizenz zugewiesen. Dies muss aber nicht so bleiben. Administratoren benötigen zur reinen Verwaltung grundsätzlich keine kostenpflichtige Lizenz. Gegebenenfalls können Sie die Lizenz vom Administratorkonto also auch entfernen und einem anderen Benutzer zuweisen. Idealerweise verwenden Sie für die Administration von Office 365 ein separates Benutzerkonto und nicht das, das Sie zur täglichen Arbeit verwenden. Damit sind Administrations- und Anwendungsaufgaben voneinander getrennt. [«]

2.2 Office 365-Portal und Office 365 Admin Center

Zentraler Startpunkt für Office 365-Anwender und -Administratoren ist die folgende URL (siehe Abbildung 2.2): *https://portal.office.com*

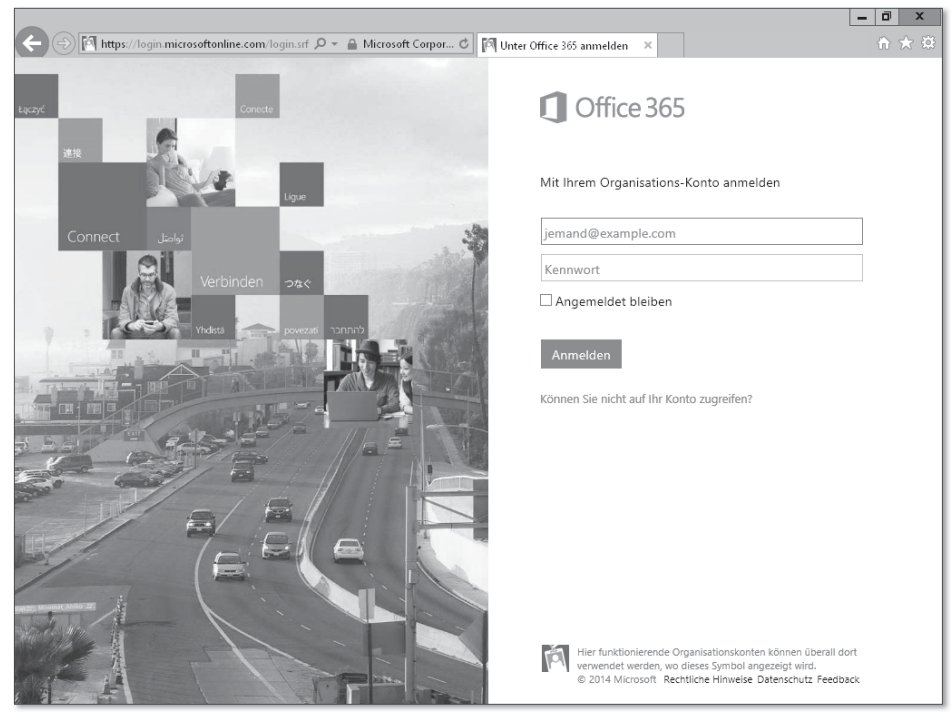

Abbildung 2.2 Anmeldung an Office 365

[»] Früher wurde als Startpunkt gerne *https://portal.microsoftonline.com* genannt. Diese URL ist nach wie vor verfügbar und führt zum selben Ziel. Melden Sie sich mit einem Benutzerkonto ohne Administratorberechtigungen an, erreichen Sie unter dieser Adresse das *Office 365-Portal* aus Abbildung 2.3.

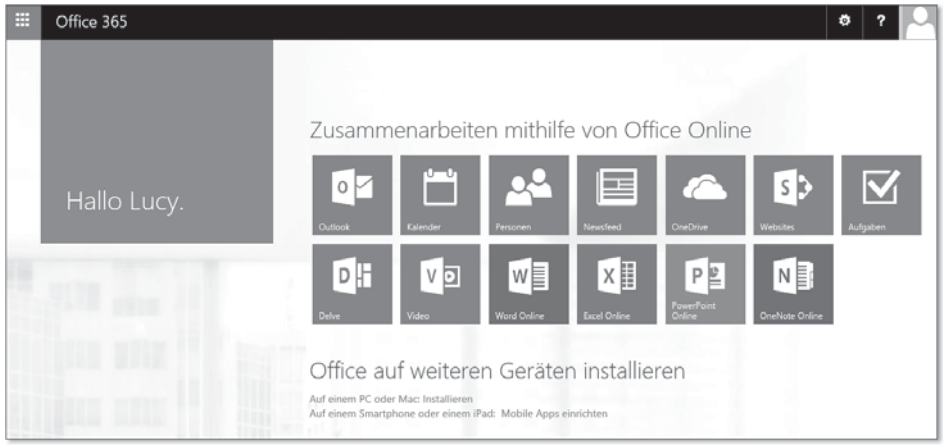

Abbildung 2.3 Office 365-Portal für Benutzer ohne Administratorberechtigungen

Verfügt das Benutzerkonto jedoch über Administratorberechtigungen, erhalten Sie statt des Office 365-Portals entweder direkt das *Office 365 Admin Center* oder Sie können mit einem Klick auf das Symbol ADMINISTRATOR dorthin wechseln (siehe Abbildung 2.4). Anwender ohne Administratorberechtigungen haben keinen Zugriff auf das Office 365 Admin Center.

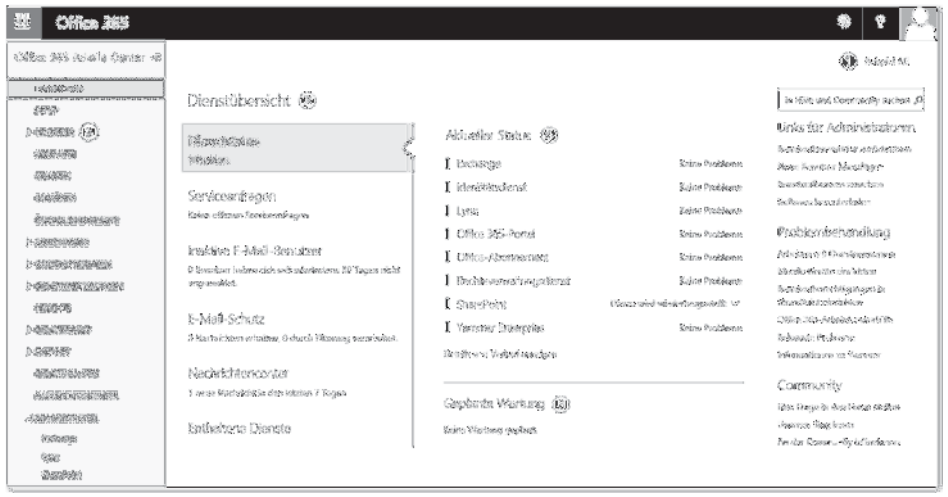

Abbildung 2.4 Office 365 Admin Center für Benutzer mit Administratorberechtigungen

Das Admin Center ist abhängig von den verfügbaren Lizenztypen ausgestattet. So kann es durchaus sein, dass bestimmte Funktionen nicht zur Verfügung stehen oder zusätzlich enthalten sind.

2.2.1 Office 365-Portal

Am oberen Rand innerhalb der Kopfnavigation in Abbildung 2.3 befindet sich rechts ein Bild des Anwenders – wenn nur ein Symbolbild zu sehen ist, kann der Anwender an dieser Stelle ein passenderes hochladen. Klickt er auf sein Bild, kann er sein Benutzerprofil (aus SharePoint) anpassen (siehe Abbildung 2.5) und sich vom Portal wieder abmelden.

Abbildung 2.5 Benutzerprofil

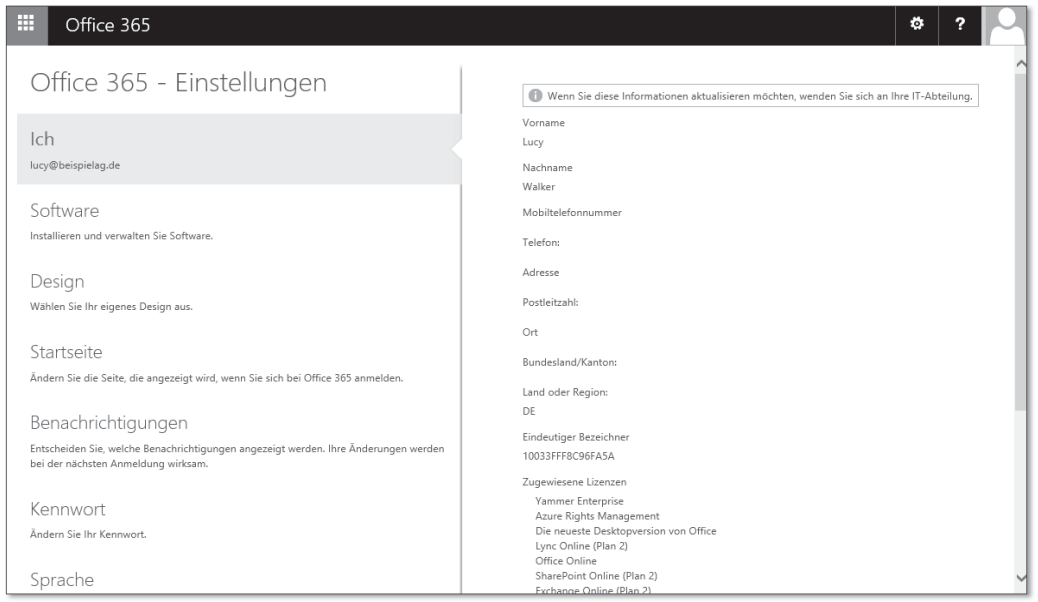

Abbildung 2.6 Einstellungen

Das Zahnrad in der Kopfnavigation führt den Anwender zu den Einstellungen (siehe Abbildung 2.6) und zur Auswahl eines Designs. Dort findet er neben rosa Katzenfarbschemata auch einige seriöse.

Bei den Einstellungen kann er im Wesentlichen Software installieren (beispielsweise das Office-Paket, sofern der Administrator ihm eine entsprechende Lizenz zugewiesen hat), sein Kennwort ändern, Kontaktinformationen angeben und eine Sprache für das Portal auswählen. Außerdem kann er sich hier für eine Startseite entscheiden, mit der er nach der Portalanmeldung beginnen will, beispielsweise mit der Outlook Web App, OneDrive for Business oder Delve.

Im mittleren Teil des Portals findet der Anwender Zugriff auf die ihm zur Verfügung stehenden Dienste und Anwendungen. Welche das sind, wird über die Lizenzen bestimmt, die dem Anwender zugewiesen wurden.

Zuletzt enthält die Kopfnavigation noch ganz links den *App-Launcher*. Dieser wird in allen Office 365-Diensten angezeigt. Klickt der Anwender auf das Symbol, erscheint ebenfalls die Auswahl der verfügbaren Dienste und Anwendungen (siehe Abbildung 2.7).

Abbildung 2.7 App-Launcher

Von hier aus erreicht der Anwender beispielsweise über das Symbol OUTLOOK die Outlook Web App (OWA; früher als *Outlook Web Access, OWA*, bezeichnet), der Browseransicht seines gegebenenfalls vorhandenen Postfachs (siehe Abbildung 2.8).

Ein anderes Beispiel ist ONEDRIVE (genauer gesagt *OneDrive for Business* – früher unter dem Namen *SkyDrive Pro* bekannt), dem persönlichen Cloud-Speicher des Anwenders (siehe Abbildung 2.9).

Der Anwender kann den Inhalt des App-Launchers auch an seine Wünsche anpassen. Derzeit ist das allerdings nur möglich, wenn das Benutzerkonto des Anwenders über eine Exchange Online-Lizenz verfügt. Ist das der Fall, erscheinen auf dem jeweiligen App-Symbol drei Punkte, wenn der Anwender mit der Maus darüber fährt. Klickt der Anwender auf diese Punkte, erscheint das Kontextmenü aus Abbildung 2.10.

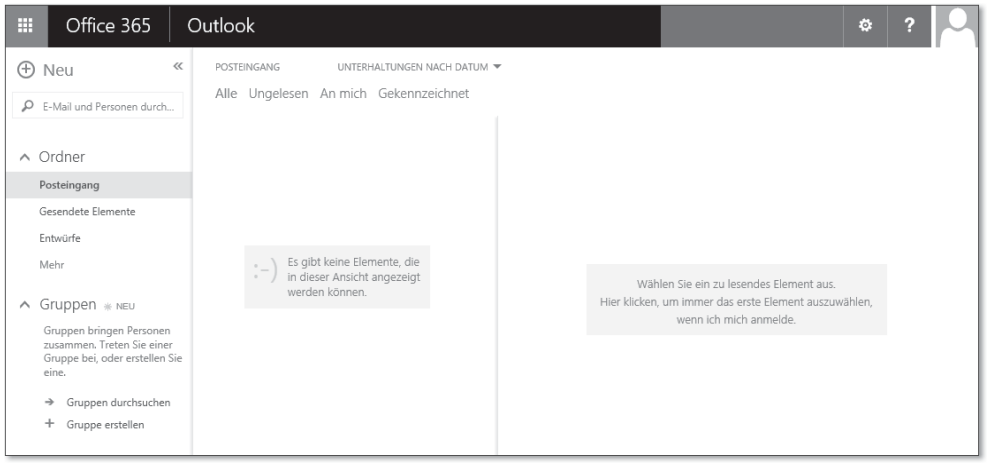

Abbildung 2.8 Outlook Web App

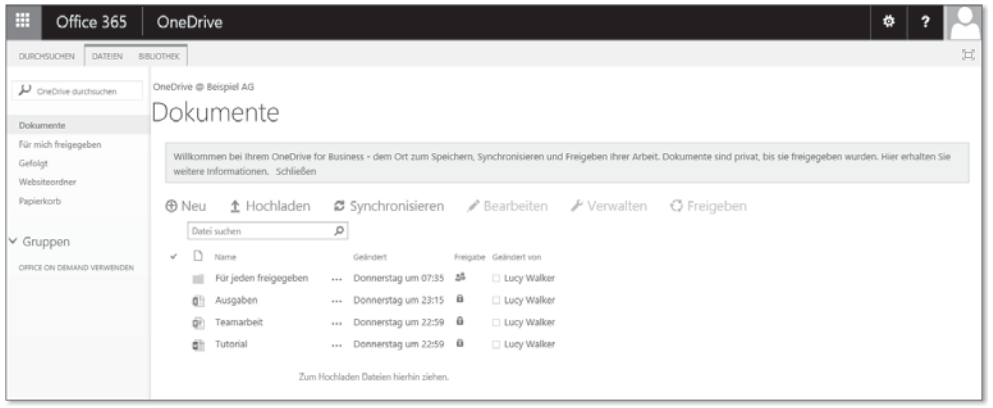

Abbildung 2.9 OneDrive for Business

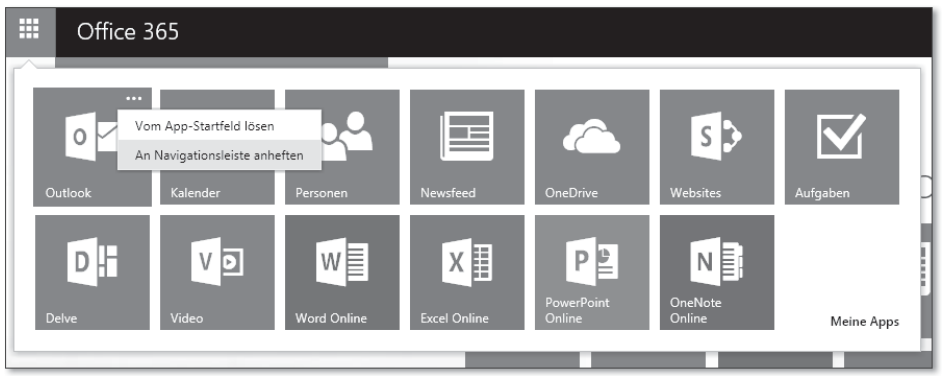

Abbildung 2.10 Anpassung des App-Launchers

Apps, die der Anwender nicht benötigt, kann er aus dem App-Launcher entfernen. Sie sind dann immer noch über MEINE APPS aufrufbar (siehe Abbildung 2.11). Außerdem kann der Anwender bis zu drei Apps in die Kopfnavigationsleiste am oberen Fensterrand aufnehmen. Diese Apps erscheinen dann links vom Einstellungen-Symbol (Zahnrad). Dies macht besonders für Apps Sinn, die der Anwender häufig benötigt.

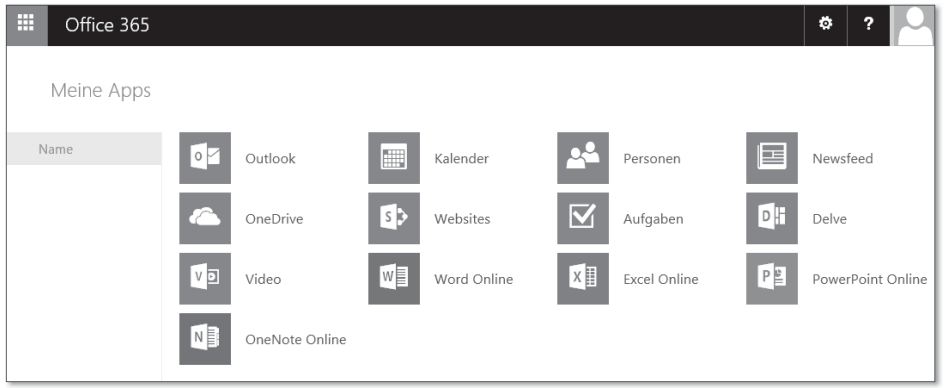

Abbildung 2.11 Meine Apps

Der App-Launcher kann auch mit weiteren Apps aus dem Office Store ausgestattet werden: *https://store.office.com/*

2.2.2 Office 365 Admin Center

Punkt ❶ in Abbildung 2.4 zeigt den Namen Ihres Unternehmens. Klicken Sie darauf, gelangen Sie zu den Organisationseinstellungen, über die Sie die Adresse Ihres Unternehmens anpassen können (siehe Abbildung 2.12). Denken Sie auch hier daran, eine geeignete E-Mail-Adresse als technischen Kontakt zu hinterlegen, damit E-Mails über technische Probleme, beispielsweise bei der Active-Directory-Synchronisierung, oder Hinweise über ablaufende Abonnements beim richtigen Ansprechpartner aufschlagen. Bei den Organisationseinstellungen finden Sie auch wieder die Standarddomäne Ihres Office 365-Mandanten, die Ihnen beim Anlegen neuer Benutzerkonten beim Benutzernamen vorgeschlagen wird.

Daneben finden Sie dort auch die Möglichkeit, das Aussehen des Office 365-Portals beziehungsweise des Admin Centers farblich ein wenig anzupassen. Auch das Anzeigen des eigenen Firmenlogos ist möglich. Die entsprechenden Optionen finden Sie im Abschnitt BENUTZERDEFINIERTE DESIGNS (siehe Abbildung 2.13).

Punkt ❷ in Abbildung 2.4 zeigt eine Dienstübersicht mit dem aktuellen Dienststatus und den Serviceanfragen, die Sie an den Office 365-Kundendienst gestellt haben. Die Dienstübersicht ist nur eine Zusammenfassung der jeweiligen Bereiche. Punkt ❸ mit der Navigation auf der linken Seite führt Sie zu den Bereichen aus Tabelle 2.1.

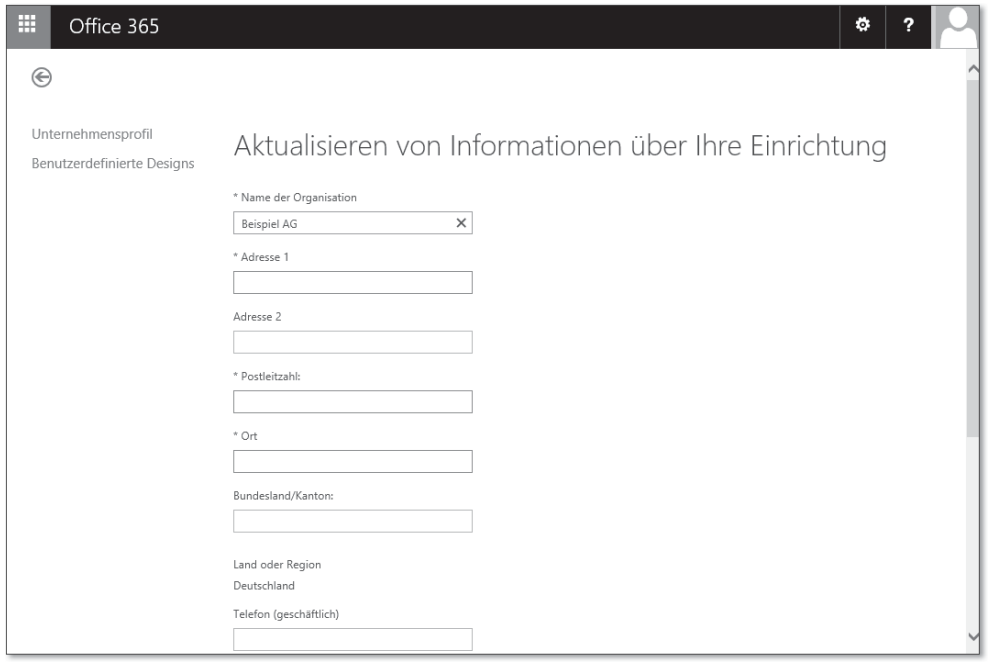

Abbildung 2.12 Organisationseinstellungen

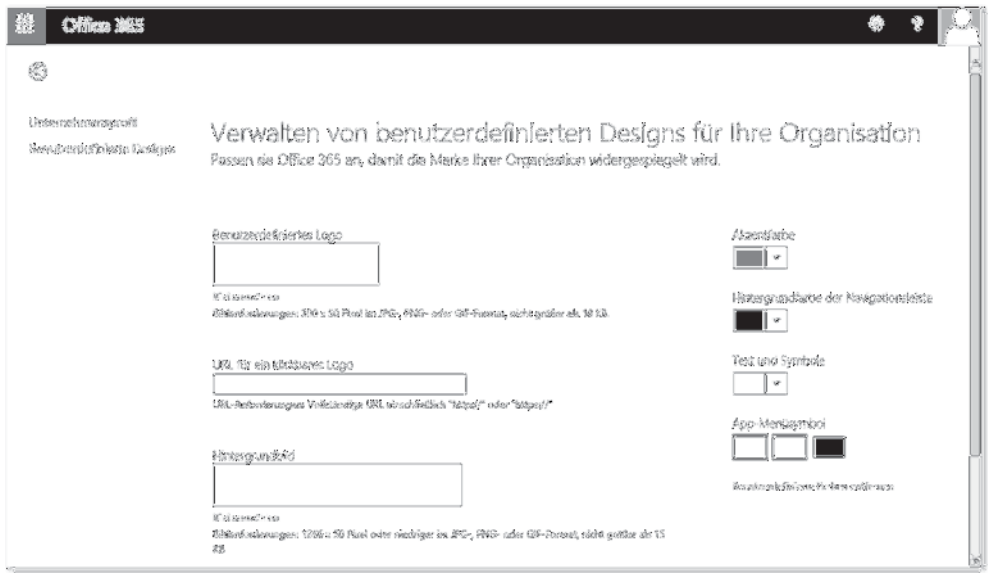

Abbildung 2.13 Designanpassungen

Punkt ❹ zeigt eine Kurzübersicht des aktuellen Status aller Dienste, und Punkt ❺ führt geplante Wartungsmaßnahmen auf.

Bereich	Bedeutung	Weitere Informationen
Dashboard	Das Dashboard enthält einen Überblick über die Dienste und ihren Status.	siehe vorliegenden Abschnitt
Setup	Ruft einen Assistenten auf, der Sie durch die Grundkonfiguration Ihres Office 365-Mandanten führt. Alternativ dazu können Sie die Konfiguration auch über die jeweiligen Bereiche im Office 365 Admin Center durchführen. Der Assistent hilft beispielsweise beim Hinzufügen einer eigenen Domäne und beim Anlegen von Benutzerkonten.	siehe Abschnitt 2.4, »Domänenverwaltung«, und Abschnitt 2.5, »Benutzerverwaltung«
Benutzer	Hier verwalten Sie die Benutzerkonten Ihres Office 365-Mandanten.	siehe Abschnitt 2.5, »Benutzerverwaltung«
Kontakte	Hier angelegte Kontakte erscheinen im Exchange-Adressbuch. Diese Kontakte gehören normalerweise nicht zu Ihrer Organisation.	siehe Abschnitt 6.5.4, »Externe Kontakte«
Gruppen	Hier verwalten Sie die Sicherheitsgruppen aus Ihrem Office 365-Mandanten, aber auch andere Gruppen.	siehe Abschnitt 2.5.6, »Sicherheitsgruppen« und 11.3, »Gruppen«
Domänen	Beim Anlegen Ihres Office 365-Mandanten haben Sie bereits eine Domäne in der Form *MANDANT-DOMÄNE.onmicrosoft.com* erstellt. Sicher wollen Sie eine oder mehrere eigene Domänen zu Ihrem Mandanten hinzufügen, um sie dann mit den Office 365-Diensten nutzen zu können. In diesem Bereich finden Sie die Domänenverwaltung.	siehe Abschnitt 2.4, »Domänenverwaltung«
Öffentliche Website	Einrichtung einer öffentlichen Website auf Basis von SharePoint Online	siehe Abschnitt 7.16, »Öffentliche Website«
Abrechnung	Dieser Bereich zeigt Ihnen eine Übersicht Ihrer Abonnements und der daraus erhaltenen Lizenzen.	siehe Abschnitt 2.3, »Abonnements«

Tabelle 2.1 Administrationsbereiche des Office 365 Admin Centers

Bereich	Bedeutung	Weitere Informationen
Externe Freigaben	Hier finden Sie diverse Freigabeoptionen für Exchange Online, Lync Online und SharePoint Online.	siehe Abschnitt 6.13.9, »Freigabe von Kalenderinformationen«, Abschnitt 7.5.3, »Externe Benutzer verwalten«, Abschnitt 9.2.5, »Externe Kommunikation«
Diensteinstellungen	Der Bereich Diensteinstellungen führt Sie direkt zu bestimmten Einstellungen der Office 365-Dienste, wie beispielsweise der Anti-Spam-Konfiguration von Exchange Online und der Websitesammlungsverwaltung von SharePoint.	siehe Kapitel 6, »Exchange Online«, **Kapitel 7**, »SharePoint Online«
Berichte	Im Bereich Berichte können Sie Auswertungen über Ihre Exchange Online-Nutzung ausführen. Diese Berichte finden Sie auch in der Administrationsoberfläche von Exchange Online.	siehe Abschnitt 2.6, »Berichte«
Dienststatus	Im Bereich Dienststatus finden Sie detailliert aufgeführt, ob es im Zeitraum der vergangenen sieben Tage zu einem Ausfall der Office 365-Dienste gekommen ist. Auch den Verlauf der letzten 30 Tage können Sie sich ausgeben lassen. Bei Problemen mit Office 365 lohnt sich ein Blick in den Dienststatus, um einen Hinweis zu bekommen, ob es ein generelles oder möglicherweise eher ein lokales Problem ist.	siehe Abschnitt 2.8, »Dienststatus«
Support	Der Bereich Support ist die erste Anlaufstelle, wenn Sie Unterstützung bei der Behebung von Problemen mit Office 365 benötigen. Er enthält neben den Telefonnummern des Supports auch das Ticketsystem und Links auf verschiedene Tools und die Community.	siehe Abschnitt 2.11, »Problembehebung«

Tabelle 2.1 Administrationsbereiche des Office 365 Admin Centers (Forts.)

Bereich	Bedeutung	Weitere Informationen
Dienste kaufen	In diesem Bereich schließen Sie direkt über Ihr Office 365 weitere Abonnements über zusätzliche Lizenzen an.	siehe Abschnitt 2.3, »Abonnements«
Nachrichtencenter	Dieser letzte Bereich hält Sie über Probleme, Neuerungen und allgemeine Informationen rund um Ihren Office 365-Mandanten auf dem Laufenden.	siehe Abschnitt 2.9, »Nachrichtencenter«
Administrator	Von hier aus gelangen Sie zu den speziellen Administrationsoberflächen der Office 365-Dienste. So verfügt beispielsweise Exchange Online über eine eigene Oberfläche, das Exchange Admin Center.	

Tabelle 2.1 Administrationsbereiche des Office 365 Admin Centers (Forts.)

2.3 Abonnements

Zur Verwaltung Ihrer Abonnements und der darin enthaltenen Lizenzen enthält das Office 365 Admin Center den Bereich Abrechnung.

Unter dem Abschnitt Abonnements erhalten Sie eine Liste aller Abonnements des Mandanten mit Lizenztyp, Anzahl, Kosten und Ablaufdatum. Die einzelnen Listeneinträge sind Links zu den Abonnementdetails, von wo aus Sie die automatische Verlängerung konfigurieren können (siehe Abbildung 2.14).

Abbildung 2.14 Abonnementdetails

Der Bereich Lizenzen enthält eine summierte Ansicht der jeweiligen Lizenzen über alle aktiven Abonnements (siehe Abbildung 2.15).

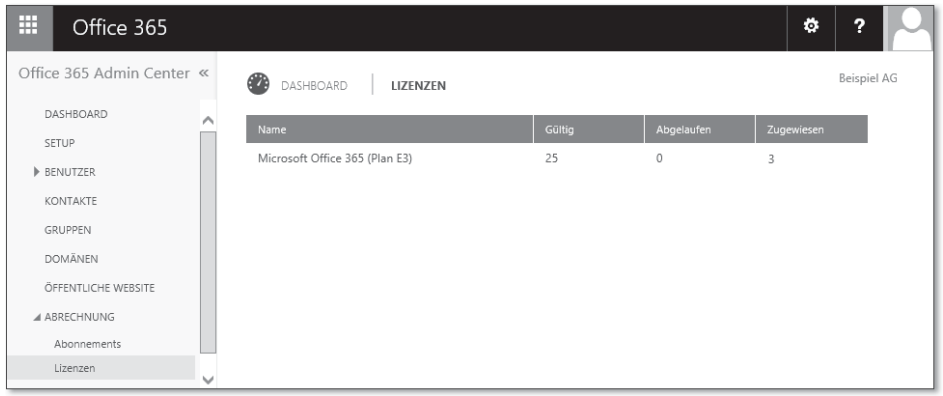

Abbildung 2.15 Lizenzübersicht

Wollen Sie weitere Lizenzen kaufen, wählen Sie in der linken Navigation den Bereich Dienste kaufen (siehe Abbildung 2.16). In der Auswahlliste sehen Sie dabei nicht nur Office 365-Produkte, sondern auch andere, wie *Dynamics CRM Online*.

Abbildung 2.16 Lizenzerwerb

2.3.1 Lizenzwechsel

Wollen Sie früher von einem Lizenztyp zu einem anderen Lizenztyp wechseln, sind dazu grundsätzlich folgende Schritte erforderlich:

1. Abschließen eines neuen Abonnements für den neuen Lizenztyp
2. Manuelles Zuweisen der neuen Lizenzen zu den Benutzern (mithilfe des Office 365-Portals oder der PowerShell)
3. Kontaktieren des Office 365-Kundendiensts, um das alte Abonnement zu beenden

In machen Konstellationen ist dieser manuelle Vorgang nicht nötig, sondern Sie können stattdessen einen Assistenten mit dem Lizenzwechsel beauftragen.

Um einen Lizenzwechsel über den Assistenten durchzuführen, müssen Sie sich über einige Einschränkungen im Klaren sein:

- Wechseln Sie einen Lizenztyp, erhalten alle Benutzer, denen der alte Lizenztyp zugewiesen ist, den neuen Lizenztyp. Eine Auswahl, welche Benutzer den neuen Lizenztyp erhalten sollen, ist nicht möglich.
- Sie können den Assistenten nur dann einsetzen, wenn maximal 300 Benutzern der zu wechselnde Lizenztyp zugewiesen ist.
- Den Assistenten können Sie nur dann einsetzen, wenn Sie Ihre Office 365-Lizenzen nicht über Produktschlüssel oder Lizenzprogramme erworben haben (Office 365-Produktschlüssel erhalten Sie beispielsweise auf einer Karte, verpackt in einer Pappschachtel, im Elektronikfachhandel).
- Sie können den Assistenten nur beim Wechsel bestimmter Lizenztypen einsetzen (siehe Tabelle 2.2).
- Der Wechsel ist nur möglich, wenn Sie Ihre Office 365-Lizenzen direkt in Ihrem Office 365-Mandanten gebucht haben und nicht über Händler oder Partner im Rahmen von Lizenzprogrammen.

Sollte eine dieser Einschränkungen dazu führen, dass Sie den Assistenten nicht einsetzen können oder wollen, bleibt Ihnen nur der manuelle Vorgang beim Lizenzwechsel.

Ausgangs-Lizenztyp	Ziel-Lizenztyp
K1, K2	E1, E3, E4
E1	E3, E4
E3	E4
Lync Online Plan 1 und 2	E1, E3, E4
Lync Online Plan 3	E4
SharePoint Online Plan 1	E1, E3, E4

Tabelle 2.2 Wechselmöglichkeiten

Ausgangs-Lizenztyp	Ziel-Lizenztyp
SharePoint Online Plan 2	E3, E4
Exchange Online Plan 1	E1, E3, E4
Exchange Online Plan 2	E3, E4
Exchange Online Kiosk	▸ E1, E3, E4, K1 ▸ Exchange Online Plan 1 und 2

Tabelle 2.2 Wechselmöglichkeiten (Forts.)

Den Assistenten zum Lizenzwechseln finden Sie im Office 365 Admin Center. Dort wechseln Sie in den Bereich ABRECHNUNG und dann zum Abschnitt ABONNEMENTS. Markieren Sie dort das betroffene Abonnement und wählen einen Wechseltarif.

Im Rahmen des Assistenten schließen Sie ein neues Abonnement ab. Der Assistent wird dann alle betroffenen Benutzerkonten automatisch mit dem neuen Lizenztyp ausstatten und das alte Abonnement beenden. Ungenutzte Gebühren aus dem alten Abonnement erhalten Sie erstattet.

Der Lizenzwechsel selbst dauert einige Minuten.

2.3.2 Kündigen von Abonnements

Grundsätzlich verlängern sich Abonnements nach Ende der Laufzeit automatisch – ganz ähnlich, wie Sie es von Zeitschriftenabonnements kennen. Allerdings weist Sie Microsoft schon lange vor dem Ablauf des Abonnements per E-Mail darauf hin. Außerdem erhalten Sie im Office 365 Admin Center deutliche Warnungen.

Um die automatische Verlängerung zu verhindern, öffnen Sie im Office 365 Admin Center den Bereich ABRECHNUNGEN und dann den Abschnitt ABONNEMENTS. Markieren Sie das betroffene Abonnement und geben Sie den Befehl AUTOMATISCHE VERLÄNGERUNG DEAKTIVIEREN.

An derselben Stelle ist auch ein vorzeitiges Kündigen eines Abonnements möglich – sofern Sie die Voraussetzungen dafür erfüllen (siehe Abschnitt 1.1.3, »Lizenzierung«).

2.4 Domänenverwaltung

Beim Erstellen Ihrer Office 365-Umgebung haben Sie sich bereits einen Domänennamen mit der Endung *onmicrosoft.com* ausgesucht, beispielsweise *beispielag.onmicrosoft.com* (siehe Abschnitt 2.1, »Anlegen eines Office 365-Mandanten«). Diese Domäne ist zwar voll funktionsfähig, doch werden Sie diese beispielsweise kaum für E-Mail-

Adressen in der Art von *lucy@beispielag.onmicrosoft.com* verwenden wollen. Auch soll Ihre öffentliche SharePoint-Website unter Ihrer eigenen Domäne und nicht unter dieser Standarddomäne erreichbar sein.

Sie können eigene Domänen zu Ihrer Office 365-Umgebung hinzufügen, und zwar nicht nur eine, sondern (derzeit) bis zu 900. Jede Domäne kann aber nur genau einem Office 365-Mandanten zugeordnet sein.

[»] Diesen Aspekt sollten Sie insbesondere bei Office 365-Mandanten berücksichtigen, die Sie nur zum Test angelegt haben. Bevor der Testzeitraum abgelaufen ist, sollten Sie Ihre eigenen Domänen aus dem Mandanten wieder entfernen. In diesem Abschnitt erfahren Sie, wie das geht.

Der Prozess zum Hinzufügen einer Domäne ist allerdings in der Praxis nicht ganz unproblematisch und besteht aus mehreren Schritten. Ein wesentlicher Punkt dabei ist, dass Sie beweisen müssen, dass Ihre Domäne auch wirklich unter Ihrer Kontrolle steht. Man spricht hier von einer *Verifikation*. Dazu werden Sie angewiesen, in der DNS-Konfiguration Ihrer Domäne (also typischerweise beim Hoster oder bei der Domänenregistrierungsstelle, über die Sie die Domäne registriert haben) einen bestimmten Eintrag zu hinterlegen. Doch nicht alle Hoster unterstützen dies in der erforderlichen Form. Sollte es hier Probleme geben, müssen Sie die Domäne zunächst zu einem anderen Anbieter umziehen. Der komplette Umzug einer Domäne zu Microsoft ist nicht möglich, sondern es ist nach wie vor ein externer DNS-Anbieter erforderlich.

Tabelle 2.3 erläutert die verschiedenen Typen von DNS-Einträgen, die für Office 365 eine Relevanz haben.

Typ	Bedeutung	Beschreibung
A	*Address Record*	Mit einem A-Eintrag weisen Sie einem *Hostnamen* eine IP-Adresse zu, also beispielsweise *remote.beispielag.de* zu 84.160.10.122. Einen A-Eintrag benötigen Sie möglicherweise bei der Einrichtung eines *Identitätsverbunds* (siehe Abschnitt 4.3, »Identitätsverbund für Single Sign-on«).
CNAME	*Canonical Name Record*	Ein CNAME-Eintrag wird auch *Alias* genannt. Mit ihm weisen Sie einem Hostnamen einen anderen Hostnamen zu, beispielsweise *beispielag.sharepoint.com* für *www.beispielag.de*. CNAME-Einträge benötigen Sie für *Exchange-AutoErmittlung (Autodiscover)*, Lync und SharePoint.

Tabelle 2.3 Typen von DNS-Einträgen

Typ	Bedeutung	Beschreibung
MX	*Mail Exchange Record*	Mit einem MX-Eintrag wird der Hostname oder die IP-Adresse des E-Mail-Systems für die jeweilige Domäne angegeben. MX-Einträge werden mit einer *Priorität* konfiguriert. Wenn mehrere MX-Einträge vorhanden sind, wird zuerst versucht, beim E-Mail-System mit der kleinsten Priorität E-Mails auszuliefern. Sollte das nicht möglich sein, werden die anderen E-Mail-Systeme in aufsteigender Priorität kontaktiert. Einen MX-Eintrag benötigen Sie bei Exchange Online für den eingehenden E-Mail-Verkehr.
SRV	*Service Locator*	Mit SRV-Einträgen können Dienste aufgefunden werden. Für Lync Online müssen Sie SRV-Einträge anlegen.
TXT	*Text Record*	Wie der Name schon sagt, handelt es sich bei TXT-Einträgen um Text. Einen TXT-Eintrag benötigen Sie für die Verifikation einer eigenen Domäne in Ihrem Office 365-Mandanten (oder alternativ einen MX-Eintrag).

Tabelle 2.3 Typen von DNS-Einträgen (Forts.)

2.4.1 Voraussetzungen an DNS-Anbieter

Damit Sie Ihre eigene Domäne erfolgreich in Office 365 einbinden und alle Dienste uneingeschränkt nutzen können, muss Ihr DNS-Anbieter einige Voraussetzungen erfüllen. Stellen Sie am besten schon vorher sicher, dass diese erfüllt sind, um nicht mitten im Integrationsprozess vor Problemen zu stehen. Achten Sie insbesondere darauf, dass der von Ihnen gebuchte Tarif beim DNS-Anbieter auch die entsprechenden Funktionen enthält; manchmal unterscheiden sich diese je nach Tarif.

In Tabelle 2.4 finden Sie eine Übersicht der Voraussetzungen.

Dienst	Erforderliche Einträge
Domänenverifikation	▸ Anlegen eines TXT-Eintrags für Ihre Domäne (das Anlegen einer Subdomäne ist nicht ausreichend) oder alternativ ▸ Anlegen eines MX-Eintrags
Basisfunktionalität	▸ Anlegen eines CNAME-Eintrags

Tabelle 2.4 Voraussetzungen DNS-Anbieter

Dienst	Erforderliche Einträge
Exchange Online	► Anlegen eines MX-Eintrags ► Anlegen eines TXT-Eintrags ► Anlegen eines CNAME-Eintrags
SharePoint Online	Anlegen eines CNAME-Eintrags (sofern die öffentliche Website unter Ihrer Domäne erreichbar sein soll)
Lync Online	► Anlegen von SRV-Einträgen ► Anlegen von CNAME-Einträgen

Tabelle 2.4 Voraussetzungen DNS-Anbieter (Forts.)

2.4.2 Domäne verifizieren

Im Office 365 Admin Center (*https://portal.office.com*) klicken Sie auf den Bereich Domänen (siehe Abbildung 2.17).

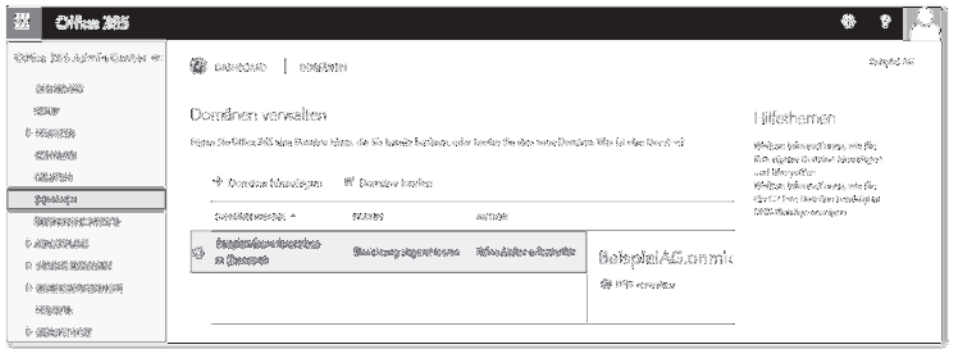

Abbildung 2.17 Domänenverwaltung im Office 365 Admin Center

In der Liste finden Sie alle Domänen, die in der Office 365-Umgebung eingetragen wurden. Die Spalte Status gibt Auskunft darüber, ob die jeweilige Domäne bereits erfolgreich verifiziert wurde. Tabelle 2.5 führt alle möglichen Stadien und deren jeweilige Bedeutung auf.

Status	Bedeutung
Einrichtung abgeschlossen	Die Domäne wurde erfolgreich zur Office 365-Umgebung hinzugefügt und kann verwendet werden.
Einrichtung abgeschlossen (DNS-Überprüfung ausgeschaltet)	Wie oben, jedoch erfolgt keine automatische Überprüfung der DNS-Einträge.

Tabelle 2.5 Domänenstadien

Status	Bedeutung
Die Einrichtung wurde nicht gestartet	Eine Domäne befindet sich im Verifikationsprozess. Dieser wurde aber noch nicht abgeschlossen.
Einrichtung wird ausgeführt (die Domäne wurde überprüft)	Die Domäne wurde erfolgreich verifiziert und befindet sich jetzt in der DNS-Konfiguration.
Mögliche Dienstprobleme	Die DNS-Einstellungen der Domäne werden regelmäßig überprüft. Sollte ein Problem festgestellt werden, können Sie die Ursache hier abrufen.

Tabelle 2.5 Domänenstadien (Forts.)

Ihre *onmicrosoft.com*-Domäne kann aus der Liste nicht entfernt werden, wohl aber können Sie über Domäne hinzufügen den Prozess zur Aufnahme einer eigenen Domäne starten. Dieser Vorgang läuft über folgende Schritte ab:

1. Domäne überprüfen
2. Benutzer hinzufügen
3. Domäne einrichten

Im Folgenden beschreibe ich jeden dieser Schritte.

Schritt 1: Domäne überprüfen

Geben Sie zunächst Ihren Domänennamen ein. In Abbildung 2.18 finden Sie das Fenster dazu abgebildet.

Verfügen Sie nur über Office 365 Business Essentials-Lizenzen, können Sie nur 2nd-Level-Domains hinzufügen (wie *beispielag.de*) und keine 3rd-Level-Domains (wie *vertrieb.beispielag.de*). [«]

Weiter geht es mit der Bestätigung des Domänenbesitzes (*Verifikation*), was gerne einmal problematisch wird. Sie erhalten die Anweisung, in der DNS-Konfiguration Ihrer Domäne wahlweise einen Textdatensatz (TXT) oder einen MX-Datensatz hinzuzufügen.

Für manche DNS-Anbieter liefert das Portal entsprechende Anleitungen, darunter *Go Daddy* und *Register.com*. Die in der Auswahl verfügbaren Anbieter werden allerdings, in unseren Breitengraden seltener eingesetzt. Ist Ihr Anbieter nicht enthalten, wählen Sie stattdessen die Option Allgemeine Anweisungen. Dabei erhalten Sie einen Textvorschlag, den Sie an Ihren DNS-Anbieter senden können, falls Sie den Eintrag nicht selbst anlegen können oder wollen.

Abbildung 2.18 Domäne angeben

Der Textdatensatz für die Überprüfung ist die bevorzugte Methode. Sollte es dabei Probleme geben oder die DNS-Konfiguration Ihres Hosters keine Textdatensätze zulassen, wählen Sie die MX-Alternative.

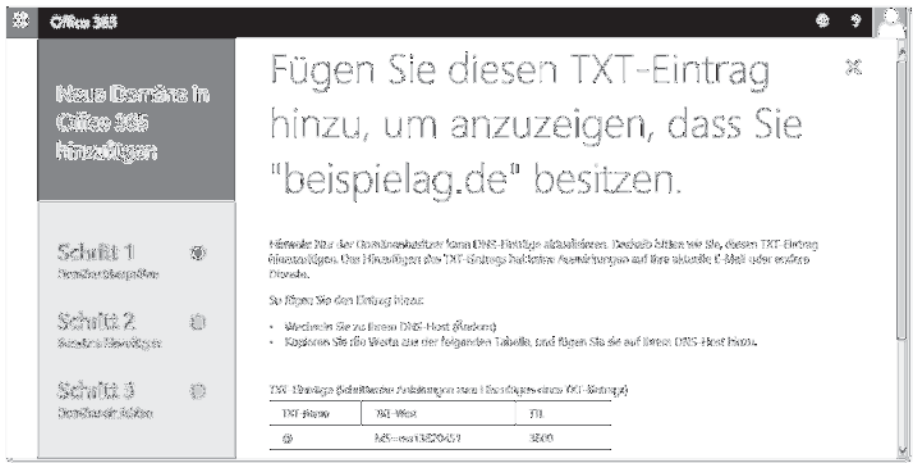

Abbildung 2.19 Domäne überprüfen

Ein Beispiel: Es soll die Domäne *beispielag.de* zur Office 365-Umgebung hinzugefügt werden. Der Textdatensatz wird wie folgt vorgegeben (siehe Abbildung 2.19):

- TXT-Name: `@`
- TXT-Wert: `MS=ms13820451`
  Achten Sie beim Erstellen des Textdatensatzes auf die korrekte Schreibweise mit Groß- und Kleinschreibung. Vermeiden Sie es auch, Leerzeichen mit einzufügen, insbesondere am Ende des Textes. Das passiert gerne, wenn Sie die Zwischenablage verwenden.

- TTL: 3600
  Nicht bei jedem Anbieter kann die Gültigkeitsdauer vorgegeben werden. In diesem Fall lassen Sie sie einfach weg.

Um diesen Vorgang zu verdeutlichen, zeige ich Ihnen anhand des Anbieters *Host Europe* im Kasten die entsprechende Vorgehensweise. Anleitungen für viele weitere Anbieter wie *1&1*, *Strato*, *domainFactory*, *Server4You* etc. finden Sie unter folgender URL: *http://community.office365.com/de-de/w/administration/default.aspx*

Domänenverifizierung mit Host Europe

Um den erforderlichen TXT-Eintrag bei Host Europe vorzunehmen, gehen Sie wie folgt vor:

- Melden Sie sich im Kunden-Informations-System (KIS) an. Die URL lautet: *https://kis.hosteurope.de*
- Wechseln Sie zum Bereich Administrator • Domainservices.
- Wählen Sie den Punkt AutoDNS Domains bearbeiten.
- Klicken Sie auf die Schaltfläche Editieren in der Zeile mit der gewünschten Domäne.
- Gehen Sie in der Tabelle DNS-Einträge ans Ende, und wählen Sie dort in der mittleren Spalte den Eintrags-Typ TXT. In das rechte Textfeld geben Sie die Zeichenfolge an, die Sie von Office 365 erhalten haben (`MS=ms13820451`; siehe Abbildung 2.20).

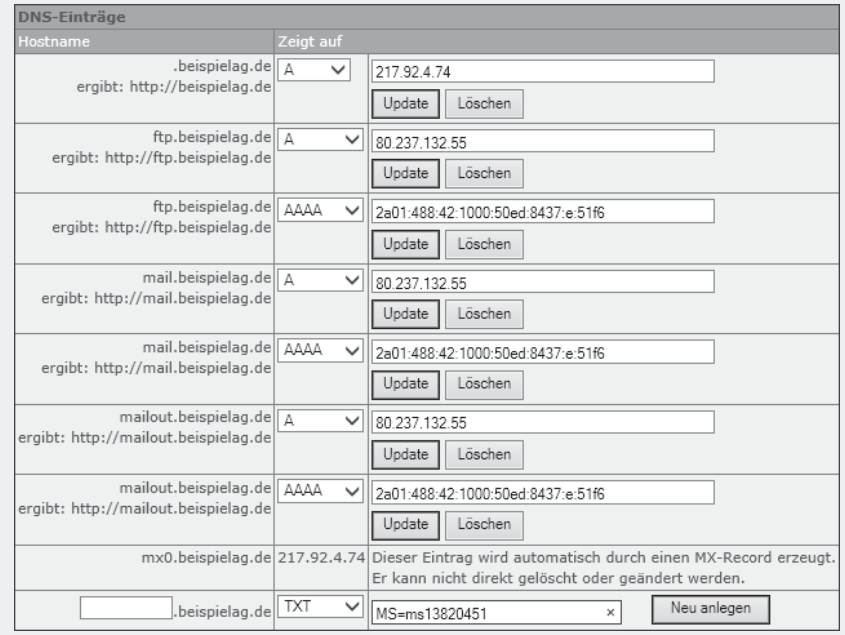

Abbildung 2.20 Neuer TXT-Eintrag

- Klicken Sie auf NEU ANLEGEN.
- Warten Sie fünf Minuten.

[»] Bei Host Europe reicht das erfahrungsgemäß aus, bis der neue Eintrag aktiv wird und von Office 365 erkannt werden kann.

Nachdem Sie den erforderlichen Eintrag in der DNS-Konfiguration bei Ihrem Anbieter hinterlegt haben, heißt es warten. Die Konfigurationsänderung muss sich erst in der DNS-Infrastruktur verbreiten. Dieser Vorgang kann zwischen wenigen Minuten und mehreren Tagen dauern. Sie können testweise auf die Schaltfläche OK, ICH HABE DEN EINTRAG HINZUGEFÜGT klicken. Kann Office 365 die Konfiguration nicht finden, erhalten Sie die Fehlermeldung aus Abbildung 2.21.

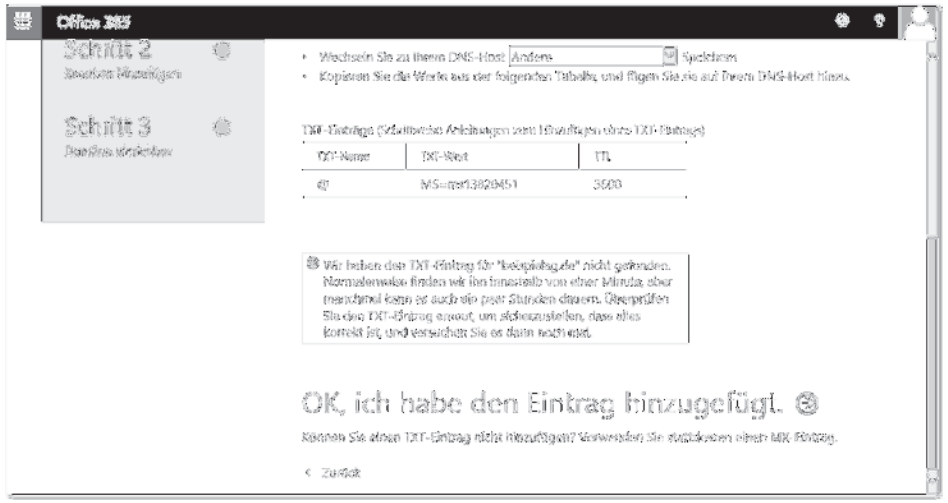

Abbildung 2.21 Fehlgeschlagene Domänenverifizierung

Haben Sie zwischenzeitlich das Office 365 Admin Center verlassen, gelangen Sie über folgenden Weg wieder zurück: Ausgehend von der Domänenliste klicken Sie auf den neben der Domäne auf EINRICHTUNG STARTEN.

Will Office 365 Ihre DNS-Konfiguration nicht erkennen, können Sie selbst sicherstellen, dass Ihr DNS-Anbieter die DNS-Einträge korrekt in seiner DNS-Infrastruktur publiziert hat. Auf Websites wie *www.dnsquery.org* geben Sie Ihren Domänennamen ein und erhalten daraufhin die entsprechenden DNS-Einträge geliefert (siehe Abbildung 2.22). Beispiel: Auf der Website geben Sie unter DNS RECORD QUERY den zu überprüfenden Domänennamen ein, die Auswahl lassen Sie auf ANY, und dann klicken Sie auf QUERY.

Unter STEP 3 stehen dann die DNS-Einträge (siehe Abbildung 2.23). Ist dort der erforderliche Eintrag nicht zu sehen, kann ihn Office 365 auch nicht auslesen. Überprüfen Sie in diesem Fall die DNS-Konfiguration.

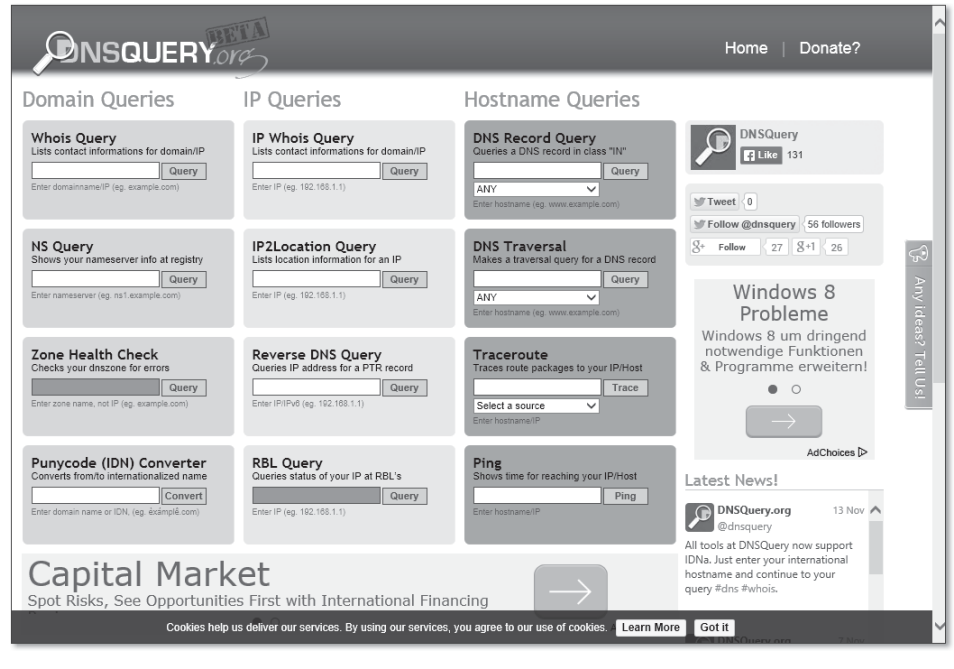

Abbildung 2.22 Abfrage von DNS-Informationen

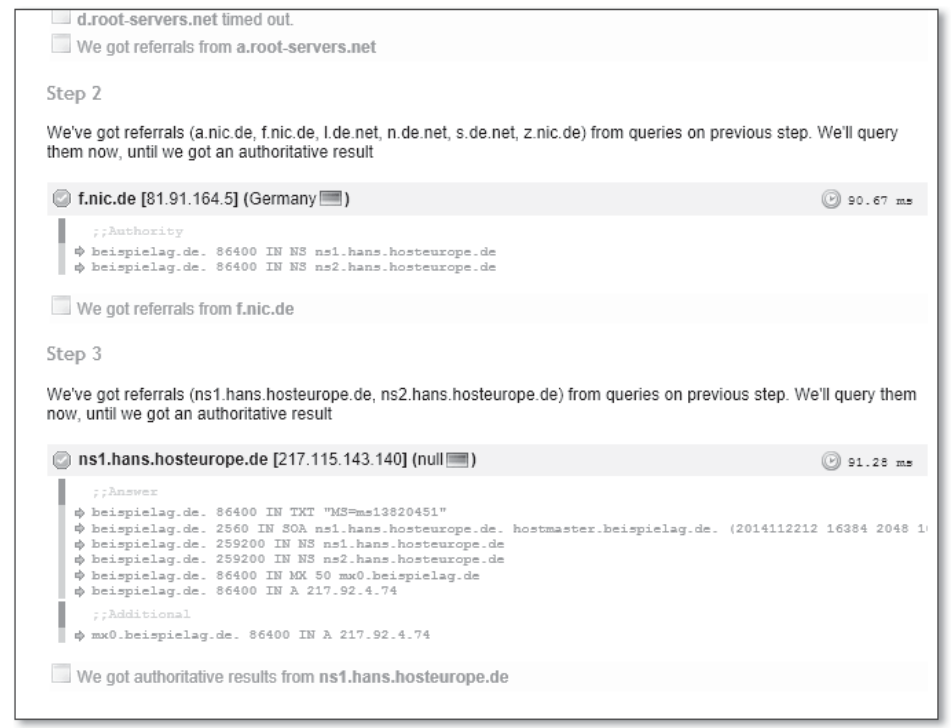

Abbildung 2.23 Ergebnis der DNS-Abfrage

[»] Theoretisch könnten Sie statt einer derartigen Website auch das Kommandozeilentool `nslookup` verwenden. Dabei müssen Sie aber beachten, dass dann die Ergebnisse gegebenenfalls nicht vom DNS-Server Ihres Providers beantwortet werden, sondern von Ihrem lokalen DNS-Server.

Hat das Überprüfen dann tatsächlich geklappt, kann es mit dem nächsten Schritt weitergehen.

Schritt 2: Benutzer hinzufügen

Wahlweise können Sie jetzt die E-Mail-Adressen (und auch die Benutzernamen) der vorhandenen Benutzerkonten auf die neue Domäne aktualisieren (siehe Abbildung 2.24).

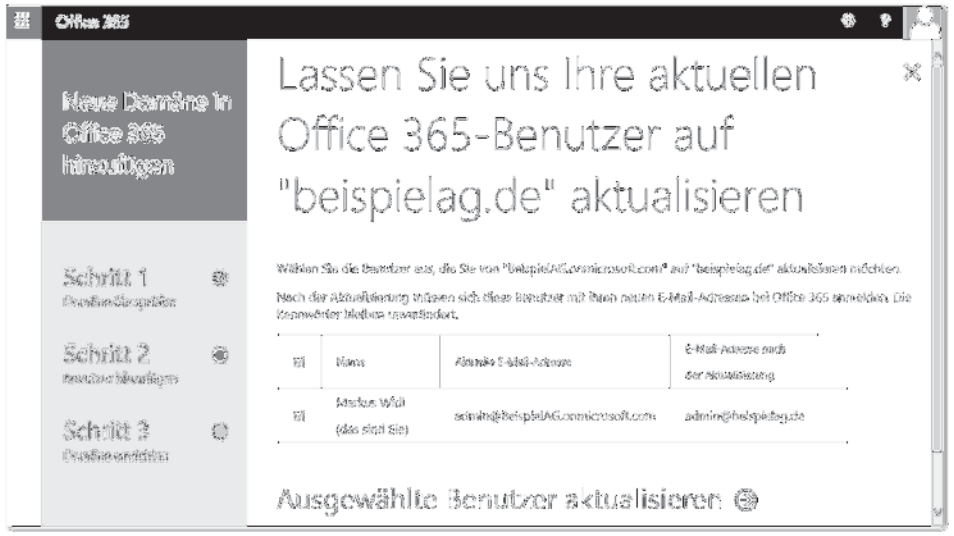

Abbildung 2.24 Benutzernamen und E-Mail-Adressen aktualisieren?

Danach können Sie in diesem Schritt einzelne Benutzer anlegen oder mithilfe einer CSV-Datei auch viele auf einmal erstellen. Ob Sie das wirklich jetzt tun, hängt von mehreren Faktoren ab. Der wichtigste dabei ist: Sie müssen entscheiden, ob Sie die Benutzerkonten tatsächlich manuell in Ihrem Office 365-Mandanten anlegen oder ob Sie das lieber über die optionale Active-Directory-Synchronisierung durchführen lassen wollen. Dabei hilft Ihnen ein Tool nicht nur, administrative Arbeit zu sparen (beispielsweise das doppelte Verwalten von Benutzerkonten – einmal lokal in Ihrem Active Directory und einmal in Office 365), sondern ist auch die Voraussetzung für manche Szenarien, wie für Single Sign-on. Aus diesem Grund lesen Sie zunächst in Abschnitt 2.5, »Benutzerverwaltung«, nach, ob es für Sie sinnvoll ist, in Office 365 direkt Benutzer anzulegen. Wenn nicht, wählen Sie die Option zum Überspringen dieses Schritts (siehe Abbildung 2.25).

Abbildung 2.25 Benutzer jetzt hinzufügen?

Auch wenn Sie Benutzerkonten in Office 365 anlegen wollen, müssen Sie dies nicht gleich jetzt tun.

Schritt 3: Domäne einrichten

Office 365 benötigt von Ihnen die Angabe, ob Sie unter dieser bereits eine Website betreiben (siehe Abbildung 2.26). Abhängig davon wird die weitere DNS-Konfiguration angepasst.

Abbildung 2.26 Besteht bereits eine Website?

Danach wird vorgeschlagen, dass Sie die aktuellen Nameserver Ihrer Domäne zu den Microsoft-Nameservern ändern wollen. (siehe Abbildung 2.27). Damit hätten Sie mit der weiteren DNS-Konfiguration nichts mehr zu tun, haben dann aber auch keinen Einfluss darauf, wie die DNS-Einträge gesetzt werden.

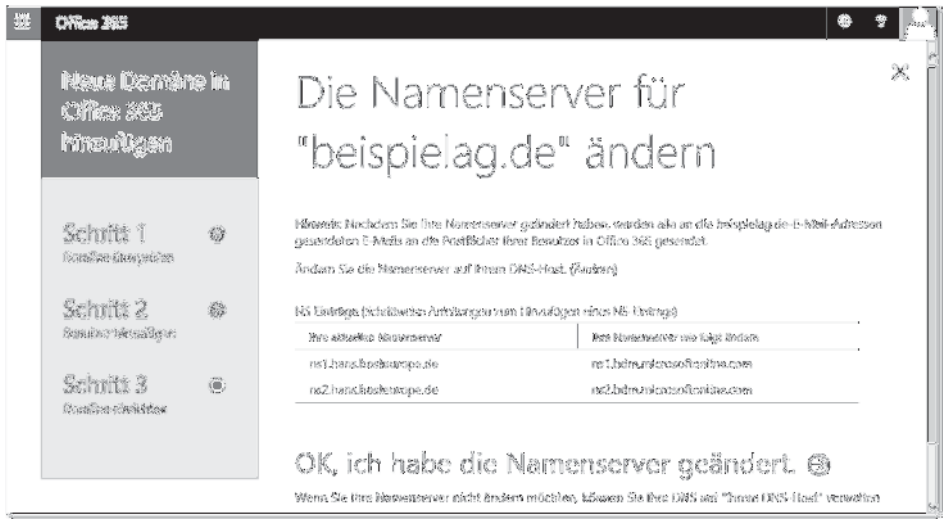

Abbildung 2.27 Änderung der Nameserver-Einträge?

Um die volle Flexibilität zu erhalten, klicken Sie auf DNS AUF "IHREM DNS-HOST" VERWALTEN.

Der Assistent fragt dann, mit welchen Diensten Sie die Domäne nutzen wollen (also EXCHANGE ONLINE und/oder LYNC ONLINE; siehe Abbildung 2.28).

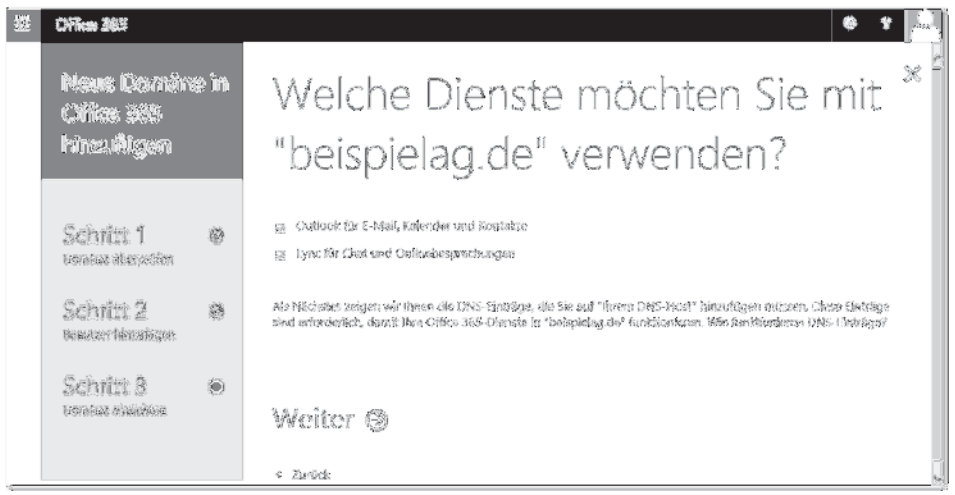

Abbildung 2.28 Dienstauswahl

Abhängig von den gewählten Diensten sind dann noch weitere Einträge in der DNS-Konfiguration Ihrer Domäne erforderlich. Ein Beispiel für Exchange Online und Lync Online sehen Sie in Abbildung 2.29.

Abbildung 2.29 DNS-Einstellungen

Diese DNS-Einträge sollten Sie erst erstellen bzw. ändern, wenn Sie die eventuell erforderliche Migration von bestehenden Systemen geplant und durchgeführt haben. Müssen Sie beispielsweise zunächst ein vorhandenes E-Mail-System migrieren, ändern Sie nicht sofort den MX-Eintrag, was nämlich zur Folge hätte, dass E-Mails bei Exchange Online und nicht bei Ihrem bestehenden E-Mail-System ausgeliefert würden. Informationen zur E-Mail-Migration finden Sie in Abschnitt 6.12, »Migration«. Brechen Sie also gegebenenfalls den Assistenten an dieser Stelle ab. In der Domänenverwaltung steht bei der Domäne dann der Status EINRICHTUNG WIRD AUSGEFÜHRT (DIE DOMÄNE WURDE ÜBERPRÜFT). Markieren Sie hier die Domäne und wählen dann die Aktion PROBLEME SUCHEN UND BEHEBEN. Sie erhalten dann die Option DIESE DOMÄNE NICHT AUF FEHLERHAFTE DNS-EINTRÄGE PRÜFEN, um die Warnmeldungen zu vermeiden (siehe Abbildung 2.30). [«]

Vergessen Sie im Zuge der Änderungen der DNS-Einträge bei Ihrem DNS-Anbieter nicht Ihren internen DNS-Server, sofern dort die hinzugefügte Domäne verwaltet wird (*Split DNS*). Ansonsten bekommen die internen Clients Probleme bei der Verbindung mit den Office 365-Diensten, da sie dafür keine oder eine alte Namensauflösung erhalten. Wichtig ist auch hier wieder, dass Sie die Einträge korrekt vornehmen, um ein einwandfreies Funktionieren der Office 365-Dienste zu ermöglichen. Allerdings gibt es hier keinen Verifikationsprozess wie bei der Aufnahme der Domäne in die Office 365-Umgebung. [«]

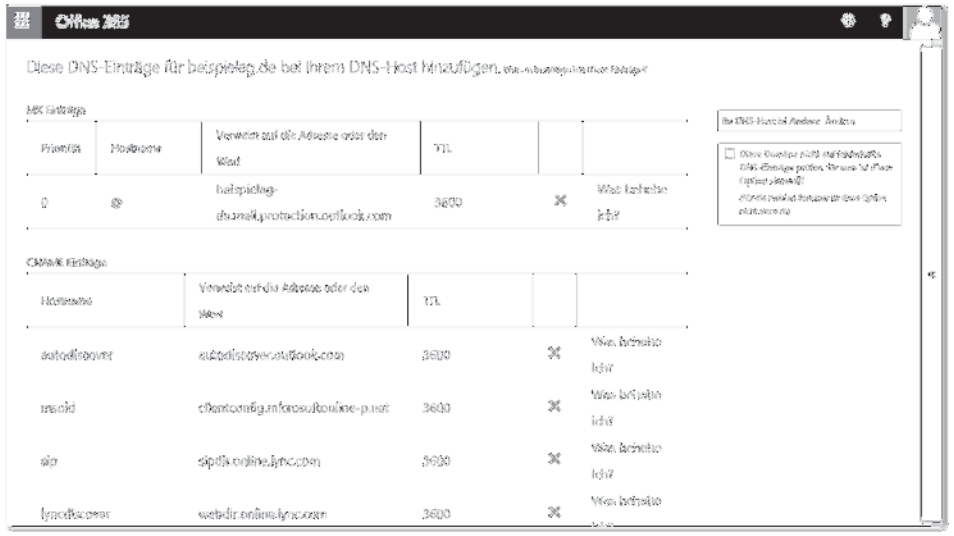

Abbildung 2.30 DNS-Überprüfung deaktivieren

Da hier das Vorgehen wieder stark abhängig ist von der Konfigurationsoberfläche Ihres Domänenanbieters, erläutere ich auch im folgenden Kasten als Beispiel erneut die Vorgehensweisen bei Host Europe (andere Anleitungen finden Sie unter *http://community.office365.com/de-de/w/administration/default.aspx*).

DNS-Einträge bei Host Europe

Beachten Sie zum Anlegen der DNS-Einträge bei Host Europe folgende Punkte:

- Exchange Online

  Den MX-Eintrag erstellen Sie in der Domänenverwaltung in der Tabelle MX-Records. Die Priorität setzen Sie nicht auf 0, sondern auf 1 (bei Host Europe ist dies der kleinstmögliche Wert). Das Präfix lassen Sie leer, und unter Hostname/IP geben Sie die Adresse an, wie sie von Office 365 geliefert wurde. Eine Angabe der Gültigkeitsdauer (TTL) für den Eintrag ist bei Host Europe nicht möglich, aber auch nicht unbedingt erforderlich. Ein Beispiel sehen Sie in Abbildung 2.31.

  Den CNAME-Eintrag erstellen Sie in der Tabelle DNS-Einträge. Die Gültigkeitsdauer bleibt wieder unberücksichtigt (siehe Abbildung 2.32).

  Den TXT-Eintrag erstellen Sie ebenfalls in der Tabelle DNS-Einträge. Das Textfeld Hostname lassen Sie dabei leer, und unter Hostname/IP geben Sie den vorgegebenen Text an. Die Gültigkeitsdauer fällt weg.

- Lync Online

  Den SRV-Eintrag erstellen Sie in der Domänenverwaltung in der Tabelle SRV-Records (siehe Abbildung 2.33). Die CNAME-Einträge erstellen Sie wie zuvor beschrieben.

- SharePoint Online

  Soll Ihre öffentliche SharePoint-Website unter Ihrer eigenen Domäne erreichbar sein, müssen Sie ebenfalls einen CNAME-Eintrag konfigurieren. Mehr dazu lesen Sie in Abschnitt 7.16.1, »Anlegen einer öffentlichen Website«.

- Zusätzliche Office 365-Einträge

  Den CNAME-Eintrag erstellen Sie wie zuvor beschrieben.

Abbildung 2.31 MX-Eintrag

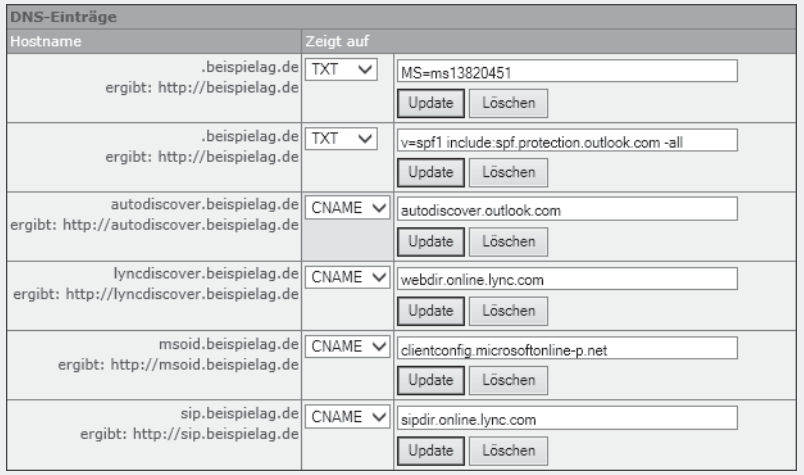

Abbildung 2.32 CNAME- und TXT-Einträge

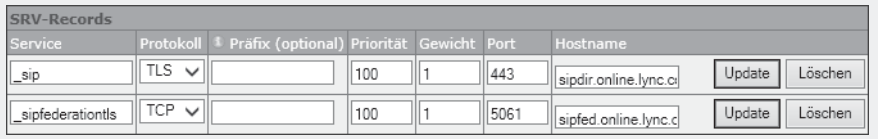

Abbildung 2.33 SRV-Eintrag

Nachdem Sie die Einträge vorgenommen haben, heißt es wieder warten – von wenigen Sekunden bis zu drei Tagen kann es dauern, bis Ihre Änderungen in der DNS-Infrastruktur veröffentlicht werden. Eine Website wie *www.dnsquery.org* kann wieder dabei helfen, zu überprüfen, ob die Konfiguration aktiv ist.

Um das Hinzufügen der Domäne abzuschließen, lassen Sie in Schritt 3 die DNS-Einstellungen überprüfen, indem Sie auf die Schaltfläche Fertig, Überprüfung starten klicken.

Danach ist es endlich geschafft – Sie können die neue Domäne für die ausgewählten Office 365-Dienste verwenden.

Domänenverifikation mithilfe der PowerShell

Die Domänenverifikation können Sie auch in der Kommandozeile über die PowerShell vornehmen. Das lohnt sich nicht unbedingt bei einer einzelnen Domäne, kann aber bei mehreren Domänen den Prozess etwas beschleunigen bzw. automatisieren. In Abschnitt 3.16.2, »Domänenverifikation«, finden Sie die dafür notwendigen Befehle.

2.4.3 Domäne entfernen

Aus der Domänenliste im Office 365 Admin Center können Sie bereits verifizierte Domänen auch wieder entfernen. Dazu darf die Domäne aber nicht mehr im Gebrauch sein, also beispielsweise weder beim Benutzernamen, bei E-Mail-Adressen, SharePoint, Lync oder als Standarddomäne zum Einsatz kommen.

Benutzernamen und Exchange Online

Wechseln Sie im Office 365 Admin Center im Bereich Benutzer zum Abschnitt Aktive Benutzer. Überprüfen Sie, ob im Benutzernamen irgendwo die zu löschende Domäne verwendet wird. Sollte dies der Fall sein, öffnen Sie den Benutzer und weisen ihm dann im Abschnitt Details eine andere Domäne zu (siehe Abbildung 2.34).

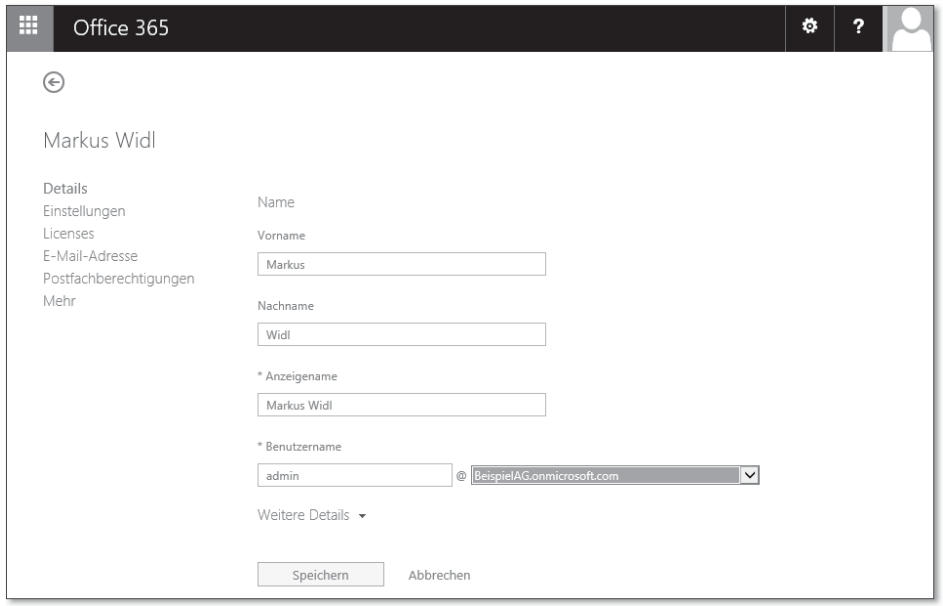

Abbildung 2.34 Domänenänderung bei einem Benutzer

Der Benutzername wird bei Exchange Online-Postfächern automatisch als E-Mail-Adresse verwendet. Sollten Sie in den Postfächern weitere E-Mail-Adressen mit der zu löschenden Domäne angegeben haben, müssen Sie diese auch entfernen. Lesen Sie hierzu Abschnitt 6.5.1, »Postfächer«.

Die hier vorgestellten Schritte gelten nicht bei Benutzern, die über die automatische Synchronisierung vom Active Directory aus angelegt wurden. Bei solchen Benutzern müssen Sie die Änderung lokal im Active Directory vornehmen, beispielsweise über die Managementkonsole *Active Directory Benutzer und Computer*. Zur Active-Directory-Synchronisierung lesen Sie mehr in Abschnitt 4.2, »Active-Directory-Synchronisierung«.

SharePoint Online

Öffnen Sie im SharePoint Admin Center den Bereich Websitesammlungen. Überprüfen Sie die Liste der URLs, und passen Sie diese gegebenenfalls an (siehe Abbildung 2.35).

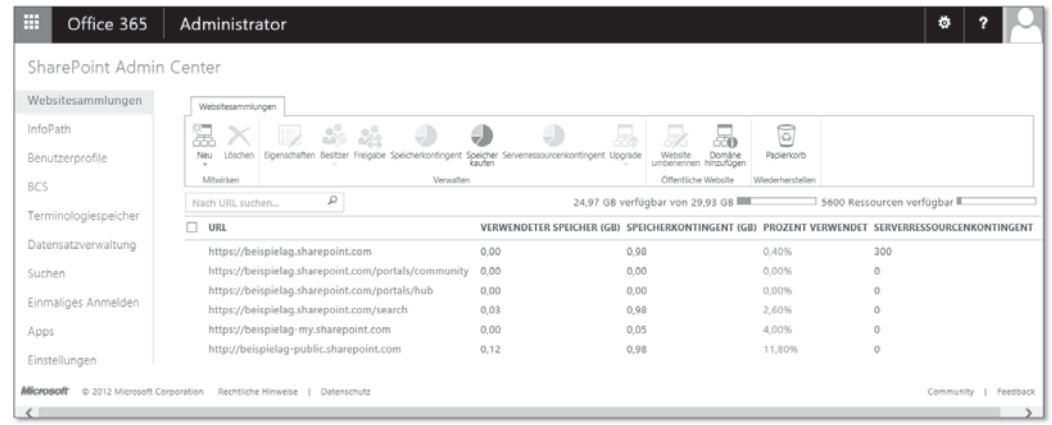

Abbildung 2.35 Überprüfen der Websitesammlungs-URLs

Lync Online

Für Lync Online-Benutzer wird automatisch eine *SIP-Adresse* vergeben, die grundsätzlich auch beim Ändern der Domäne des Benutzerkontos mit geändert wird.

Standarddomäne

Wechseln Sie im Office 365 Admin Center zum Bereich Dashboard, und klicken Sie dann auf den Namen Ihrer Organisation. Im erscheinenden Formular wählen Sie unter Standarddomäne eine andere als die, die Sie löschen wollen (siehe Abbildung 2.36).

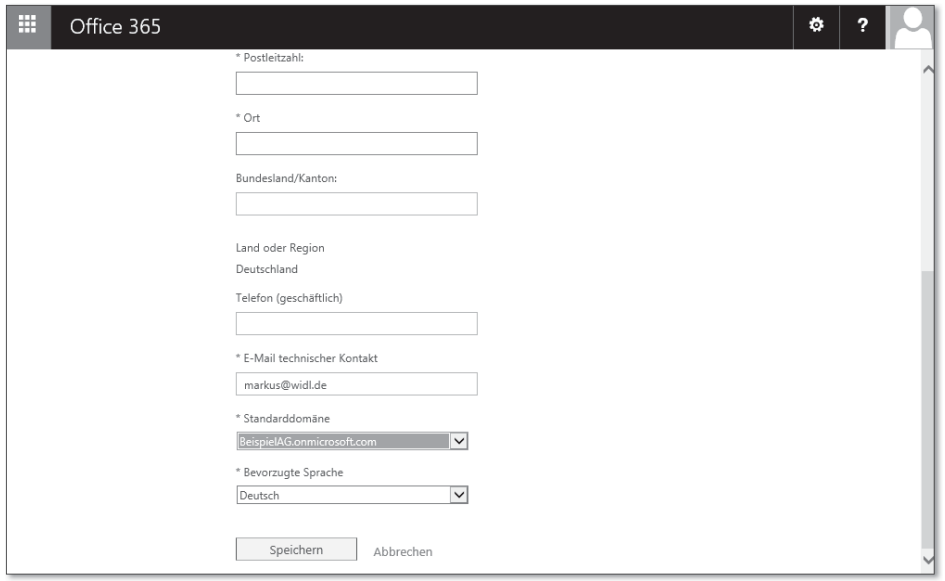

Abbildung 2.36 Ändern der Standarddomäne

In Abschnitt 3.16.2, »Domänenverifikation«, finden Sie ein PowerShell-Skript, mit dem Sie überprüfen können, wo eine Domäne noch angegeben ist. Mit der Ausgabe des Skripts bekommen Sie möglicherweise einen Hinweis darauf, warum eine Domäne nicht entfernt werden kann.

2.5 Benutzerverwaltung

Die Benutzerverwaltung rufen Sie im Office 365 Admin Center über den Punkt BENUTZER • AKTIVE BENUTZER in der linken Navigationsleiste auf (siehe Abbildung 2.37).

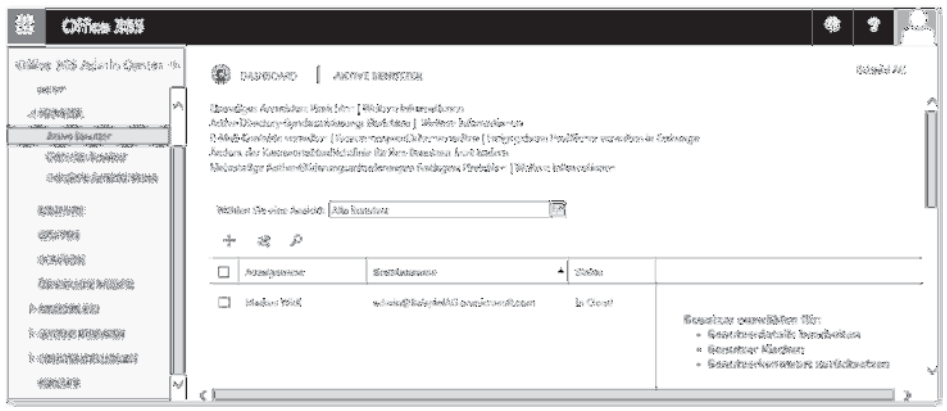

Abbildung 2.37 Benutzerverwaltung

Es hängt allerdings von Ihrer Umgebung ab, ob Sie dort tatsächlich manuell neue Benutzer anlegen oder ob diese automatisch über eine separate Anwendung, ein *Active-Directory-Verzeichnissynchronisierungstool*, angelegt werden. Damit Sie entscheiden können, welche Vorgehensweise für Ihre Umgebung geeignet ist, müssen wir zunächst den Begriff *Microsoft-Online-ID* klären.

2.5.1 Microsoft-Online-ID

So wie Sie in Ihrer lokalen Umgebung einen *Verzeichnisdienst* einsetzen – nämlich höchstwahrscheinlich das *Active Directory* –, verfügt auch Office 365 über einen eigenen Verzeichnisdienst mit dem Namen *Azure Active Directory (AAD)*. Bei den dort angelegten Benutzerkonten handelt es sich um *Microsoft-Online-IDs*. Sie benötigen zunächst für jeden Anwender eine solche Microsoft-Online-ID, die Sie dann mit der passenden Lizenz ausstatten und damit entscheiden, welche Office 365-Dienste der Anwender wie nutzen kann. Die Frage ist nun, ob Sie die IDs selbst anlegen (über das Office 365 Admin Center) oder anlegen lassen (über ein Active-Directory-Verzeichnissynchronisierungstool). Solch ein Synchronisierungstool wird auf einem Server im lokalen Netzwerk installiert und hat die Aufgabe, regelmäßig neue Active-Directory-Benutzer im Office 365-Verzeichnisdienst anzulegen, lokal gelöschte ebenfalls zu löschen etc. Das Tool kümmert sich dabei nicht nur um Benutzerkonten, sondern auch um Gruppen und Kontakte. Werden über so ein Tool neue Office 365-Benutzer angelegt, müssen Sie diese nachträglich mit einer entsprechenden Lizenz ausstatten, beispielsweise über das Office 365-Portal. Es gibt aber auch andere Wege, etwa automatisiert über die PowerShell. Außerdem benötigt der neue Office 365-Benutzer möglicherweise ein Kennwort. Manch ein Verzeichnissynchronisierungstool beherrscht aber auch eine Kennwortsynchronisierung, mit der das lokale Kennwort auch zur Anmeldung an Office 365 genutzt werden kann.

In diesem Abschnitt beschreibe ich das manuelle Anlegen von Benutzern über das Office 365-Portal. Die Vorgehensweise mit einem Active-Directory-Verzeichnissynchronisierungstool erläutere ich in Abschnitt 4.2, »Active-Directory-Synchronisierung«.

Unabhängig davon, wer nun letztendlich die Microsoft-Online-IDs anlegt, haben sie für den Endanwender zunächst einen Nachteil: Sie müssen sich bei der Anmeldung an einen Office 365-Dienst wie Exchange Online oder SharePoint Online erneut anmelden. Das heißt, der Anwender meldet sich typischerweise an seinem Computer mit seinem Active-Directory-Benutzerkonto an. Dann greift er etwa auf sein Exchange-Postfach zu. Dabei ist dann eine separate Anmeldung des Benutzers mit seiner Microsoft-Online-ID, also dem Benutzerkonto aus dem Office 365-Verzeichnisdienst, erforderlich. Der Aufbau ist in Abbildung 2.38 abgebildet.

Für den Endanwender ist das nicht die eleganteste Lösung, es gibt aber auch mit dem *Identitätsverbund* eine Alternative. Mithilfe dieser Technik kann sich der Anwender mit seinem Active-Directory-Benutzerkonto auch an den Office 365-Diensten anmel-

den (Stichwort *Single Sign-on*). In Abschnitt 4.3, »Identitätsverbund für Single Sign-on«, lesen Sie, wie das geht.

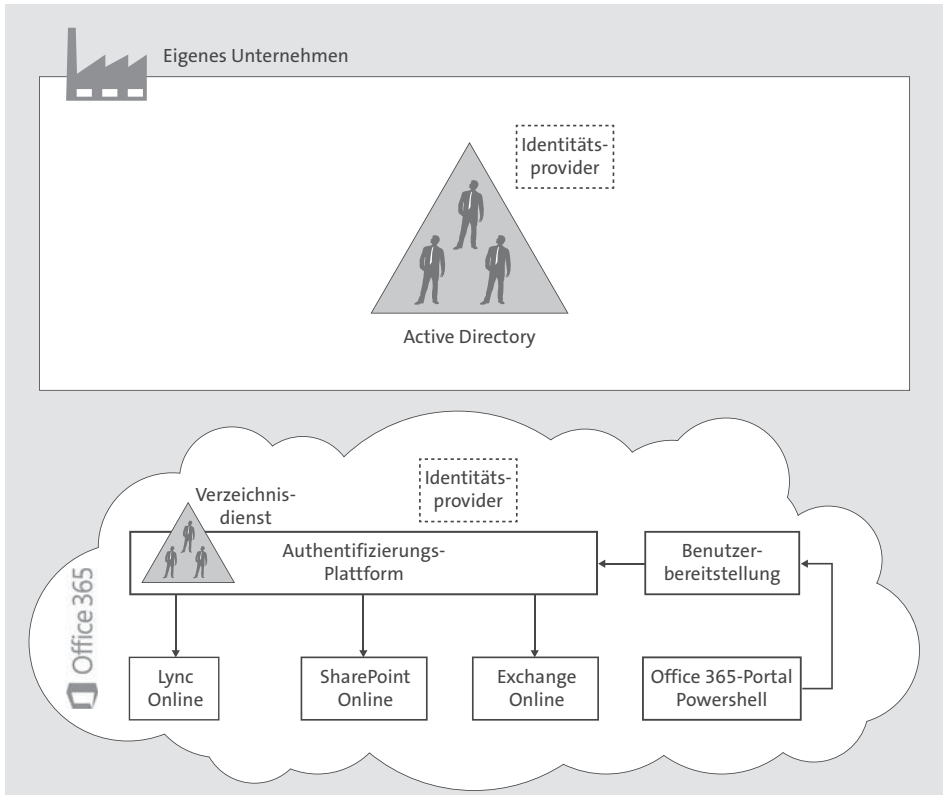

Abbildung 2.38 Verzeichnisdienste im eigenen Unternehmen und in Office 365

Entscheiden Sie sich für die Active-Directory-Synchronisierung, verwalten Sie Ihre Office 365-Benutzerkonten nicht über die Office 365-Benutzerverwaltung, sondern über die üblichen Tools Ihres lokalen Active Directorys, beispielsweise der Verwaltungskonsole *Active Directory Benutzer und Computer*.

[»] Eine weitere Hilfestellung für die Benutzeranmeldung stellt ein spezielles Add-in für den *Microsoft Windows Server 2012 (R2) Essentials* dar. Lesen Sie Details dazu in Abschnitt 12.5, »Windows Server 2012 (R2) Essentials«.

2.5.2 Benutzer anlegen

Ausgehend von der Benutzerverwaltung im Office 365 Admin Center klicken Sie auf NEU (PLUS-SYMBOL) für einen einzelnen Benutzer oder auf MASSENHINZUFÜGEN (rechts daneben) für viele Benutzer.

Einzelne Benutzer anlegen

Das Anlegen eines einzelnen Benutzers ist schnell erledigt (siehe Abbildung 2.39).

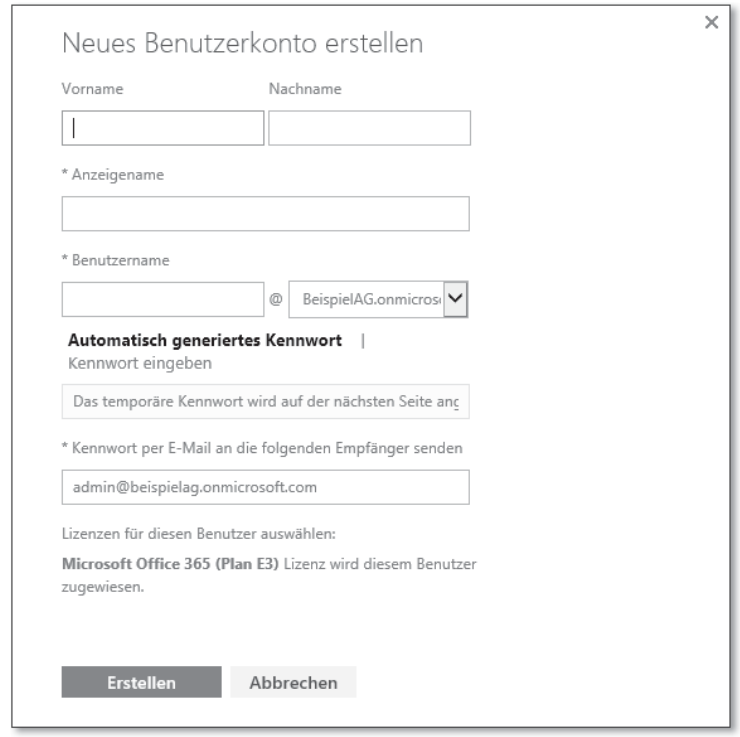

Abbildung 2.39 Anlegen eines Benutzers

Geben Sie neben einem Vor- und einem Nachnamen einen Anzeigenamen und den gewünschten Benutzernamen an. Die Auswahlliste bei der Domäne des Benutzernamens enthält die Mandantdomäne und gegebenenfalls weitere Domänen, die Sie bereits zu Ihrem Office 365-Mandanten hinzugefügt haben (siehe Abschnitt 2.4, »Domänenverwaltung«).

Soll der Benutzer später zum Administrator werden, müssen Sie den Vor- und den Nachnamen vergeben. Ansonsten sind diese beiden Angaben optional. [«]

Im Standardfall erzeugt Office 365 für den Benutzer ein Initialkennwort. Wollen Sie selbst das Initialkennwort vergeben, können Sie dies auf dem Formular tun. In beiden Fällen muss der Benutzer das Kennwort bei der ersten Anmeldung ändern. Wollen Sie das umgehen, hilft PowerShell (siehe Abschnitt 3.16.3, »Benutzer anlegen«). Unabhängig davon, wer das Kennwort vergibt, müssen Sie es an einen Empfänger per E-Mail senden lassen. Natürlich verwenden Sie hier nicht die E-Mail-Adresse des neuen Benutzers, sondern die eines Administrators, denn der Benutzer kann sich ja noch nicht anmelden, ohne das Kennwort zu wissen.

[»] Das Kennwortangabe entfällt, wenn Sie einen Domänenverbund (siehe Abschnitt 4.3, »Identitätsverbund für Single Sign-on«) für Single Sign-on aktiviert haben – in diesen Fällen gilt das Kennwort des lokalen Benutzerkontos.

Zuletzt wählen Sie gegebenenfalls noch eine oder mehrere Lizenzen, die dem Benutzer zugewiesen werden sollen. Abhängig von den gewählten Lizenzen kann der Anwender dann mit den Office 365-Diensten arbeiten. Wählen Sie beispielsweise eine Exchange Online-Lizenz, wird daraufhin automatisch ein Postfach für den Benutzer angelegt.

Unmittelbar danach kann sich der Benutzer an den lizenzierten Office 365-Diensten anmelden.

Mehrere Benutzer auf einmal anlegen

Ist Ihnen das Durchlaufen der einzelnen Schritte beim Anlegen mehrerer Benutzer zu aufwendig, können Sie über den Befehl Massenhinzufügen (Personen-Symbol) auch viele Benutzer auf einmal anlegen lassen (siehe Abbildung 2.40). Die Grundlage ist dabei eine *CSV-Datei* (*CSV = Comma-separated Values*), die Sie vorher in folgendem Format anlegen müssen:

```
Benutzername,Vorname,Nachname,Anzeigename,Position,Abteilung,Büronummer,
Telefon (geschäftlich),Mobiltelefon,Faxnummer,Adresse,Ort,Bundesland/
Kanton,Postleitzahl,Land oder Region
```

Listing 2.1 Aufbau einer CSV-Datei

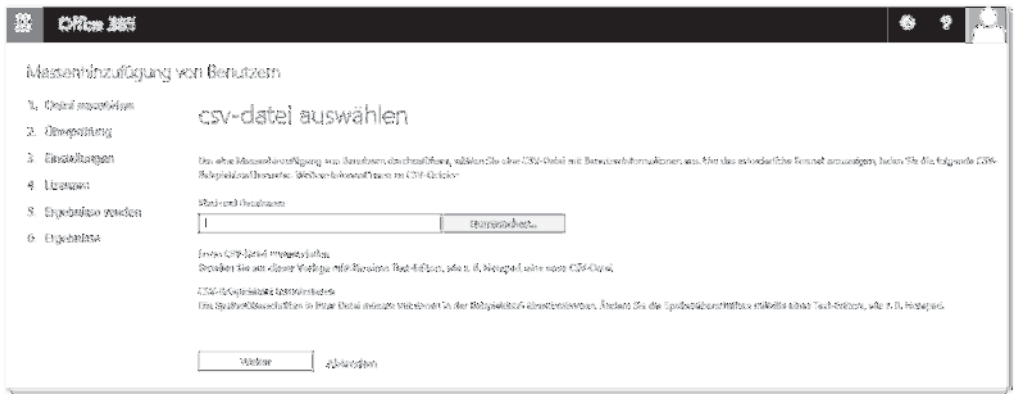

Abbildung 2.40 Massenanlegen von Benutzern

Nachdem Sie die CSV-Datei hochgeladen haben, wird der Inhalt analysiert. Dabei wird beispielsweise überprüft, ob Sie beim Anmeldenamen nur Domänen angegeben haben, die Bestandteil Ihrer Office 365-Umgebung sind. Ist die Datei in Ordnung,

machen Sie dann die Angaben wie beim Anlegen eines einzelnen Benutzers, nur dass diese dann für alle neuen Benutzer aus der CSV-Datei gelten.

Benutzer können Sie auch automatisiert mithilfe der PowerShell anlegen und dabei auch eigene Kennwörter vergeben. Wie das geht, lesen Sie in Abschnitt 2.5.2, »Benutzer anlegen«. [«]

2.5.3 Benutzer verwalten

Über die Benutzerverwaltung können Sie nicht nur neue Benutzer anlegen, sondern auch bestehende verwalten. Sie klicken dazu einfach auf den jeweiligen Anzeigenamen des Benutzers. Dort finden Sie folgende Einstellungen:

- DETAILS (siehe Abbildung 2.41)

  Neben den Namen des Benutzers können Sie weitere Angaben wie Telefonnummern und Adresse hinterlegen.

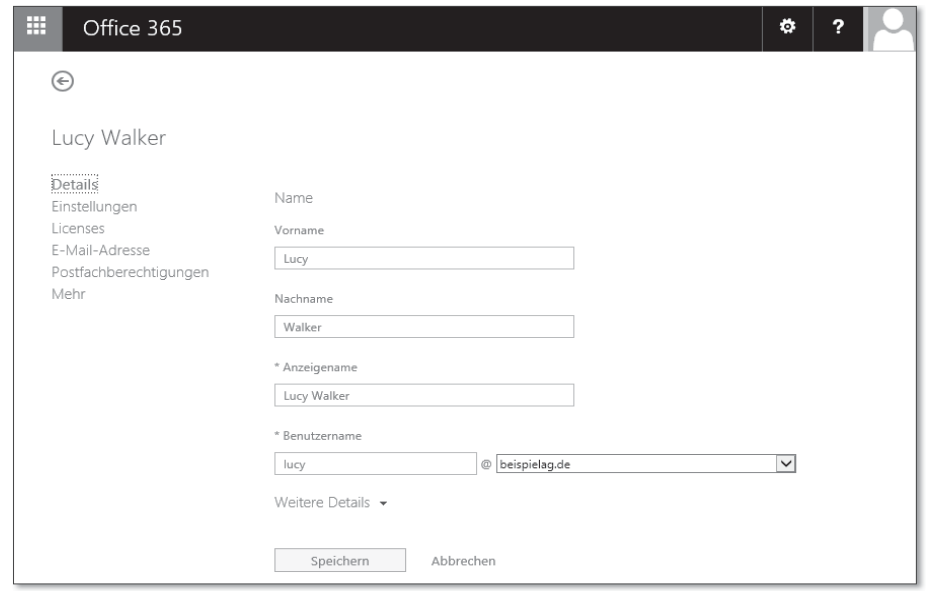

Abbildung 2.41 Details

- EINSTELLUNGEN (siehe Abbildung 2.42)

  Dieser Punkt besteht aus zwei Abschnitten, der ROLLE und dem ANMELDESTATUS. Sie können dem neuen Benutzerkonto eine *Administratorrolle* zuweisen, die es dem Anwender ermöglicht, verschiedene Verwaltungsaufgaben in Ihrer Office 365-Umgebung vorzunehmen. Tabelle 2.6 listet die Rollen samt deren Berechti-

gung auf. In Tabelle 2.7 ist außerdem aufgeführt, ob und welche Rolle ein Administrator automatisch bei den Diensten Exchange, SharePoint und Lync erhält.

Wählen Sie eine Administratorrolle, müssen Sie auch eine alternative E-Mail-Adresse angeben, über die der Benutzer im Falle eines vergessenen Kennworts ein neues erstellen kann. Dazu muss im Benutzerkonto auch eine Mobilfunknummer eingetragen werden. Mehr dazu lesen Sie in Abschnitt 2.11.2, »Administratorkennwort zurücksetzen«.

Um dem Benutzer die Anmeldung an Office 365 zu verwehren, wählen Sie die Option BLOCKIERT.

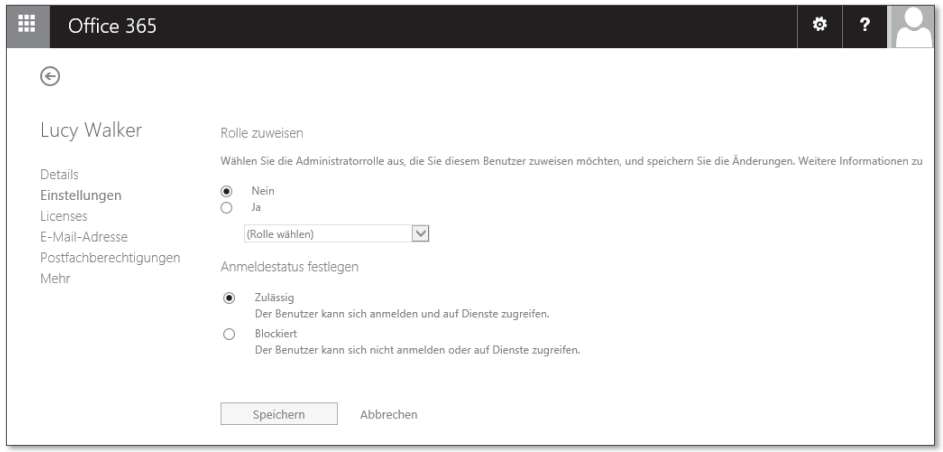

Abbildung 2.42 Einstellungen

Berechtigung	Rechnungsadministrator	Globaler Administrator	Kennwortadministrator	Dienstadministrator	Benutzerverwaltungsadministrator
Anzeige von Organisations- und Benutzerinformationen	ja	ja	ja	ja	ja
Verwaltung von Serviceanfragen	ja	ja	ja	ja	ja

Tabelle 2.6 Administratorrollen

Berechtigung	Rechnungsadministrator	Globaler Administrator	Kennwortadministrator	Dienstadministrator	Benutzerverwaltungsadministrator
Kennwörter zurücksetzen	nein	ja	ja (nicht bei anderen Administratoren)	nein	ja (nicht bei anderen Administratoren)
Verwaltung von Abonnements	ja	ja	nein	nein	nein
Anlegen und Verwalten von Benutzeransichten	nein	ja	nein	nein	ja
Verwaltung von Benutzern, Gruppen und Lizenzen	nein	ja	nein	nein	ja (kann keinen globalen Administrator löschen oder andere Administratoren anlegen)
Domänenverwaltung	nein	ja	nein	nein	nein
Verwaltung von Organisationsinformationen	nein	ja	nein	nein	nein
Delegierung von Administratorrollen	nein	ja	nein	nein	nein
Verwaltung der Active-Directory-Synchronisierung	nein	ja	nein	nein	nein

Tabelle 2.6 Administratorrollen (Forts.)

Office 365-Administratorrolle	Rolle in Exchange Online	Rolle in SharePoint Online	Rolle in Lync Online
Globaler Administrator	Exchange Online Administrator	SharePoint Online Administrator	Lync Online Administrator
Rechnungsadministrator	–	–	–
Kennwortadministrator	Help Desk Administrator	–	Lync Online Administrator
Dienstadministrator	–	–	–
Benutzerverwaltungsadministrator	–	–	Lync Online Administrator

Tabelle 2.7 Administratoren in Exchange, SharePoint, Lync

- LIZENZEN (siehe Abbildung 2.43)

  Bevor Sie einem Benutzer eine Lizenz zuweisen können, muss ein BENUTZERSTANDORT ausgewählt sein. Abhängig von dieser Auswahl kann es sein, dass einige Funktionen der Office 365-Dienste für diesen Benutzer nur eingeschränkt verfügbar sind. Auch kann es aufgrund von Ausfuhrbeschränkungen sein, dass der Benutzer Office 365 nicht nutzen darf. Beim ersten Anlegen des Benutzers wird der Standort automatisch gewählt. Eine Übersicht der Einschränkungen pro Land finden Sie unter folgender URL:

  http://office.microsoft.com/de-de/business/microsoft-office-license-restrictions-FX103037529.aspx

  Weisen Sie dem Benutzer eine Lizenz zu. Verfügen Sie über Lizenzpakete, die mehrere Einzellizenzen umfassen (beispielsweise E3), können Sie an dieser Stelle auch einzelne Bestandteile aus dem Paket herausnehmen (beispielsweise das Office-Paket, wenn Sie dieses anderweitig lizenzieren oder nicht benötigen). Nicht zugewiesene Bestandteile eines Lizenzpakets können Sie aber nicht einem anderen Benutzer zuweisen.

  Klicken Sie dann auf die Schaltfläche WEITER, erhalten Sie abhängig vom Benutzerstandort den Hinweis, dass es Einschränkungen bei bestimmten Diensten gibt.

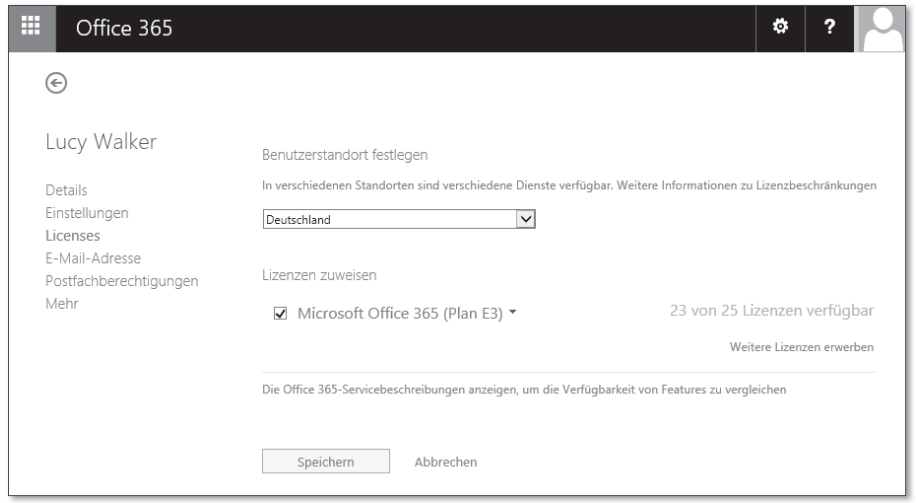

Abbildung 2.43 Lizenzen

- E-MAIL-ADRESSE (siehe Abbildung 2.44)

  Verfügt der Benutzer über eine Exchange Online-Lizenz, können Sie hier die E-Mail-Adressen des Benutzers anpassen. Dies würde aber auch über das Exchange Admin Center gehen.

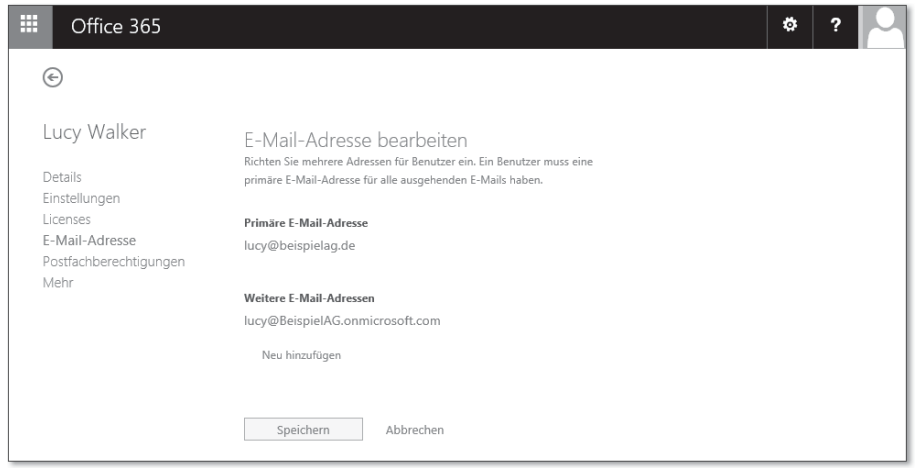

Abbildung 2.44 E-Mail-Adresse

- POSTFACHBERECHTIGUNGEN (siehe Abbildung 2.45)

  Auch hierfür ist eine Exchange Online-Lizenz erforderlich. Mit den Optionen können Sie beispielsweise Berechtigungen einrichten, die den Assistenten befähigen, auf das Postfach der Abteilungsleiterin zugreifen zu dürfen.

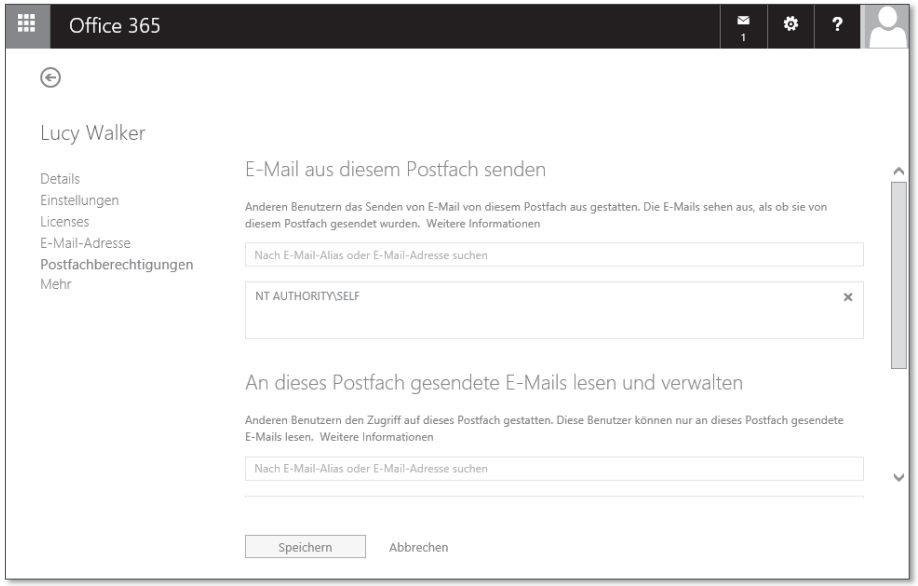

Abbildung 2.45 Postfachberechtigungen

- MEHR (siehe Abbildung 2.46)

  Abhängig von den zugewiesenen Lizenzen können Sie an dieser Stelle weitere Optionen auswählen (hier im Beispiel Einstellungen zu Exchange und Lync, da dem Benutzer eine E3-Lizenz zugewiesen wurde).

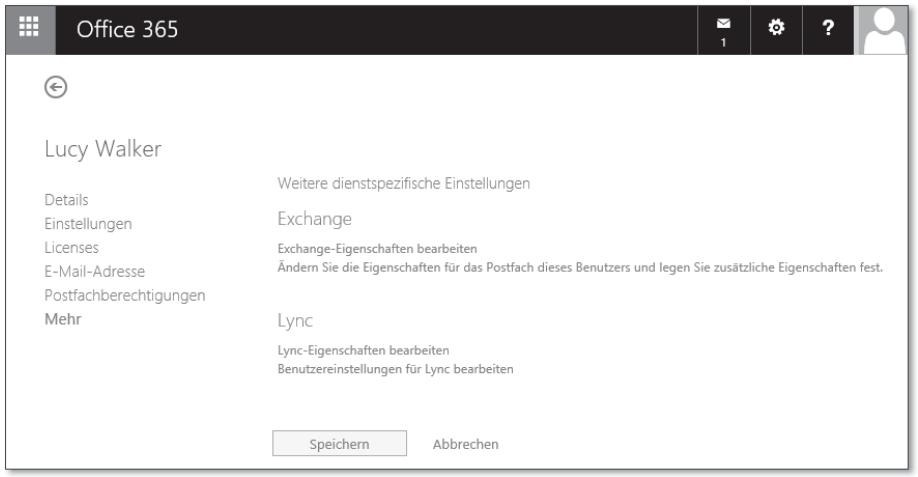

Abbildung 2.46 Mehr (Optionen)

Klicken Sie in der Benutzerliste nicht auf den Anzeigenamen, sondern markieren den Benutzer, können Sie auch folgende Aktionen durchführen (siehe Abbildung 2.47):

- Zurücksetzen von Kennwörtern
- Benutzer zu Gruppen hinzufügen
- Löschen von nicht mehr benötigten Benutzerkonten

  Das automatisch angelegte Administratorkonto beim Erstellen des Office 365-Mandanten sollten Sie möglichst nicht entfernen. Damit das Konto keine Kosten verursacht, können Sie die Lizenz vom Benutzerkonto entfernen und sie einem anderen Benutzerkonto hinzufügen.

  Haben Sie versehentlich einen Benutzer gelöscht, können Sie ihn unter Umständen wiederherstellen. Lesen Sie dazu Abschnitt 2.5.4, »Gelöschte Benutzer wiederherstellen«.

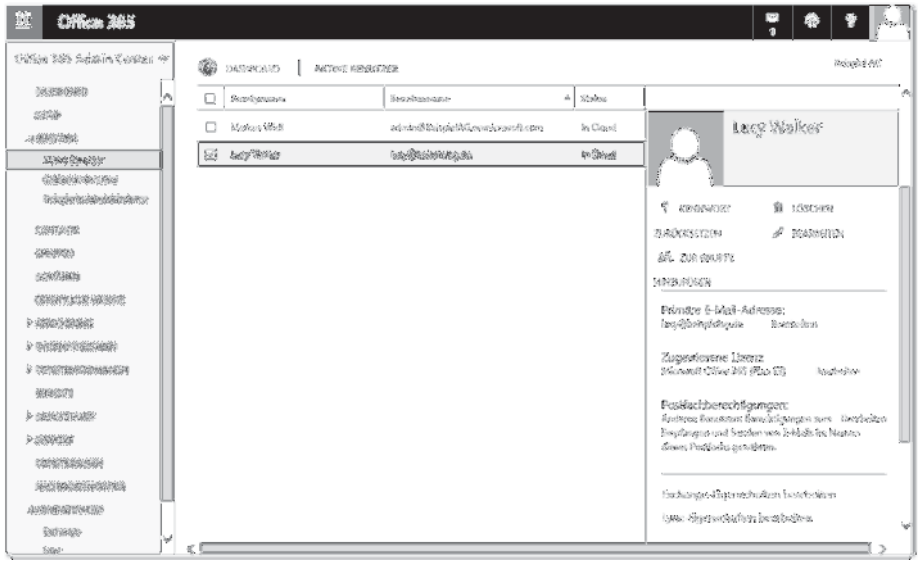

Abbildung 2.47 Benutzer bearbeiten

- Synchronisierte Benutzer aktivieren

  Diese Aktion ist nur möglich, wenn die Benutzer über ein Active-Directory-Verzeichnissynchronisierungstool automatisch angelegt wurden. Die Benutzer benötigen eine Office 365-Lizenz und möglicherweise ein Kennwort (sofern Single Sign-on und die Kennwortsynchronisierung nicht zum Einsatz kommen).

Um Ihnen die Verwaltung von vielen Benutzerkonten zu vereinfachen, stehen verschiedene Ansichten zur Auswahl bereit, beispielsweise »Benutzer mit Fehler« und »Nicht lizenzierte Benutzer« (siehe Abbildung 2.48). Um diese Ansichten aufzurufen, klicken Sie auf FILTER (TRICHTER-SYMBOL). Sie können auch eigene Ansichten anlegen und dabei etwa auf die optionalen Eigenschaften der Benutzer, wie beispielsweise die Adresse, zugreifen. Eine neue Ansicht erstellen Sie über den Befehl NEUE ANSICHT.

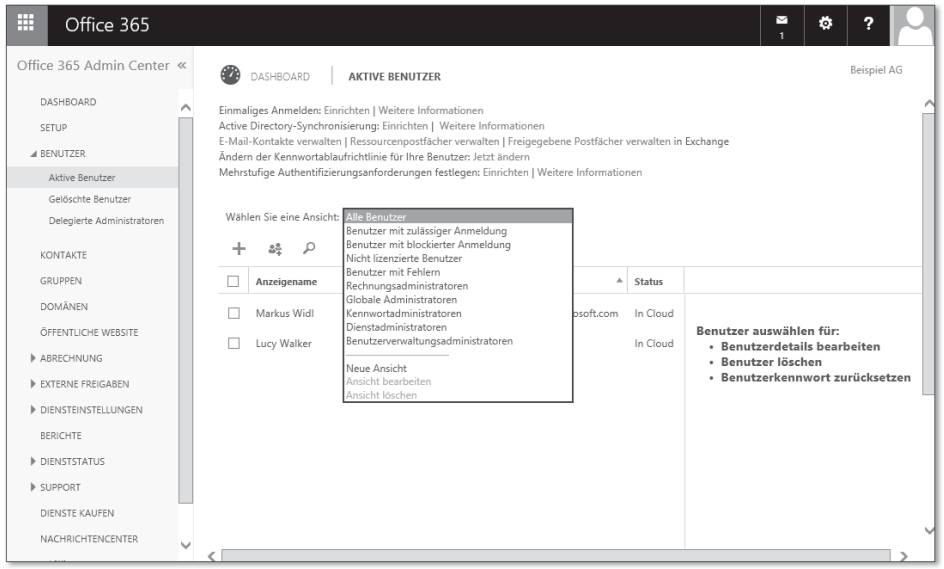

Abbildung 2.48 Auswahl einer Ansicht

2.5.4 Gelöschte Benutzer wiederherstellen

Innerhalb von 30 Tagen lassen sich gelöschte Benutzer wiederherstellen. Dazu wechseln Sie im Bereich Benutzer zum Abschnitt Gelöschte Benutzer (siehe Abbildung 2.49).

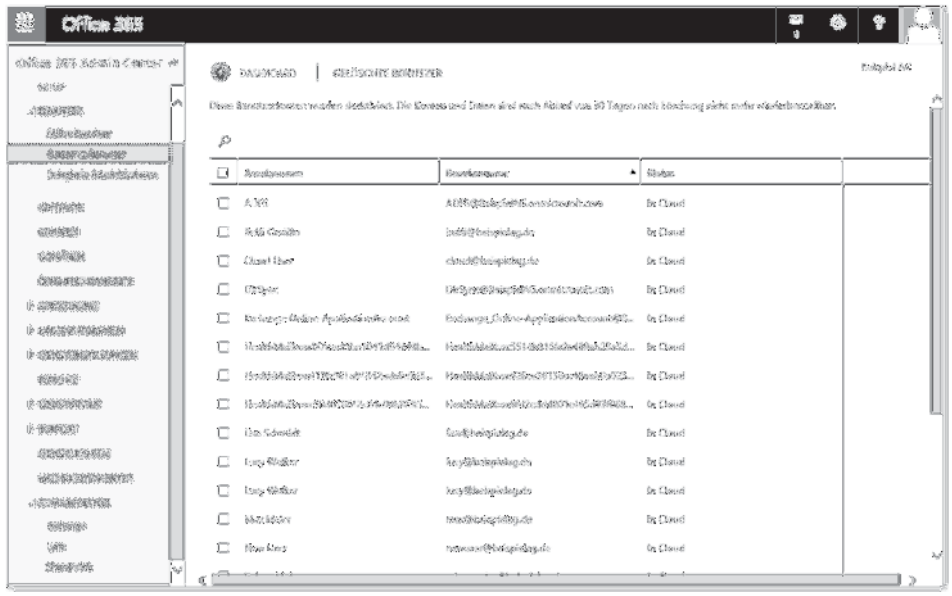

Abbildung 2.49 Verwaltung gelöschter Benutzer

Hatte der gelöschte Benutzer ein Postfach, wird auch dieses wiederhergestellt. Beachten Sie, dass ein gelöschtes Benutzerkonto nach 30 Tagen nicht mehr wiederhergestellt werden kann – auch nicht über eine Anfrage an den Microsoft-Kundendienst.

Die Wiederherstellung können Sie auch über PowerShell automatisieren. Außerdem gibt es dort eine Möglichkeit, einen gelöschten Benutzer schon vor Ablauf der 30 Tage dauerhaft zu entfernen. Lesen Sie hierzu Abschnitt 3.16.5, »Benutzer löschen und wiederherstellen«.

2.5.5 Kennwortablaufrichtlinie

In der Standardkonfiguration laufen bei Office 365-Benutzerkonten die Kennwörter regelmäßig nach 90 Tagen ab. Allerdings gibt es davon auch Ausnahmen:

- Sie haben über die PowerShell das Ablaufen des Kennworts für bestimmte Benutzerkonten deaktiviert (siehe Abschnitt 3.16.3, »Benutzer anlegen«).
- Sie verwenden die Kennwortsynchronisierung eines Active-Directoy-Synchronisierungstools. In diesem Fall gelten die Kennwortrichtlinien Ihres lokalen Active Directorys und nicht die von Office 365 (siehe Abschnitt 4.2, »Active-Directory-Synchronisierung«).
- Sie verwenden einen Identitätsverbund (*Single Sign-on*). Auch in diesem Fall gelten die Kennwortrichtlinien Ihres lokalen Active Directorys (siehe Abschnitt 4.3, »Identitätsverbund für Single Sign-on«).

Zur Anpassung der Kennwortablaufrichtlinie für Office 365-Benutzerkonten existieren zwei Einstellungen:

- Die Anzahl der Tage, bis ein Kennwort abläuft
  Diese Anzahl kann zwischen 14 und 730 liegen. Der Standardwert beträgt 90 Tage.
- Die Anzahl der Tage, bis Benutzer über das Ablaufen des Kennworts benachrichtigt werden
  Hier gilt im Standard 14 Tage. Der Zeitraum muss außerdem kleiner gewählt werden als der Zeitraum bis zum Ablaufen des Kennworts.

Diese beiden Optionen können Sie über das Office 365 Admin Center bearbeiten:

Öffnen Sie im Bereich Diensteinstellungen den Abschnitt Kennwörter (siehe Abbildung 2.50).

Nach einem Klick auf die Schaltfläche Speichern gelten die neuen Angaben ausschließlich für die Standarddomäne Ihres Office 365-Mandanten und nicht für alle Domänen gleichermaßen. Welche Domäne Ihre Standarddomäne ist, sehen Sie nicht in der Domänenverwaltung, sondern in den Einstellungen Ihrer Organisation. Um dorthin zu gelangen, öffnen Sie den Bereich Dashboard und klicken rechts oben auf Ihren Firmennamen. Dort können Sie auch die Standarddomäne ändern.

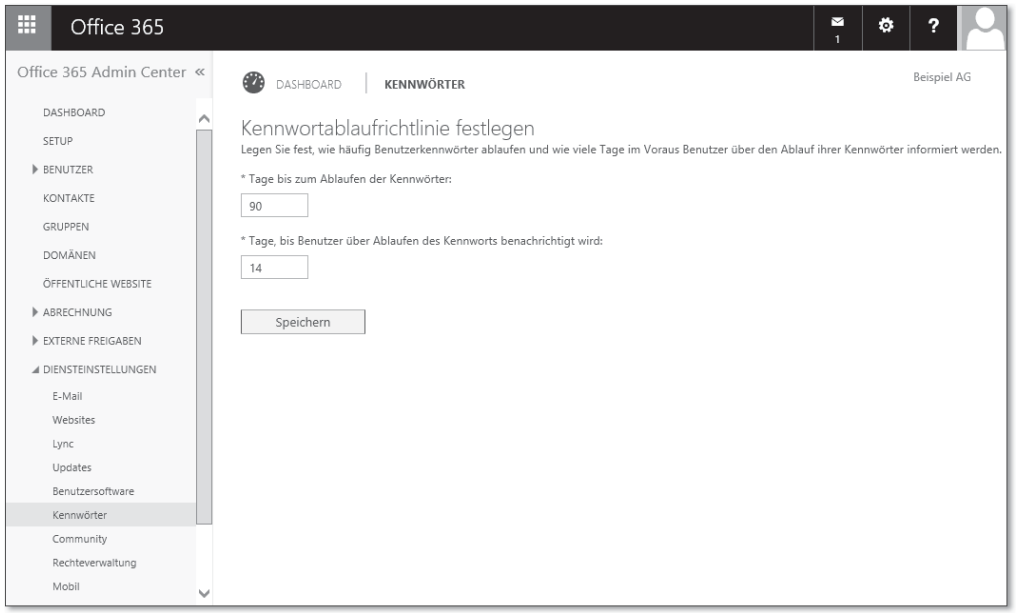

Abbildung 2.50 Kennwortablaufrichtlinie

Den PowerShell-Ansatz zur Anpassung der Kennwortablaufrichtlinie finden Sie in Abschnitt 2.5.2, »Benutzer anlegen«.

2.5.6 Sicherheitsgruppen

Sicherheitsgruppen sind kein neues Konzept, sondern beispielsweise auch im Active Directory enthalten. Mit ihnen gruppieren Sie Benutzerkonten, um sie beispielsweise als Grundlagen von Berechtigungen in SharePoint Online-Umgebungen einzusetzen.

Die Sicherheitsgruppen verwalten Sie im Office 365 Admin Center im Bereich GRUPPEN (siehe Abbildung 2.51).

Wie auch Benutzerkonten können Sie direkt im Admin Center weitere Sicherheitsgruppen anlegen oder dies über das Active-Directory-Verzeichnissynchronisierungstool automatisch erledigen lassen (siehe Abschnitt 4.2, »Active-Directory-Synchronisierung«).

Beim manuellen Anlegen gehen Sie wie folgt vor:

1. Klicken Sie auf HINZUFÜGEN (PLUS-SYMBOL).
2. Geben Sie einen GRUPPENNAMEN für die neue Gruppe an, und klicken Sie auf ERSTELLEN.

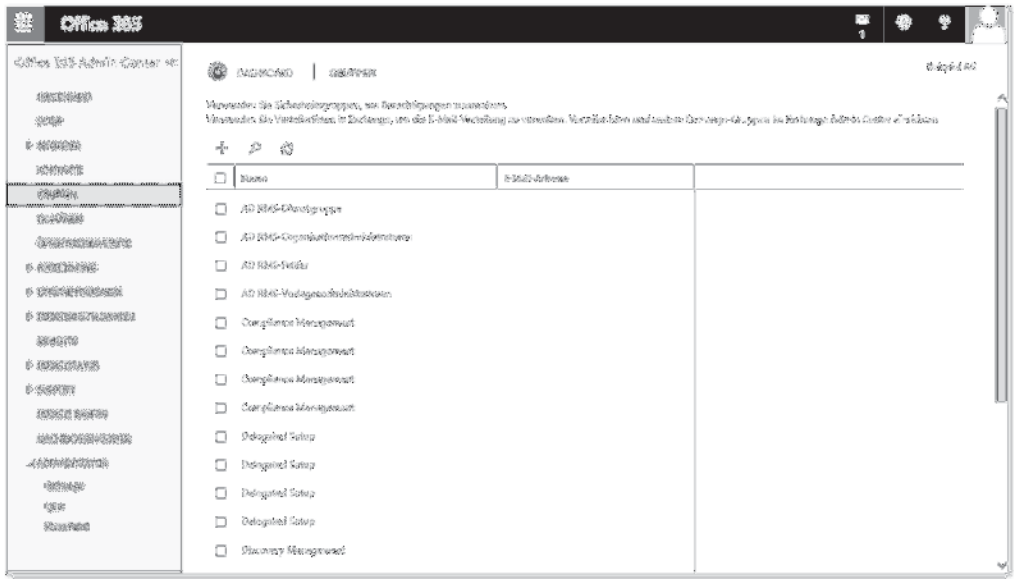

Abbildung 2.51 Sicherheitsgruppenverwaltung

Wählen Sie mit einem Klick auf MITGLIEDER BEARBEITEN die gewünschten Gruppenmitglieder aus (siehe Abbildung 2.52).

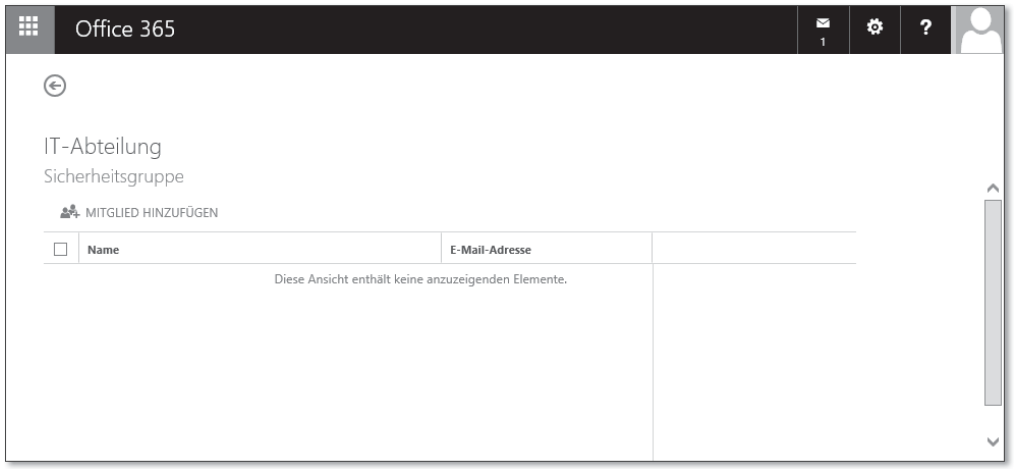

Abbildung 2.52 Auswahl von Gruppenmitgliedern

Neben dem Anlegen neuer Sicherheitsgruppen können Sie auch die vorhandenen bearbeiten und löschen.

Informationen zur Verwaltung von E-Mail-aktivierten Sicherheitsgruppen sowie von Verteilergruppen finden Sie in Abschnitt 6.5.2, »Gruppen«. [«]

2.6 Berichte

Als Administrator haben Sie im Office 365 Admin Center Zugriff auf eine ganze Reihe verschiedener Berichte, die Ihnen helfen, den Überblick über Ihr Office 365-Mandant und die Aktivitäten Ihrer Anwender zu behalten. Die verschiedenen Berichte aus Tabelle 2.8 erreichen Sie über den Bereich BERICHTE (siehe Abbildung 2.53).

[»] Der Begriff *DLP* aus der Tabelle steht für *Data Loss Prevention*. Mehr dazu lesen Sie in Abschnitt 6.9.4, »Verhinderung von Datenverlust«.

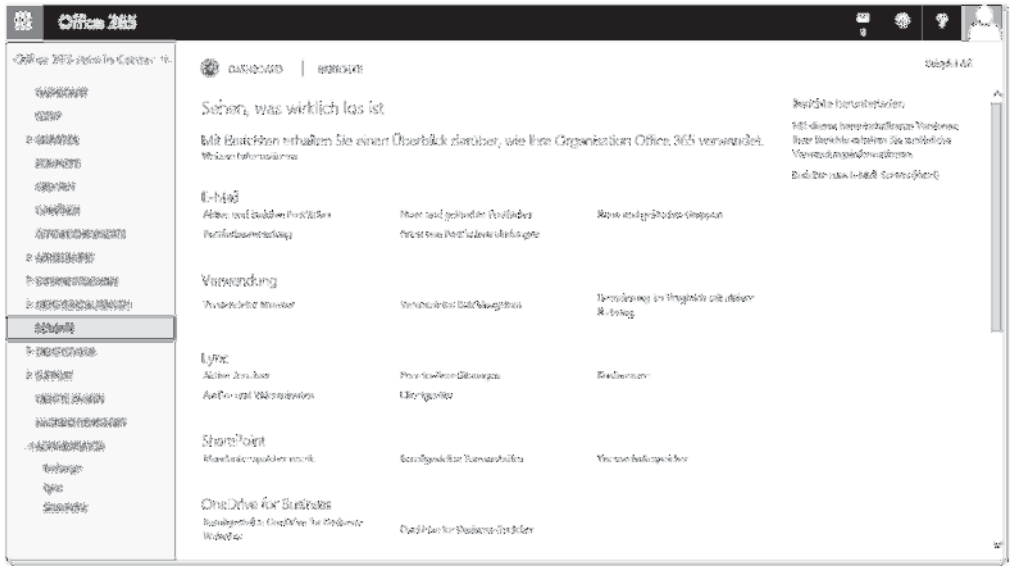

Abbildung 2.53 Berichte im Office 365 Admin Center

Bereich	Bericht
E-MAIL	▸ aktive und inaktive Postfächer ▸ neue und gelöschte Postfächer ▸ neue und gelöschte Gruppen ▸ Postfachverwendung ▸ Arten von Postfachverbindungen
NUTZUNG	▸ verwendeter Browser ▸ verwendetes Betriebssystem ▸ Lizenzierung im Vergleich mit aktiver Nutzung

Tabelle 2.8 Berichte im Office 365 Admin Center

Bereich	Bericht
LYNC	▸ aktive Benutzer ▸ Peer-to-Peer-Sitzungen ▸ Konferenzen ▸ Audio- und Videominuten ▸ Clientgeräte
SHAREPOINT	▸ Mandantenspeichermetrik ▸ bereitgestellte Teamwebsites ▸ Teamwebsitespeicher
ONEDRIVE FOR BUSINESS	▸ bereitgestellte OneDrive for Business-Websites ▸ OneDrive for Business-Speicher
ÜBERWACHUNG	▸ Postfachzugriff durch andere Personen als Besitzer ▸ Änderungen der Rollengruppe ▸ Durchsuchen und Aufbewahren von Postfachinhalten ▸ Beweissicherungsverfahren für Postfächer ▸ Azure AD-Berichte
SCHUTZ	▸ häufigste Absender und Empfänger ▸ häufigste Schadsoftware für E-Mails ▸ Schadsoftwareerkennung ▸ Spam-Entdeckung ▸ gesendete und empfangene E-Mails
REGELN	▸ häufigste Regelentsprechungen für E-Mails ▸ Regelentsprechungen für E-Mails
DLP	▸ häufigste DLP-Richtlinienentsprechungen für E-Mails ▸ häufigste DLP-Regelentsprechungen für E-Mails ▸ DLP-Richtlinienentsprechungen für E-Mails nach Schweregrad ▸ DLP-Richtlinienentsprechungen, Außerkraftsetzungen und falsch positive Meldungen für E-Mails

Tabelle 2.8 Berichte im Office 365 Admin Center (Forts.)

Zusätzlich zu den im Office 365 Admin Center angebotenen Berichten gibt es für den Bereich E-Mail-Sicherheit noch ein spezielles Plug-in für Excel 2013, das sehr ausführliche Berichte erzeugt. Das Plug-in mit dem langen Namen *Microsoft Office 365 Excel*

Plugin for Exchange Online Reporting finden Sie unter folgender URL (derzeit nur in englischer Sprache):

http://www.microsoft.com/en-us/download/details.aspx?id=30716

Nach der Installation finden Sie ein Symbol auf dem Desktop, mit dem das Plug-in geöffnet wird. Klicken Sie dann auf die Schaltfläche QUERY, und geben Sie Ihre Office 365-Zugangsdaten ein. Anschließend können Sie noch ein Zeitintervall auswählen. Bis die gewünschten Daten abgefragt werden, dauert es einige Sekunden. Über verschiedene Blätter in der Arbeitsmappe finden Sie nun verschiedene Diagramme. Ein Beispiel sehen Sie in Abbildung 2.54.

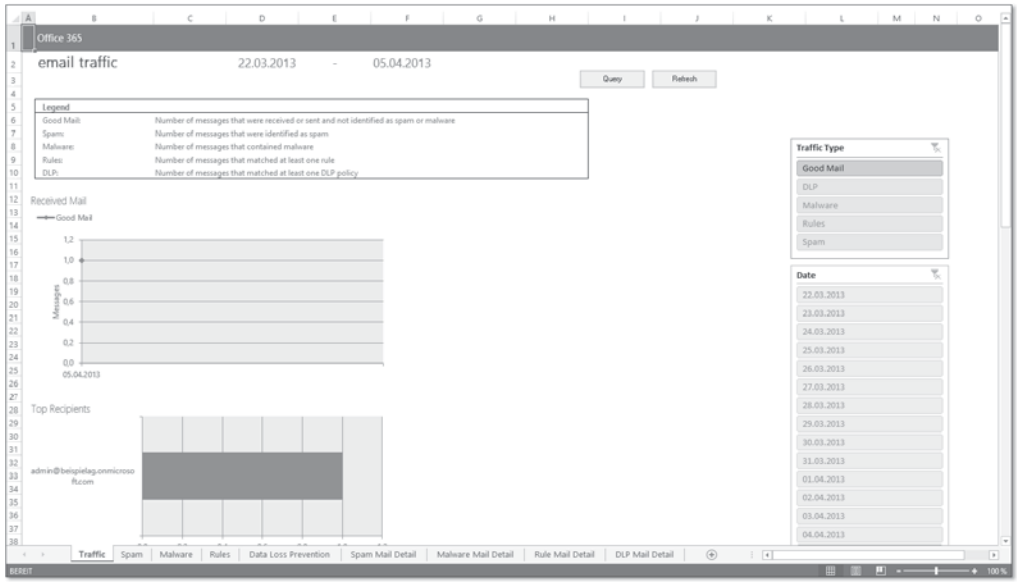

Abbildung 2.54 Berichte in Excel

2.7 Clientkonfiguration

In Abschnitt 1.1.4, »Systemvoraussetzungen«, haben Sie bereits die groben Systemvoraussetzungen für die Windows-Clients gesehen. Daneben sind je nach Windows-Version und installierten Updates manchmal weitere Softwarekomponenten erforderlich, beispielsweise Hotfixes. Dies ist insbesondere dann vonnöten, wenn Sie ältere Software wie Office 2010 einsetzen. Die entsprechende Einrichtung können Sie über zwei Wege durchführen:

1. auf einzelnen Clients mithilfe der Anwendung *Office 365-Desktopsetup*
2. im großen Stil über Softwareverteilung, Gruppenrichtlinien etc.

2.7.1 Office 365-Desktopsetup

Die Anwendung *Office 365-Desktopsetup* kann Ihre Clients überprüfen und aktualisieren sowie lokal vorhandene Anwendungen für den Betrieb mit Office 365 konfigurieren. Das Desktopsetup wird empfohlen für den Betrieb eines Computers mit Office 2007 oder 2010. Bei Office 2013 ist es nicht erforderlich.

Die Anwendung hat im Wesentlichen folgende Aufgaben:

- Installation erforderlicher Updates
- Installation des *Microsoft Online Services-Anmelde-Assistenten*
- Konfiguration der lokal installierten Anwendungen wie den Internet Explorer für SharePoint Online

Das Desktopsetup selbst wird oftmals einmalig aufgerufen und ist anschließend nicht mehr erforderlich. Es ist also keine aktive Komponente, die ständig laufen muss.

Aufruf

Melden Sie sich bei Office 365 mit einem Benutzer an, der auch eine Lizenz zugewiesen hat, und wechseln Sie dann zu den EINSTELLUNGEN (ZAHNRAD) • OFFICE 365-EINSTELLUNGEN. Auf der erscheinenden Seite wechseln Sie zum Bereich SOFTWARE und dann zum DESKTOPSETUP (siehe Abbildung 2.55).

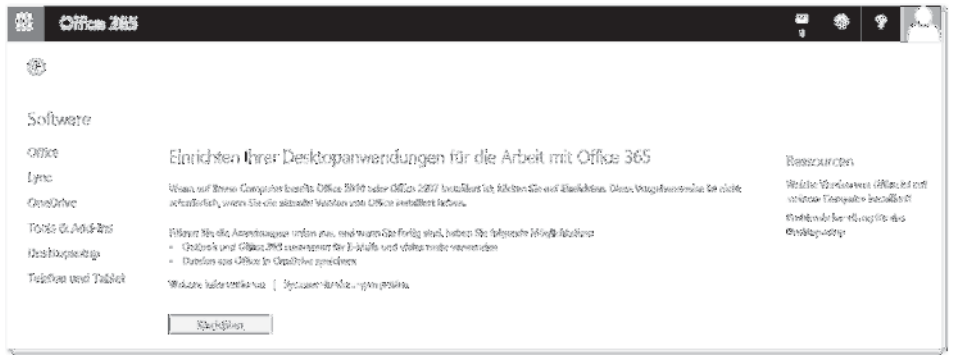

Abbildung 2.55 Start des Office 365-Desktopsetups

Die direkte URL zum Downloadbereich ist folgende:

https://portal.office.com/OLS/mysoftware.aspx

Öffnen Sie den Downloadbereich auf einem Nicht-Windows-Rechner, wird das Desktopsetup nicht angezeigt.

Mit einem Klick auf EINRICHTEN starten Sie die Anwendung. Dabei müssen Sie sich zunächst mit einem Office 365-Benutzer anmelden. Anschließend erhalten Sie eine Übersicht, welche Komponenten installiert werden, und Sie haben die Auswahl, welche Anwendungen konfiguriert werden sollen (siehe Abbildung 2.56).

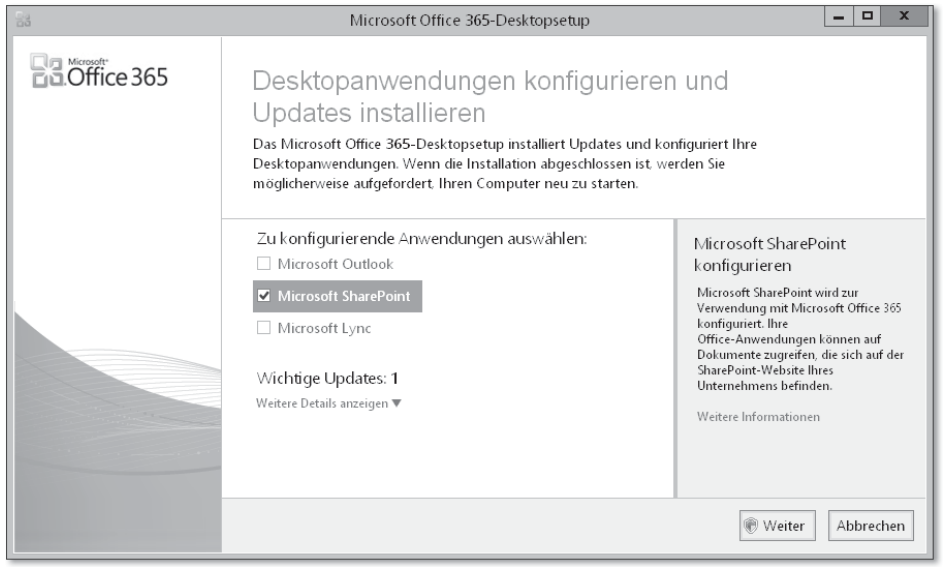

Abbildung 2.56 Office 365-Desktopsetup

Je nach installierten Updates ist anschließend ein Neustart des Rechners erforderlich.

Das Desktopsetup ist auf einzelnen Clients ein gangbarer Weg, um diese für den Office 365-Einsatz fit zu machen. Bei größeren Umgebungen ist das aber keine Option, denn dort soll die Clienteinrichtung möglichst automatisiert ablaufen. Deshalb sind die Schritte, die das Desktopsetup ausführt, auch über eigene Techniken wie Softwareverteilung, Gruppenrichtlinien etc. durchführbar. Dabei ist der folgende Artikel hilfreich: *http://office.microsoft.com/en-us/office365-suite-help/manually-update-and-configure-desktops-for-office-365-HA102817833.aspx#_Toc325445031*

2.7.2 Konfiguration von mobilen Endgeräten

Windows Phone 8.x ist für die Konfiguration eines Office 365-Zugangs bereits vorbereitet. Ein Assistent kümmert sich um die Einbindung des Exchange-Postfachs, die Verlinkung der SharePoint-Website und weist auf den im Marketplace kostenfrei verfügbaren Lync-Client hin.

Zur Konfiguration Ihres Office 365-Zugangs bei einem Windows Phone 8.x-Gerät gehen Sie wie folgt vor:

1. In den Einstellungen Ihres Geräts wählen Sie den Punkt E-Mail-Konten + andere.
2. Wählen Sie den Befehl Konto hinzufügen (siehe Abbildung 2.57) und dann Exchange (siehe Abbildung 2.58).

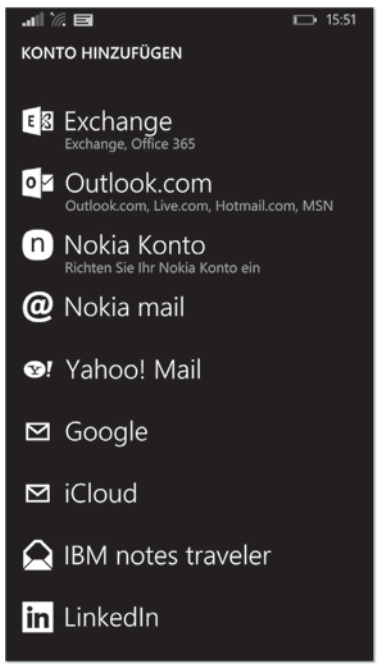

Abbildung 2.57 Verwaltung der E-Mail-Konten bei Windows Phone 8.x

Abbildung 2.58 Hinzufügen eines Office 365-Zugangs

3. Geben Sie Ihre Office 365-Zugangsdaten ein (siehe Abbildung 2.59).

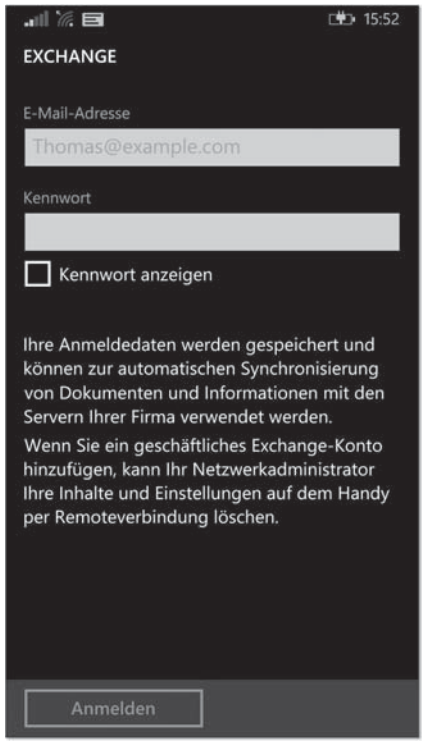

Abbildung 2.59 Eingabe der Zugangsdaten

Nachdem die Zugangsdaten überprüft wurden, können Sie mit Office 365 arbeiten.

[»] Das Windows Phone bietet dann den direkten Download der Lync-App an. Stellen Sie sicher, dass es sich dabei um die Lync 2013- und nicht die Lync 2010-App handelt. Gegebenenfalls erhalten Sie die Lync 2013-App auch über den Store.

Für Apple iOS- und Google Android-Geräte gibt es keinen speziellen Konfigurationsassistenten für Office 365. In den folgenden Kapiteln werde ich diese beiden Betriebssysteme aber nicht vernachlässigen, sondern bei den entsprechenden Anwendungen auf die Konfiguration und die Besonderheiten bei der Arbeit mit Office 365 hinweisen.

2.8 Dienststatus

Bevor Sie eine Serviceanfrage stellen, können Sie sich über den Bereich DIENSTSTATUS vergewissern, dass es derzeit keine Ausfälle an den Office 365-Diensten gibt (siehe Abbildung 2.60).

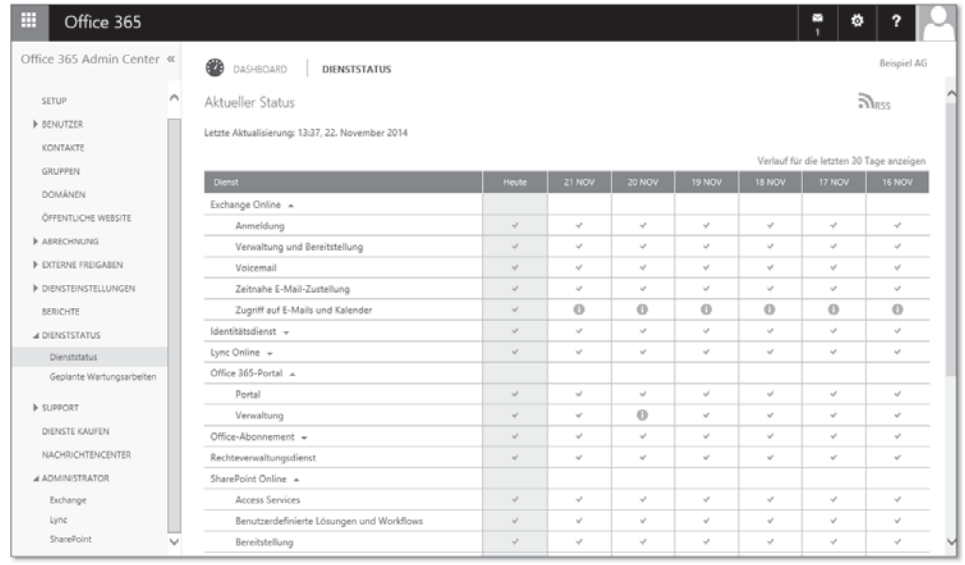

Abbildung 2.60 Dienststatus

Den Dienststatus können Sie über diese Seite als *RSS-Feed* abonnieren.

In diesem Bereich finden Sie auch den Abschnitt GEPLANTE WARTUNGSARBEITEN. Hier werden Wartungen an der Office 365-Umgebung angekündigt (siehe Abbildung 2.61). Damit können Sie sich auf mögliche Dienstausfälle vorbereiten.

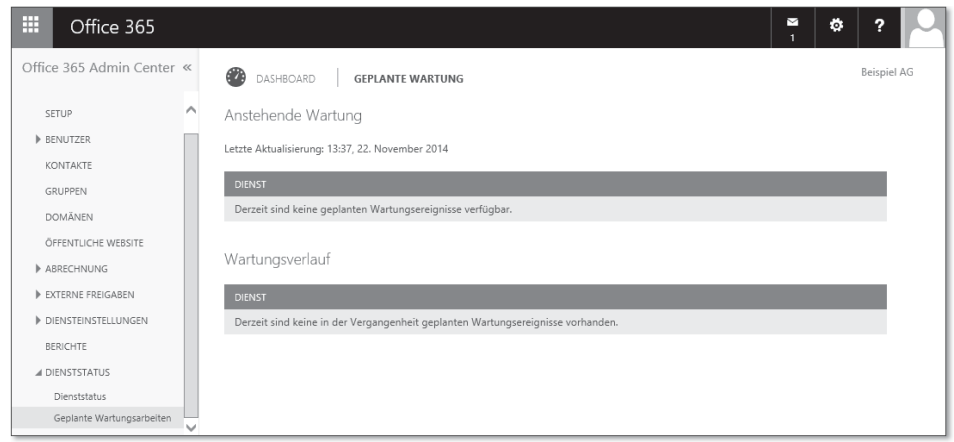

Abbildung 2.61 Geplante Wartungsarbeiten

Betreiben Sie einen *System Center Operations Manager (SCOM)*, können Sie den Dienststatus über ein spezielles Management-Pack einbinden. Das Pack erhalten Sie unter folgender URL: [«]

http://www.microsoft.com/en-us/download/details.aspx?id=43708

2.9 Nachrichtencenter

Das Office 365 Admin Center hält Sie über wichtige Änderungen rund um Ihren Office 365-Mandanten auf dem Laufenden. Dazu wählen Sie den Bereich NACHRICHTENCENTER (siehe Abbildung 2.62).

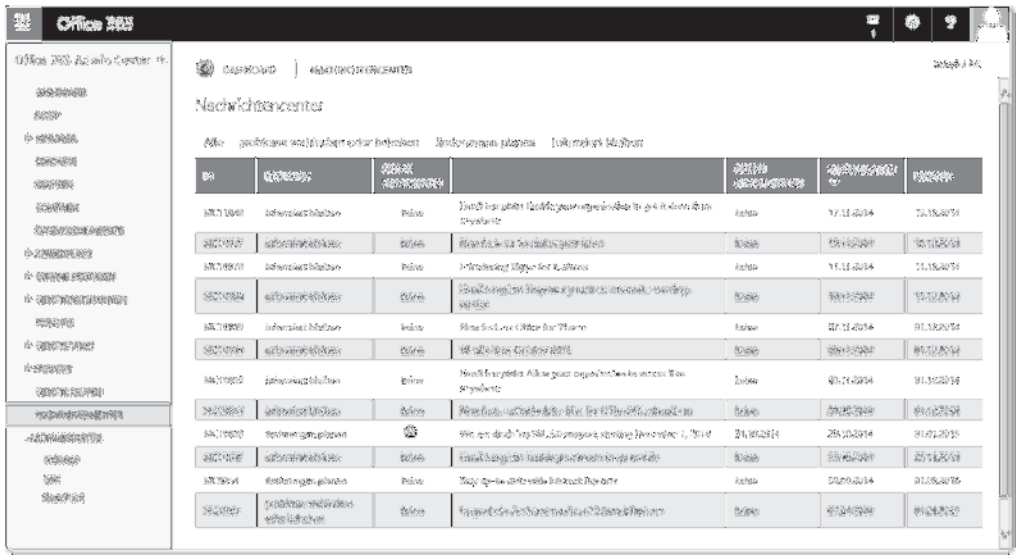

Abbildung 2.62 Nachrichtencenter

Hier finden Sie Informationen wie die wegfallende Unterstützung von Betriebssystemen (z. B. Windows XP) und Browsern (z. B. Internet Explorer 8), die geplante Einführung neuer Funktionen und Änderungen am bestehenden Funktionsumfang.

2.10 Erstveröffentlichung neuer Funktionen

Office 365 ist ein sehr lebendiges Produkt, bei dem in kurzen Abständen neue Funktionen eingeführt werden. Einen Überblick finden Sie auf der offiziellen Roadmap:

http://office.com/roadmap

Allerdings werden die meisten neuen Funktionen nicht über Nacht bei allen Kunden aktiviert, sondern es gibt einen Übergangszeitraum, der durchaus mehrere Monate betragen kann. Wenn Sie Ihren Office 365-Mandanten möglichst frühzeitig mit neuen Funktionen ausstatten wollen, aktivieren Sie in den DIENSTEINSTELLUNGEN des Office 365 Admin Centers die Option ERSTVERÖFFENTLICHUNG (siehe Abbildung 2.63).

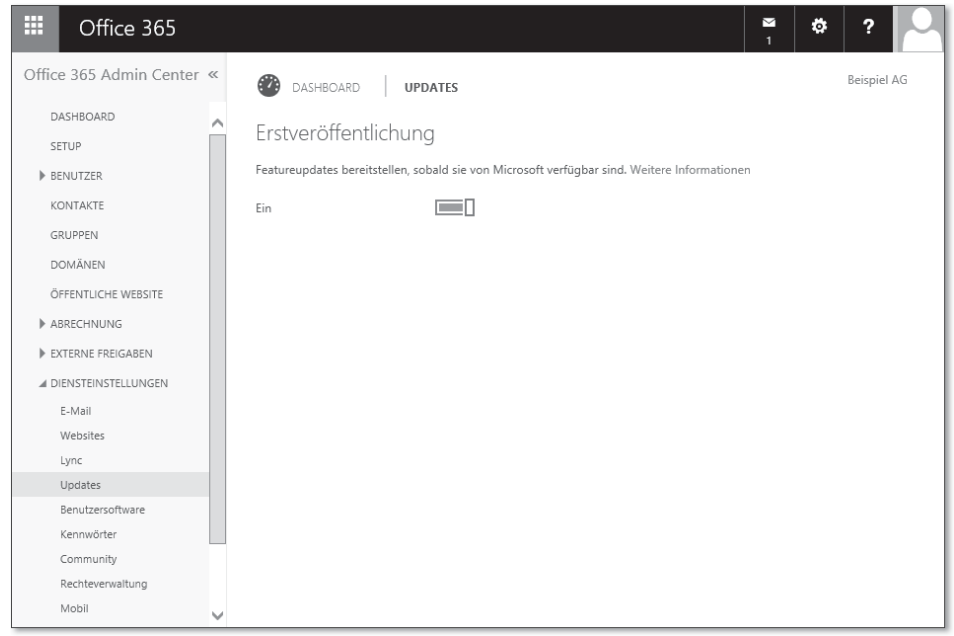

Abbildung 2.63 Erstveröffentlichung

Vielleicht wollen Sie diese Option nicht in Ihrem produktiven Mandanten aktivieren, sondern nur in einem Mandanten, den Sie für Tests angelegt haben. So können Sie schon frühzeitig mit den neuen Funktionen arbeiten und sind vorbereitet, sobald sie den Anwendern zur Verfügung stehen.

2.11 Problembehebung

Gibt es ein Problem mit Ihrer Office 365-Umgebung, finden Sie im Bereich SUPPORT verschiedene Hilfestellungen (die natürlich nur dann funktionieren, wenn das Portal selbst noch zugänglich ist):

- ÜBERSICHT

  Dieser Abschnitt enthält verschiedene Artikel zur Problemlösung und Links zu verschiedenen Tools.

- SERVICEANFRAGEN

  Können Sie das Problem nicht lösen, haben Sie die Möglichkeit, eine Anfrage an den Office 365-Kundendienst zu schicken (siehe Abbildung 2.64). Dabei können Sie auch Dateien – beispielsweise eine Bildschirmabbildung – hochladen, die möglicherweise einen Hinweis auf die Problemursache liefern.

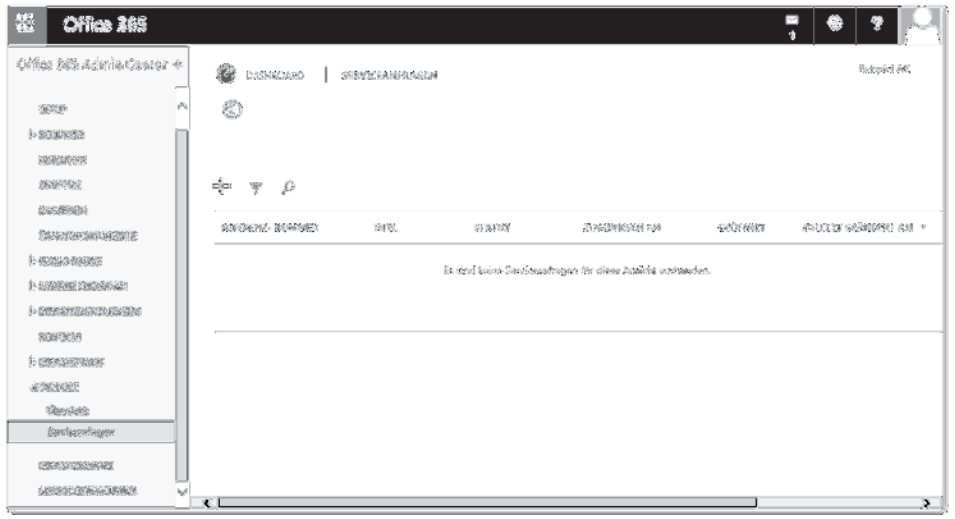

Abbildung 2.64 Serviceanfragen

2.11.1 Domänenproblembehandlung

Vermuten Sie ein Problem bei den DNS-Einstellungen Ihrer Domäne, können Sie die DOMÄNENPROBLEMBEHANDLUNG starten, um sicherzustellen, dass Sie die erforderlichen DNS-Einträge korrekt eingegeben haben. Gehen Sie dazu wie folgt vor: In der Domänenverwaltung markieren Sie die Domäne und klicken auf den Link PROBLEME SUCHEN UND BEHEBEN.

Der Assistent überprüft dann die Einstellungen und präsentiert sein Ergebnis. Wie das aussehen kann, sehen Sie in Abbildung 2.65.

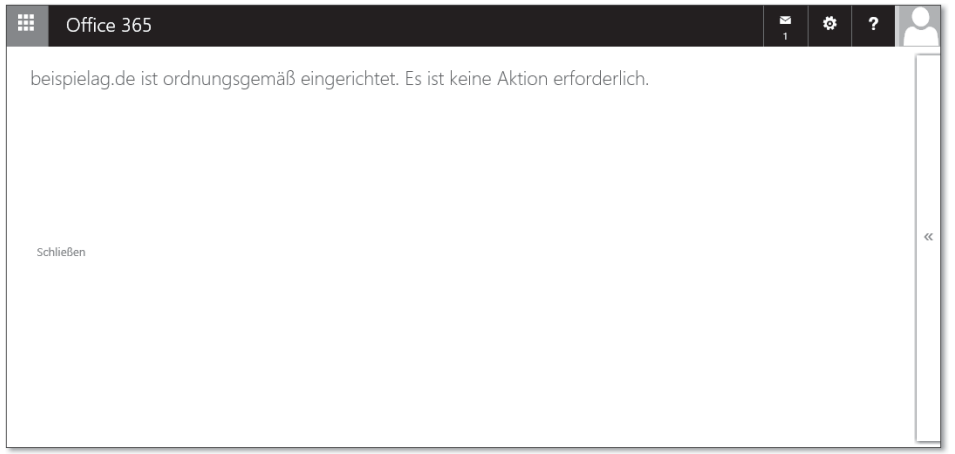

Abbildung 2.65 Assistent zur Domänenproblembehandlung

2.11.2 Administratorkennwort zurücksetzen

Vergisst einer Ihrer Anwender sein Kennwort zur Anmeldung an Office 365, ist das nicht weiter tragisch. Ein Administrator mit passender Rollenzugehörigkeit (siehe Abschnitt 2.5.2, »Benutzer anlegen«) kann das Kennwort zurücksetzen. Sollte allerdings ein Administrator sein Kennwort vergessen, ist das etwas aufwendiger:

- Wenn ein anderer globaler Administrator verfügbar ist:
  Ist ein globaler Office 365-Administrator greifbar, kann er das Kennwort eines anderen Administrators zurücksetzen.

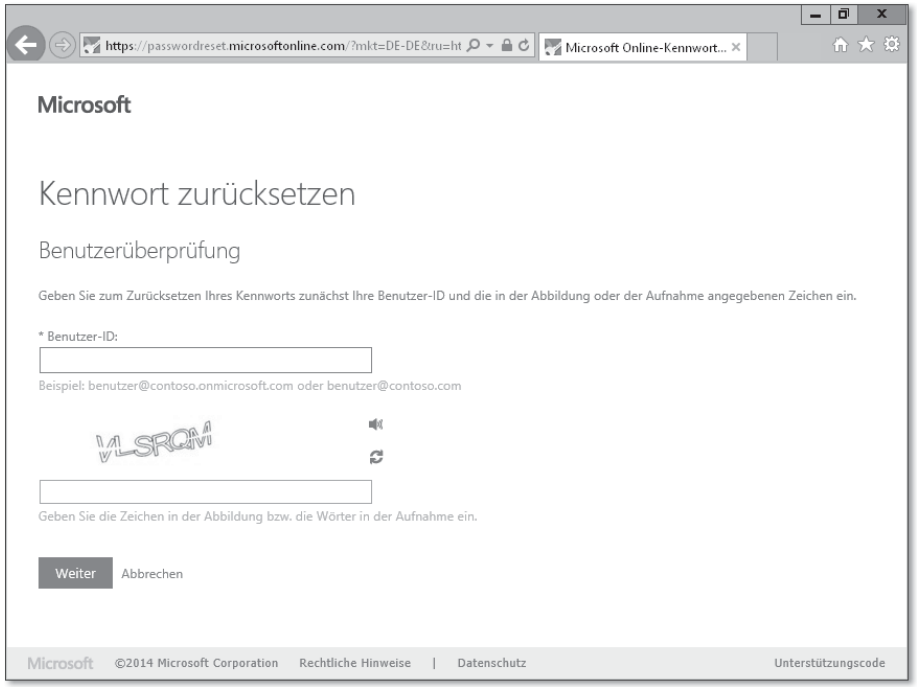

Abbildung 2.66 Kennwort vergessen

- Wenn *kein* anderer globaler Administrator verfügbar ist:
  In diesem Fall kann der Administrator über das Anmeldefenster des Office 365-Portals angeben, dass er sein Kennwort vergessen hat (siehe Abbildung 2.66). Vorausgesetzt, im Benutzerkonto wurde bei der Zuweisung der Administratorrolle eine alternative E-Mail-Adresse angegeben und bei den weiteren Einstellungen des Benutzerkontos auch eine Mobilfunknummer, dann werden dem Anwender an die alternative E-Mail-Adresse ein Link und ein Rücksetzcode per SMS zugesandt. Mit beiden gemeinsam kann der Administrator dann sein Kennwort zurücksetzen (siehe Abbildung 2.67).

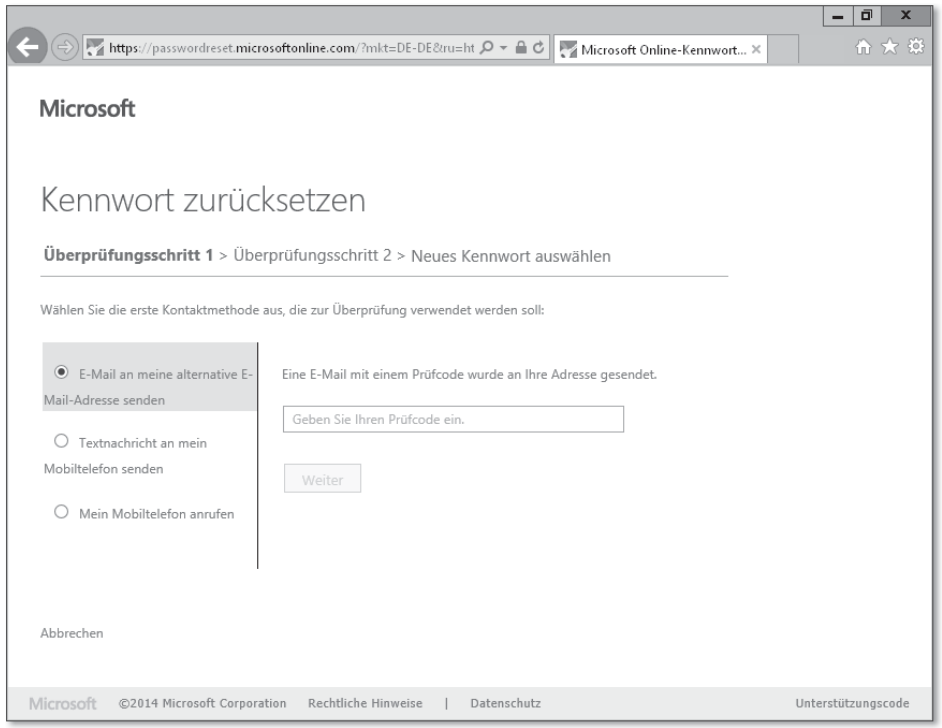

Abbildung 2.67 Kennwort zurücksetzen

Nicht-Administratoren steht dieser Vorgang nicht zur Verfügung. Sollte es Schwierigkeiten geben, hilft der Office 365-Kundendienst.

[»] Die Option, dass der Anwender selbst sein Kennwort zurücksetzen kann, ist aber außerhalb von Office 365 über Microsoft Azure buchbar. Mehr Informationen erhalten Sie unter folgender URL:

http://technet.microsoft.com/en-us/library/dn510386

2.11.3 Weitere Hilfestellungen

Daneben gibt es weitere Hilfestellungen, die manchmal die erhoffte Lösung bringen:

- *Office 365 Technical Network* auf Yammer

  Offizielle Anlaufstelle zur Unterstützung bei Fragestellungen rund um Office 365 mit Antworten von Herstellerseite und aus der Community

  https://www.yammer.com/itpronetwork

- *Office 365-Supportcenter*

  Das offizielle Supportcenter von Microsoft für Office 365 finden Sie unter:

  http://support.microsoft.com/ph/15834

- *Twitter*

  Unter @Office365 werden größere Ausfälle getwittert:

  http://twitter.com/Office365

2.11.4 Verbindungsprobleme

Bestehen Probleme bei der Kommunikation zwischen Ihrer lokalen Umgebung und Office 365, kann das an der Firewallkonfiguration liegen. Auf der folgenden Seite finden Sie eine Übersicht der von Office 365 verwendeten URLs und IP-Adressbereiche:

http://technet.microsoft.com/de-de/library/hh373144.aspx

2.12 So geht es weiter

In diesem Kapitel haben Sie die Grundkonfiguration eines Office 365-Mandanten kennengelernt. Nun können wir uns im dritten Kapitel auf die kommandozeilenbasierte Administration mithilfe der PowerShell stürzen. Diese werden Sie zwar nicht ständig benötigen, doch gibt es einige Funktionsbereiche, die Sie nur mit der PowerShell administrieren können. Außerdem ist sie ein gutes Werkzeug zur Automatisierung. Deshalb werden wir in den späteren Kapiteln immer wieder auf die Kommandozeile zurückgreifen.

Kapitel 4

Identitäten und Active-Directory-Synchronisierung

Im vierten Kapitel lernen Sie verschiedene Identitätsarten kennen, koppeln Ihr lokales Active Directory mit dem Azure Active Directory, richten Same Sign-on und Single Sign-on ein und erhöhen mit der mehrstufigen Authentifizierung die Sicherheit, falls die Anwender Ihr Kennwort verlieren.

Typischerweise wollen Sie Ihre Endanwender bei der Arbeit unterstützen und alltägliche Schritte vereinfachen. Dazu gehört beispielsweise die Bereitstellung von *Same Sign-on* oder *Single Sign-on*. Bei Office 365 bedeutet Same Sign-on, dass sich die Anwender mit demselben Benutzernamen und demselben Kennwort an den Clouddiensten anmelden können. Single Sign-on geht noch weiter: Ihre Anwender müssen sich im Idealfall an den Clouddiensten nicht erneut anmelden – die einmalige Anmeldung an der lokalen Domäne ist ausreichend.

Voraussetzung für Same Sign-on und Single Sign-on – und nicht nur da – ist die Aktivierung der Active-Directory-Synchronisierung. Sie installieren dazu auf einem lokalen Server eine Softwarekomponente, die in regelmäßigen Abständen lokal vorhandene Benutzerkonten, Gruppen und Kontakte automatisch im Verzeichnisdienst von Office 365, dem *Azure Active Directory (AAD)*, anlegt und Änderungen an diesen Objekten übernimmt. Dadurch entfällt für Sie als Administrator der doppelte Pflegeaufwand, beispielsweise beim Anlegen von Benutzerkonten für Mitarbeiter. Doch es gibt darüber hinaus weitere Vorteile, die ich in diesem Kapitel noch besprechen werde.

4.1 Verschiedene Identitäten

Office 365 verwendet intern mit dem Azure Active Directory (AAD) einen eigenen Verzeichnisdienst, so wie Sie selbst höchstwahrscheinlich lokal ein Active Directory einsetzen. Für jeden Ihrer Office 365-Anwender muss im AAD ein Benutzerkonto angelegt sein, das dann für die verschiedenen Dienste lizenziert wird (siehe Abbildung 4.1). Das ist auch der Fall, wenn Sie Same Sign-on oder Single Sign-on einrichten.

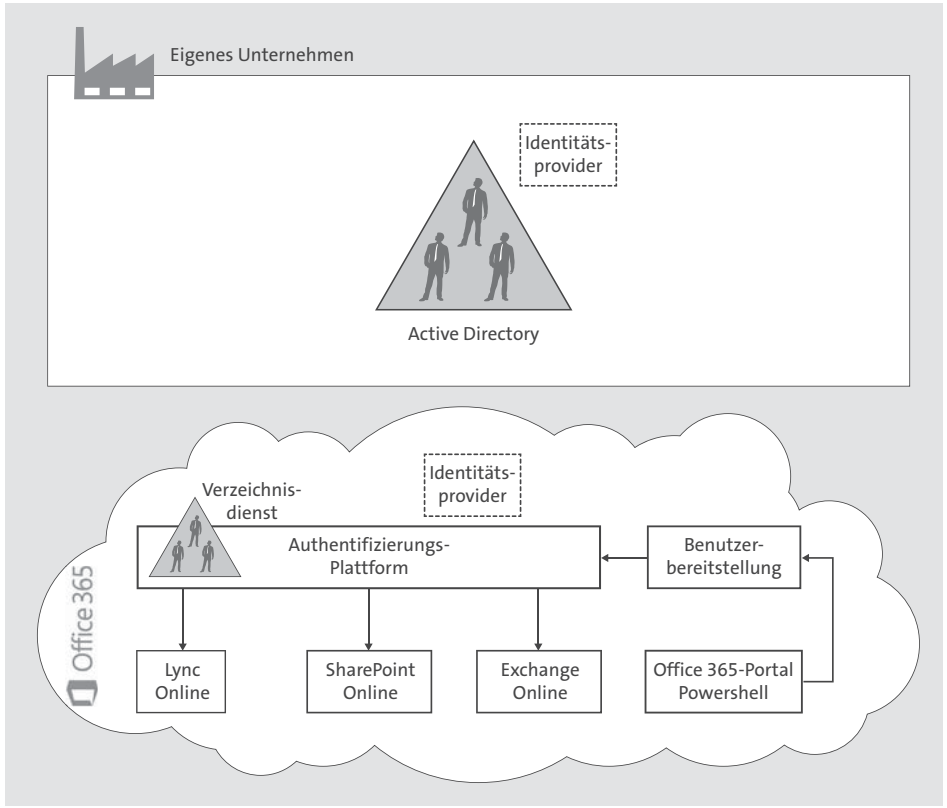

Abbildung 4.1 Office 365 verfügt über einen eigenen Verzeichnisdienst.

[»] Das AAD wird übrigens nicht nur von Office 365, sondern beispielsweise auch von *Dynamics CRM Online* und *Microsoft Intune* eingesetzt. Mehr zu diesen beiden Produkten lesen Sie in Kapitel 12, »Weitere Dienste«. Das AAD wird auch außerhalb von Office 365 in verschiedenen Ausbaustufen angeboten. Das AAD, das Sie kostenfrei mit Office 365 erhalten, entspricht der Free-Edition ohne Objektlimitierung und zusätzlich der Multi-Factor-Authentifizierung für Cloudbenutzer. Mehr zum AAD finden Sie hier:

http://msdn.microsoft.com/library/azure/dn532272.aspx

Die Frage ist nun, wie Sie in der Praxis mit diesem zusätzlichen Verzeichnisdienst umgehen, obwohl Sie ja schon selbst einen haben. Dabei gibt es mehrere verschiedene Varianten. Um die zu verstehen, müssen wir zunächst drei Begriffe klären:

- *Microsoft-Online-Identität*
  Für jeden Office 365-Anwender wird im Office 365-Verzeichnisdienst ein Benutzerkonto angelegt. Diesen Benutzerkonten weisen Sie eine Office 365-Lizenz zu. Ihre Anwender melden sich dann an Office 365 mit diesen Benutzerkonten an – den Microsoft-Online-Identitäten. Diese haben mit den im lokalen Verzeichnisdienst

vorhandenen Benutzerkonten zunächst nichts zu tun. Der *Identitätsprovider* wird von Office 365 gestellt. Daneben verwenden Sie mit Ihrem lokalen Active Directory einen weiteren Identitätsprovider.

- *Verbundidentität*
  Auch bei Verbundidentitäten (*Federated Identity*) werden im Office 365-Verzeichnisdienst Benutzerkonten angelegt und mit einer Lizenz versehen. Allerdings melden sich Ihre Anwender an Office 365 nicht mit den Benutzerkonten aus dem Office 365-Verzeichnisdienst an, sondern mit einem Sicherheitstoken, mit dem sie identifiziert werden können. Dieses Sicherheitstoken wird dabei von einer lokalen AD FS-Infrastruktur erstellt. Nach der Anmeldung arbeiten die Anwender entsprechend der Lizenz Ihres Benutzerkontos aus dem Office 365-Verzeichnisdienst. Der Identitätsprovider ist hier Ihr lokales Active Directory.
- *Active-Directory-Synchronisierung*
  Dabei handelt es sich um eine im lokalen Netzwerk zu installierende Komponente, die in einem regelmäßigen Intervall im Active Directory vorhandene Objekte im Office 365-Verzeichnisdienst nachpflegt. Dazu gehören die Benutzerkonten, Gruppen und Kontakte. Setzen Sie diese optionale Komponente ein, werden die Active-Directory-Benutzer in Office 365 automatisch angelegt, und Sie müssen sie nur noch mit einer Lizenz (und gegebenenfalls einem Kennwort) ausstatten. Die Active-Directory-Synchronisierung sehen wir uns in Abschnitt 4.2, »Active-Directory-Synchronisierung«, im Detail an.

Grundsätzlich gibt es in Office 365 drei unterschiedliche Szenarien, wie Sie mit Identitäten umgehen. Sehen wir uns diese genauer an:

- *Szenario »Microsoft-Online-Identität«*
  In diesem Szenario legen Sie im Office 365-Verzeichnisdienst manuell Benutzerkonten für Ihre Anwender an. Dies können Sie beispielsweise ganz klassisch über das Office 365-Portal durchführen, wie ich es in Abschnitt 2.5.2, »Benutzer anlegen«, beschrieben habe. Eine Alternative zur Automatisierung wäre die PowerShell, wie in Abschnitt 3.16.3, »Benutzer anlegen«, beschrieben.

  Ihre Anwender melden sich an Office 365 über das Benutzerkonto aus dem Office 365-Verzeichnisdienst an. Die Authentifizierung erfolgt also nicht im lokalen Active Directory, sondern direkt in Office 365.

  Lassen Sie sich dieses Szenario durch den Kopf gehen, erkennen Sie verschiedene Nachteile, beispielsweise:

  – Die Anwender müssen mit zwei Identitäten umgehen – einmal mit der lokalen Identität und einmal mit der Identität aus Office 365. Sie müssen also auch mit zwei unterschiedlichen Kennwörtern und manchmal auch mit unterschiedlichen Benutzernamen umgehen können und erkennen, wann sie welches einzugeben haben.

– Identische Kennwörter sind dabei oft nicht möglich, da unterschiedliche Kennwortrichtlinien und Ablaufzeiten bestehen (siehe Abschnitt 2.5.5, »Kennwortablaufrichtlinie«). Vergisst ein Anwender sein Kennwort, muss es potenziell an zwei unterschiedlichen Stellen zurückgesetzt werden.

Dieses Szenario hat aber auch zwei große Vorteile:

– Es fällt zu Beginn der geringste Konfigurationsaufwand an.
– Es kann direkt nach dem Anlegen eines Office 365-Mandanten angewandt werden, ohne dass an der lokalen Umgebung Änderungen vorgenommen werden müssen.

Abbildung 4.1 zeigt das Szenario in einem Schaubild.

- *Szenario »Microsoft-Online-Identität mit Active-Directory-Synchronisierung«*
  Im Unterschied zum ersten Szenario legen Sie hier die Benutzerkonten im Office 365-Verzeichnisdienst nicht selbst an, sondern lassen das über eine optionale Softwarekomponente erledigen. Dabei werden in Office 365 automatisch die im lokalen Active Directory vorhandenen Benutzer, Gruppen und Kontakte erstellt (siehe Abbildung 4.2).

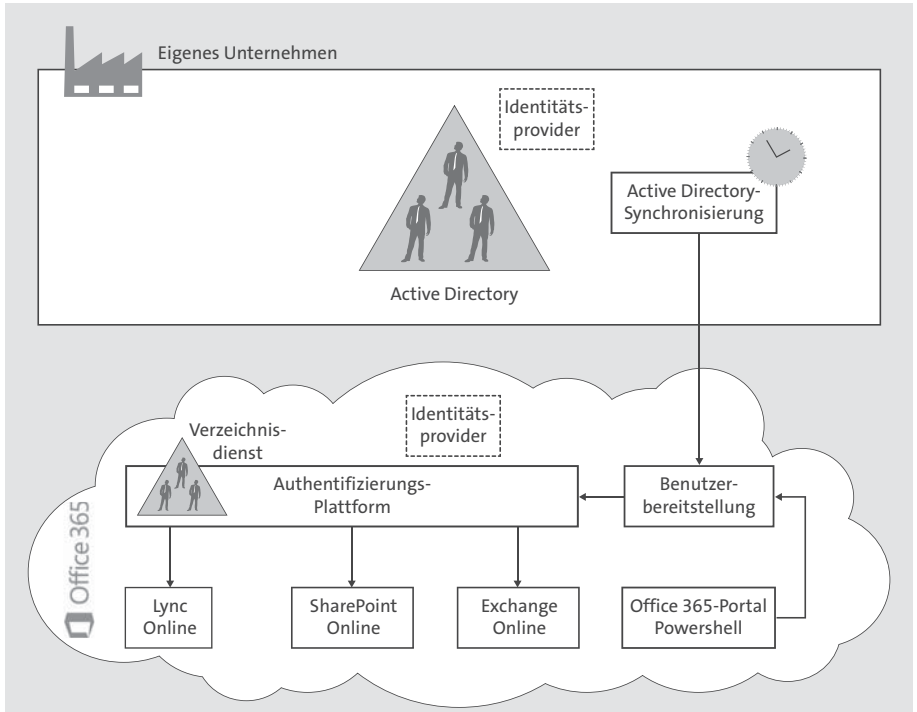

Abbildung 4.2 Microsoft-Online-Identitäten mit Active-Directory-Synchronisierung

Sie können in diesem Szenario optional die Kennwortsynchronisierung aktivieren. Dabei werden die Hash-Werte der lokalen Kennwörter abermals gehasht (ein

»Fingerabdruck« wird erzeugt) und zum Office 365-Verzeichnisdienst übertragen. Klartextkennwörter werden dabei also nicht ausgetauscht.

Wird die Kennwortsynchronisierung aktiviert, können sich Ihre Anwender an Office 365 mit dem gleichen Benutzernamen und dem gleichen Kennwort anmelden wie an der lokalen Umgebung. Vorausgesetzt wird hier jedoch, dass sich die Anwender mit dem *User Principal Name (UPN)* anmelden (dieser hat die Form `user@domäne` – im Gegensatz zum *SAM Account Name* in der Form `Domäne\Benutzer`; dazu später mehr). Da die Anwender in der Regel aber dennoch für die lokale Umgebung und für Office 365 unterschiedliche Benutzerkonten verwenden, spricht man hier von einem *Same Sign-on*.

- *Szenario »Verbundidentität mit Active-Directory-Synchronisierung«*
  Die Active-Directory-Synchronisierung ist in diesem Szenario obligatorisch. Im Vergleich zu den beiden vorangegangenen Szenarien gibt es einen ganz wesentlichen Unterschied: Obwohl durch die Synchronisierung auch im Office 365-Verzeichnisdienst für jeden Anwender ein Benutzerkonto angelegt wird, verwenden die Anwender diese nicht für die Anmeldung.

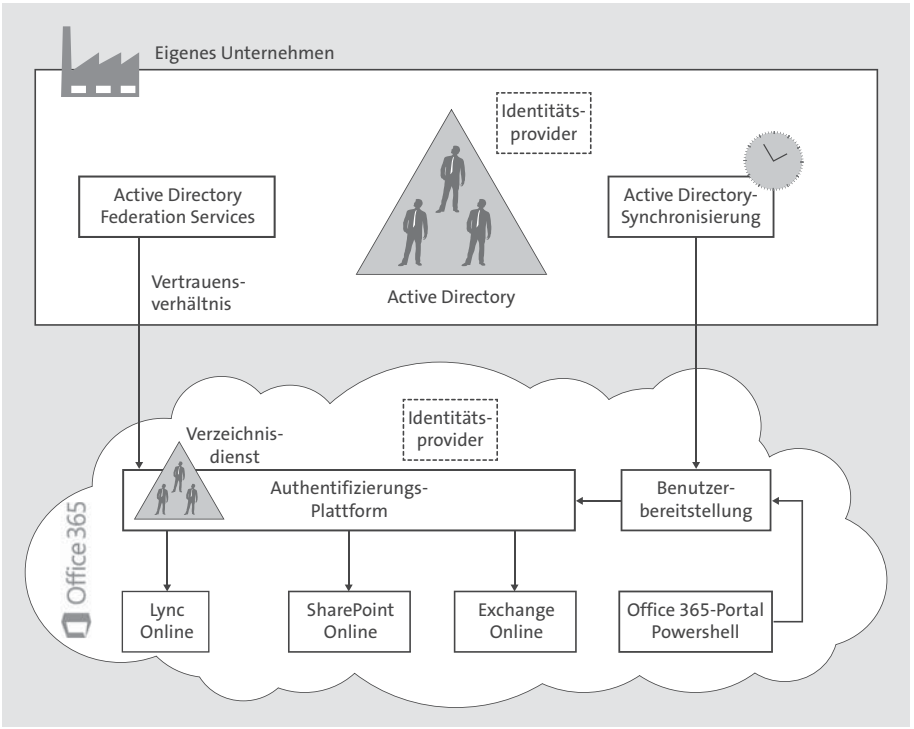

Abbildung 4.3 Verbundidentitäten mit Active-Directory-Synchronisierung

Über ein Vertrauensverhältnis zwischen Office 365 und dem lokalen Active Directory erkennt Office 365 die lokale Anmeldung an, mit dem Ziel, ein *Single-Sign-on-Verfahren* zu erreichen. Die Lizenzierung erfolgt aber nach wie vor in Office 365,

weshalb dort auch die Benutzerkonten über die Active-Directory-Synchronisierung angelegt werden müssen (siehe Abbildung 4.3). Dieses Szenario erfordert eine relativ aufwendige Konfiguration auf Basis der *Active Directory Federation Services* (*AD FS* oder auf Deutsch *Active Directory-Verbunddienste*). Wie das geht, werde ich Ihnen in Abschnitt 4.3, »Identitätsverbund für Single Sign-on«, zeigen.

Same Sign-on oder Single Sign-on?

Bei der Integration von Office 365 mit Ihrer lokalen Active-Directory-Umgebung müssen Sie entscheiden, ob Same Sign-on (Kennwortsynchronisierung) ausreichend ist, oder ob doch Single Sign-on auf Basis von AD FS erforderlich ist. Identisch sind die beiden Verfahren nicht. Hier die wichtigsten Unterschiede:

- Same Sign-on ist nicht gleich Single Sign-on

  Die Kennwortsynchronisierung bei Same Sign-on sorgt lediglich dafür, dass die Kennwörter der Office 365-Benutzerkonten identisch mit den lokalen Active-Directory-Benutzerkonten sind – eine Anmeldung an Office 365 ist aber dennoch erforderlich. Mit Single Sign-on wäre dies im Idealfall nicht erforderlich. Beispiel: Ein Benutzer ist am lokalen Active Directory angemeldet. Er öffnet den Internet Explorer und ruft eine SharePoint Online-Website auf. Haben Sie die Kennwortsynchronisierung eingerichtet, muss er nun seine Office 365-Benutzerdaten angeben (diese sind identisch mit den lokalen Benutzerdaten). Bei Single Sign-on ist keine erneute Anmeldung erforderlich, und das Anmeldefenster wird auch nicht angezeigt (sofern alle erforderlichen Konfigurationen durchgeführt wurden, beispielsweise die SharePoint-URL zu den vertrauenswürdigen Sites im Internet Explorer hinzugefügt wurde).
- Same Sign-on kennt keine Zugriffssteuerung

  Mit AD FS können Sie konfigurieren, von wo aus der Zugriff auf Office 365 möglich sein soll. So könnten Sie den Zugriff einschränken, wenn er von außerhalb Ihrer Netzwerkumgebung erfolgt. Auch das Einschränken von bestimmten Anwendungen und Protokollen wäre möglich. Solche Konfigurationen sind mit der Kennwortsynchronisierung dagegen nicht machbar.
- Manche Szenarien erfordern Single Sign-on

  Dazu gehört beispielsweise die kombinierte Suche bei SharePoint: Setzen Sie sowohl eine lokale SharePoint-Umgebung als auch SharePoint Online ein und möchten die Anwender bei einer SharePoint-Suche die Ergebnisse von beiden Umgebungen kombiniert erhalten, muss Single Sign-on eingerichtet sein. Mehr dazu lesen Sie im Abschnitt 7.20.2, »Kombinierte Suche«.
- Single Sign-on erfordert meist zusätzliche Server

  Mit Ausnahme des Servers, auf dem das Synchronisierungstool läuft, ist für Same Sign-on kein zusätzlicher Server erforderlich. Gerade für kleinere Firmen ist dies ein wichtiges Merkmal. Single Sign-on erfordert dagegen AD FS, was typischerweise auf mehreren Servern eingerichtet wird. Diese Server können zwar gerne virtuell sein, jedoch müssen sie dennoch lizenziert, überwacht und gewartet werden.

- Fällt AD FS aus, ist keine Office 365-Anmeldung möglich

  Sollte die komplexe AD FS-Infrastruktur bei Single Sign-on ausfallen oder kann sie aufgrund von Problemen mit Ihrem Internetprovider nicht erreicht werden, können sich Ihre Anwender nicht mehr an Office 365 anmelden. Fällt dagegen das Synchronisierungstool bei Same Sign-on aus, ist eine Anmeldung an Office 365 weiterhin möglich, und sollte es Probleme mit dem Internetprovider geben, können Ihre Anwender im Zweifelsfall über UMTS & Co. durchaus noch mit Office 365 arbeiten.

  Die Kennwortsynchronisierung kann als Übergangslösung bei Problemen mit AD FS eingesetzt werden. Lesen Sie hierzu Abschnitt 4.3.10, »Wenn AD FS ausfällt«. [«]

Grundsätzlich gilt die Empfehlung, Verbundidentitäten – also Single Sign-on – nur dann einzusetzen, wenn es einen wirklich triftigen Grund dafür gibt, denn der Kosten- und Verwaltungsaufwand für die dabei notwendige AD FS-Umgebung ist viel zu groß. Die Erfahrung zeigt, dass für die meisten Unternehmen Same Sign-on durchaus ausreichend ist.

Tabelle 4.1 zeigt einen Vergleich der drei Identitätsvarianten.

Kriterium	Microsoft-Online-Identität	Microsoft-Online-Identität + Synchronisierung	Verbundidentität + Synchronisierung
Zielgruppe	kleine Unternehmen	mittlere und große Unternehmen mit eigenem Active Directory	große Unternehmen mit eigenem Active Directory
Same Sign-on	nein	optional	nein
Single Sign-on	nein	nein	ja
Identitäten pro Anwender	2	2	1
Welche Kennwortrichtlinien gelten?	lokal + Office 365	nur lokal (bei aktiver Kennwortsynchronisierung, sonst lokal + Office 365)	nur lokal

Tabelle 4.1 Vergleich der Identitätsalternativen

Kriterium	Microsoft-Online-Identität	Microsoft-Online-Identität + Synchronisierung	Verbundidentität + Synchronisierung
Ort der Authentifizierung	lokal + Office 365	lokal + Office 365	nur lokal
Ort der Benutzerverwaltung	lokal + Office 365	nur lokal	nur lokal
Zusätzliche lokale Installation erforderlich	nein	ja, für Synchronisierung	ja, für Synchronisierung + AD FS

Tabelle 4.1 Vergleich der Identitätsalternativen (Forts.)

In den folgenden Abschnitten werden wir uns um die Einrichtung dieser Szenarien kümmern.

[»] Microsoft arbeitet gerade an einem Assistenten namens Azure AD Connect, der die Einrichtung der Active-Directory-Synchronisierung und optional auch eines Identitätsverbunds vereinfacht. Sie können dabei mit einem einzigen Tool sowohl die Synchronisierung als auch die erforderliche AD FS-Umgebung für Single Sign-on einrichten. Ist das Tool bereits verfügbar, wenn Sie diese Zeilen lesen, können Sie dennoch die Informationen dieses Kapitels nutzen, um das Tool mit den für Ihre Umgebung geeigneten Einstellungen zu konfigurieren. Die Konfigurationsoberfläche ähnelt dabei der von AADSync, welches den Schwerpunkt des nächsten Abschnitts bildet. Bei Interesse können Sie die Preview-Version von Azure AD Connect hier erhalten: *http://connect.microsoft.com/site1164/program8612*

4.2 Active-Directory-Synchronisierung

Bei der Active-Directory-Synchronisierung handelt es sich um eine optionale Konfiguration. Ein Vorteil dabei ist, dass Sie bei der Verwaltung Ihres Office 365-Mandanten entlastet werden. Die Synchronisierung wird über ein *Verzeichnissynchronisierungstool* durchgeführt. Zur Auswahl stehen dabei mehrere Tools:

- *DirSync* – das bis Ende 2014 für Single-Forest-Umgebungen primär eingesetzte Verzeichnissynchronisierungstool im Rahmen von Office 365
- *AADSync* (siehe Abbildung 4.4) – der seit Herbst 2014 verfügbare Nachfolger von DirSync, der im Gegensatz zu DirSync auch Multi-Forest-Umgebungen unterstützt.
- *Forefront Identity Manager (FIM)* mit dem *Forefront Identity Manager Connector for Azure Active Directory* – insbesondere für Kunden, die FIM bereits einsetzen und diese Infrastruktur auch für Office 365 nutzen wollen

Tabelle 4.2 vergleicht die drei Tools miteinander.

	DirSync	AADSync	FIM + Connector
Single-Forest-Umgebungen	ja	ja	ja
Multi-Forest-Umgebungen	nein	ja	ja
Kennwortsynchronisierung (optional)	ja	ja	nein

Tabelle 4.2 Vergleich Verzeichnissynchronisierungstools

DirSync erhalten Sie heute als Download über Ihren Office 365-Mandanten. Allerdings hat Microsoft die Weiterentwicklung des Tools eingestellt. Der Nachfolger ist AADSync. Damit bildet AADSync auch den Schwerpunkt in diesem Kapitel. DirSync und AADSync nutzen eine angepasste Konfiguration von FIM. Mit dessen Administrationskonsole kommen Sie in manchen Fällen in Berührung, beispielsweise bei der Fehlersuche oder bei der Konfiguration von Filtern, mit deren Hilfe Objekte synchronisiert werden sollen. Die Nutzung von FIM außerhalb von AADSync werde ich hier nicht weiter berücksichtigen, um den Rahmen des Buches nicht zu sprengen.

AADSync läuft im Hintergrund und gleicht in einem regelmäßigen Intervall von drei Stunden automatisch Elemente Ihres Active Directorys mit dem Verzeichnisdienst von Office 365 ab. Betroffen sind dabei folgende Objekte:

- Benutzerkonten
- Gruppen
- Kontakte

Eine Auflistung der synchronisierten Attribute finden Sie unter der folgenden URL:

http://msdn.microsoft.com/library/azure/dn764938.aspx

Neu angelegte Objekte im lokalen Active Directory werden automatisch beim nächsten Synchronisationslauf im Office 365-Verzeichnisdienst angelegt, beispielsweise die Benutzerkonten neuer Mitarbeiter. Löschen oder ändern Sie lokal ein Objekt, wird es auch in Office 365 gelöscht oder geändert.

Dabei handelt es sich grundsätzlich um eine *Pushsynchronisierung* ausgehend von Ihrem Active Directory hin zu Office 365. Nur bei zwei Szenarien werden manche Active-Directory-Eigenschaften vom AAD Ihres Office 365-Mandanten zurück in Ihr Active Directory synchronisiert:

- Exchange-Hybridbereitstellung (siehe Abschnitt 6.13, »Hybridbereitstellung«)
- Kennwort zurückschreiben – dabei werden Kennwortänderungen, die der Anwender in Office 365 vornimmt, zur lokalen Umgebung übertragen (nur möglich, wenn Sie über AAD Premium verfügen, was separat über Microsoft Azure eingekauft werden muss)

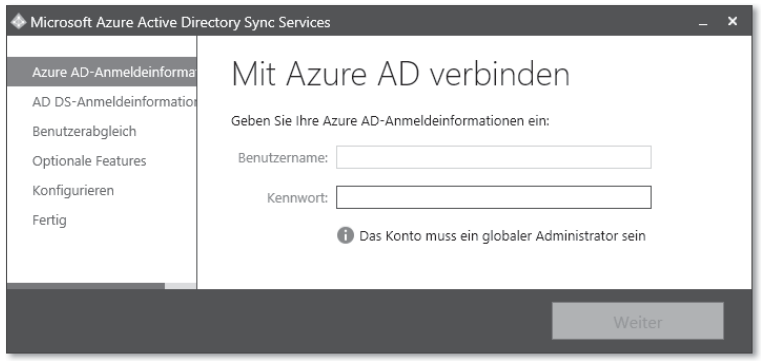

Abbildung 4.4 Konfiguration von AADSync

Nach der Aktivierung der Active-Directory-Synchronisierung verwalten Sie Ihre Benutzer, Gruppen und Kontakte primär mit den Verwaltungstools des lokalen Active Directorys. Die Benutzerverwaltung von Office 365 verwenden Sie dagegen primär für die Lizenzierung der synchronisierten Benutzerkonten.

Die Synchronisierung ist insbesondere in folgenden Szenarien eine Voraussetzung:

- für die Einrichtung eines Identitätsverbunds (siehe Abschnitt 4.3, »Identitätsverbund für Single Sign-on«)
- für die Einrichtung einer Exchange-Hybridbereitstellung (siehe Abschnitt 6.13, »Hybridbereitstellung«)
- für die mehrstufige Exchange-Migration (siehe Abschnitt 6.12.4, »Mehrstufige Migration«)

4.2.1 Synchronisierungsvorgang

Nachdem Sie das Verzeichnissynchronisierungstool installiert und konfiguriert haben, erfolgt eine vollständige Synchronisierung der unterstützten Objekte. Diese initiale Synchronisierung (*Full Sync*) dauert am längsten. Bei den weiteren Synchronisierungsläufen werden nur die Änderungen berücksichtigt (*Delta Sync*).

Während der Synchronisierung werden in der Standardkonfiguration zwei Strategien angewandt, die Objekte aus dem lokalen Active Directory mit dem Verzeichnisdienst von Office 365 abzugleichen:

1. GUID-Vergleich
   Wird ein Objekt durch das Synchronisierungstool im Office 365-Verzeichnisdienst angelegt, erhält es dort eine Markierung mit der Object-GUID des entsprechenden Objekts aus dem lokalen Active Directory (*Net-ID* genannt). Daran wird es bei zukünftigen Synchronisierungsverläufen erkannt.
2. SMTP-Vergleich
   Wird im Office 365-Verzeichnisdienst kein Objekt mit passender GUID gefunden, werden (sofern vorhanden) die primären SMTP-Adressen verglichen. Dieser Fall tritt beispielsweise dann auf, wenn Sie schon vor der Aktivierung der Synchronisierung im Office 365-Mandanten Benutzerkonten mit entsprechenden SMTP-Adressen anlegen. Zuständig ist das Active-Directory-Attribut `proxyAddresses`. Die primäre SMTP-Adresse ist dort als Wert in der Form `SMTP:benutzer@domäne` hinterlegt. SMTP muss dabei für die primäre Adresse großgeschrieben sein.

   Während der Synchronisierung werden passende Office 365-Benutzer dann mit den lokalen Active-Directory-Benutzern verbunden.

   Achtung: Verfügen die lokalen Benutzer über ein Exchange-Postfach und die Office 365-Benutzer bereits über ein Exchange Online-Postfach (dieses wird automatisch angelegt, wenn dem Benutzer eine Exchange Online-Lizenz zugewiesen wird), kann das zu Problemen führen. Das äußert sich beispielsweise so, dass die Migration der Postfachinhalte über den dafür vorgesehenen Weg nicht möglich ist. Ein nicht benötigtes Exchange Online-Postfach können Sie durch Lizenzentzug entfernen. [«]

Active Directory-GUID und die Net-ID

Die GUID von lokalen Active-Directory-Benutzerkonten und die zugehörige Net-ID können Sie selbst über die PowerShell auslesen. Die Objekt-GUID steht in der Eigenschaft `ObjectGUID` des Active-Directory-Benutzerkonto-Objekts, die Net-ID in der Eigenschaft `ImmutableId` des Office 365-Benutzerkonto-Objekts. Die `ObjectGUID` ist vom Typ *GUID*, die `ImmutableId` vom Typ *Base 64 String*.

Ist die `ImmutableId` leer, wurde das Benutzerkonto nicht über die Active-Directory-Synchronisierung angelegt.

Hier ein Beispiel, um die IDs auszulesen:

```
$upn = "lucy@beispielag.de"

Import-Module ActiveDirectory
Import-Module MSOnline

#Office 365-Anmeldung
Connect-MsolService
```

```
#Ermittlung der lokalen Objekt-GUID
$ObjectGUID =
   (Get-ADUser -Filter { UserPrincipalName -eq $upn }).ObjectGUID

#Ermittlung der ImmutableId
$ImmutableIdBase64 =
   (Get-MsolUser -UserPrincipalName $upn).ImmutableId

#Umwandlung von Base 64 String zu GUID
$ImmutableId =
   [GUID]([System.Convert]::FromBase64String($ImmutableIdBase64))

#Ausgabe
"Objekt-GUID: " + $ObjectGUID.Guid
"Net-ID (Base 64): " + $ImmutableIdBase64
"Net-ID (GUID): " + $ImmutableId.Guid
```

Listing 4.1 Auslesen von Objekt-GUID und Net-ID

UPN steht im Skript für *User Principal Name* oder auf Deutsch *Benutzerprinzipalname*, also für den Benutzernamen des Kontos.

Voraussetzung für diesen Code ist jedoch, dass Sie über das `ActiveDirectory`-Modul (siehe Abschnitt 3.17, »PowerShell und Active Directory«) und über das Azure Active Directory-Modul für Windows PowerShell (siehe Abschnitt 3.16.1) verfügen und dass die Active-Directory-Synchronisierung bereits eingerichtet wurde. Ein Beispiel für die Ausgabe sehen Sie in Abbildung 4.5.

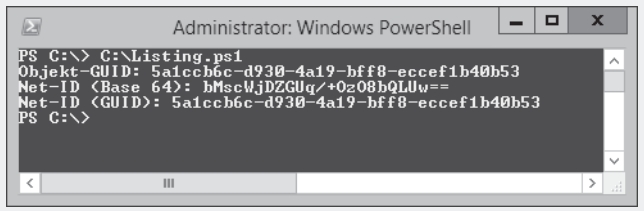

Abbildung 4.5 Auslesen von Objekt-GUID und Net-ID

In der Praxis gibt es Situationen, in denen Sie selbst die Net-ID eines Office 365-Benutzerkontos festlegen wollen. Nehmen wir beispielsweise dieses Szenario: Sie haben bisher Office 365 nur für SharePoint Online eingesetzt. Die erforderlichen Benutzerkonten haben Sie manuell in der Office 365-Benutzerverwaltung angelegt und mit einer SharePoint Online-Lizenz ausgestattet. Die Benutzernamen der Benutzerkonten haben Sie genauso angegeben wie bei den Benutzerkonten im lokalen Active Directory. Da Sie nur SharePoint Online-Lizenzen vergeben haben, verfügen die Office 365-Benutzerkonten über keine E-Mail-Adresse. Nun wollen Sie die Verzeichnissynchronisierung verwenden, erhalten aber Synchronisierungsfehler wie in Abbildung 4.6.

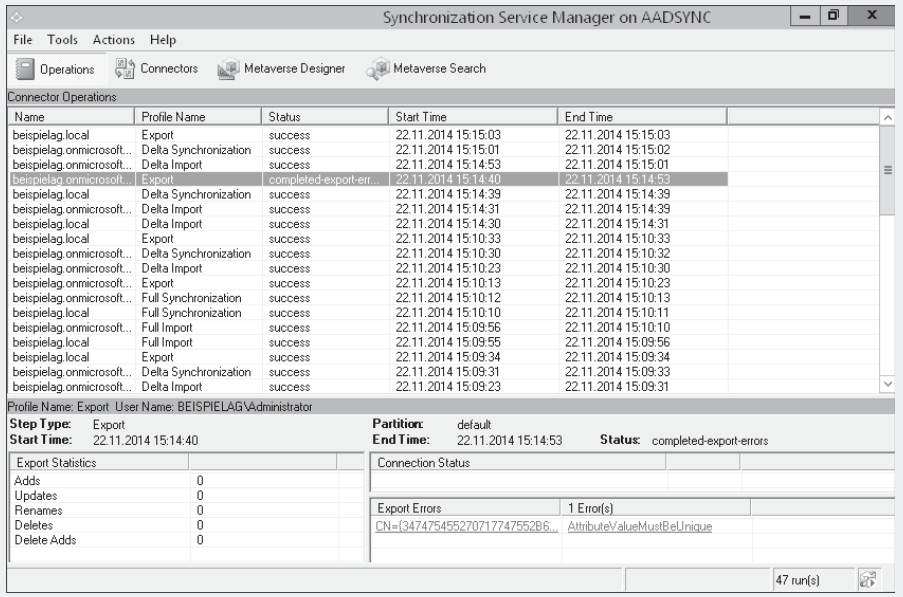

Abbildung 4.6 Synchronisierungsfehler

Der Grund dafür ist folgender: Das Synchronisierungstool versucht zunächst einen GUID-Vergleich, was nicht geht, da bei den Office 365-Benutzern keine Net-ID vorhanden sind. Dann versucht es einen SMTP-Vergleich, was auch nicht geht, da bei den Office 365-Benutzern keine E-Mail-Adresse vorhanden ist. Dennoch werden in beiden Verzeichnisdiensten Benutzerkonten mit identischen Benutzernamen gefunden – und damit schlägt die Synchronisierung bei diesen Benutzern fehl.

Um in dieser Situation die Office 365-Benutzer manuell mit der richtigen Net-ID auszustatten, können Sie folgendes PowerShell-Skript verwenden:

```
$upn = "lucy@beispielag.de"

Import-Module ActiveDirectory
Import-Module MSOnline

#Office 365-Anmeldung
Connect-MsolService

#Ermittlung der lokalen Objekt-GUID
$ObjectGUID = (Get-ADUser -Filter {
   UserPrincipalName -eq $upn }).ObjectGUID

#Umwandlung von GUID zur Base 64 String
$ImmutableId = [System.Convert]::ToBase64String($ObjectGUID.ToByteArray())
```

```
#Setzen der ImmutableId
Set-MsolUser -UserPrincipalName $upn -ImmutableId $ImmutableId
```

Listing 4.2 Manuelles Setzen der Net-ID

Damit »weiß« das Synchronisierungstool, welche Benutzerkonten zusammengehören.

Eine Alternative zum Setzen der Net-ID besteht im Setzen der Proxy-Adressen (dazu gehören E-Mail- und SIP-Adressen). Vorausgesetzt, Sie haben den Benutzerkonten in Office 365 Exchange Online-Lizenzen zugewiesen, verfügen diese über Proxy-Adressen. Wichtig ist dabei die primäre E-Mail-Adresse. Setzen Sie die primäre E-Mail-Adresse in das entsprechende Attribut des lokalen Benutzerkontos, kann das Synchronisierungstool auf Basis dessen ebenfalls eine Zuordnung vornehmen. Mit einem PowerShell-Skript könnten Sie die Proxy-Adressen eines Office 365-Benutzerkontos auslesen und das lokale Benutzerkonto entsprechend modifizieren. Hier ein Beispiel:

```
$upn = "lucy@beispielag.de"
Import-Module ActiveDirectory
Import-Module MSOnline

#Office 365-Anmeldung
Connect-MsolService

$localuser = Get-ADUser -Filter { UserPrincipalName -eq $upn }
$o365proxy = (Get-Mailbox -Identity $upn).EmailAddresses
Set-ADUser -Identity $localuser -Add @{ proxyAddresses = @($o365proxy) }
```

Listing 4.3 Übertragen der Proxy-Adressen

Diese Kommandos setzen voraus, dass lokal das Azure Active Directory-Modul für PowerShell vorhanden ist (siehe Abschnitt 3.16.1) und dass mit PowerShell eine Verbindung zu Exchange Online aufgebaut wurde (siehe Abschnitt 6.3.3). Mit `Get-ADUser` wird der lokale Benutzer gesucht, mit `Get-Mailbox` das Postfach des Office 365-Benutzers. Von Letzterem werden die Proxy-Adressen ausgelesen (Eigenschaft `EmailAddresses`), um diese dann mit `Set-ADUser` auf den lokalen Benutzer zu übertragen (Eigenschaft `proxyAddresses`). Es wird hier angenommen, dass das Attribut `proxyAddresses` leer ist.

[»] Das Auslesen der Office 365-Proxy-Adressen sollte in der Praxis nicht mit dem Cmdlet `Get-MsolUser` vorgenommen werden. Der Befehl liefert zwar über die Eigenschaft `ProxyAddresses` die E-Mail-Adressen, nicht aber die SIP-Adresse. Um alle Proxy-Adressen zu berücksichtigen, ist das Vorgehen über `Get-Mailbox` erforderlich.

Das Intervall zwischen den Synchronisierungsverläufen beträgt fest vorgegeben drei Stunden. Allerdings können Sie die Synchronisierung bei Bedarf manuell starten, beispielsweise wenn das Benutzerkonto des neuen Mitarbeiters sofort in Office 365 verfügbar sein soll und nicht erst nach bis zu drei Stunden (siehe Abschnitt 4.2.7, »Manueller Start der Synchronisierung«).

4.2.2 Kennwortsynchronisierung

Mit AADSync werden auf Wunsch Änderungen an den Kennwörtern der lokalen Benutzerkonten erkannt, und das neue Kennwort wird zum zugehörigen Office 365-Benutzerkonto übertragen. Dabei gelten die Kennwortrichtlinien des lokalen Active Directorys, die Richtlinien von Office 365 werden außer Kraft gesetzt. Anwender müssen sich also nicht mehr unterschiedliche Kennwörter merken.

AADSync überträgt dabei nicht die Kennwörter selbst, sondern daraus generierte Hash-Werte. Damit ist ein Zugriff auf die Klartextkennwörter nie erforderlich.

Die Synchronisation der Kennwörter nimmt AADSync nur in einer Richtung vor, und zwar vom lokalen Active Directory nach Office 365. Mit Aktivierung der Kennwortsynchronisierung kann der Anwender sein Kennwort in Office 365 nicht mehr ändern.

Eine Ausnahme stellt hier die Option *Kennwort zurückschreiben* dar. Dabei werden Kennwortänderungen, die der Anwender in Office 365 vornimmt, an die lokale Umgebung übertragen. Das allerdings ist nur möglich, wenn Sie über AAD Premium verfügen, was separat über Microsoft Azure eingekauft werden muss. [«]

Aktivieren Sie die Kennwortsynchronisierung, verbleibt das Intervall zur Synchronisation von Active-Directory-Objekten bei drei Stunden. Für die Kennwortsynchronisierung gilt dieses Intervall aber nicht: Änderungen an den Kennwörtern werden in der Praxis spätestens innerhalb weniger Minuten übertragen.

Sehen wir uns verschiedene Szenarien an:

- Ein neues lokales Active-Directory-Benutzerkonto wird angelegt

  Mit dem Start des nächsten Intervalls (alle drei Stunden) wird AADSync ein passendes Benutzerkonto in Office 365 anlegen.

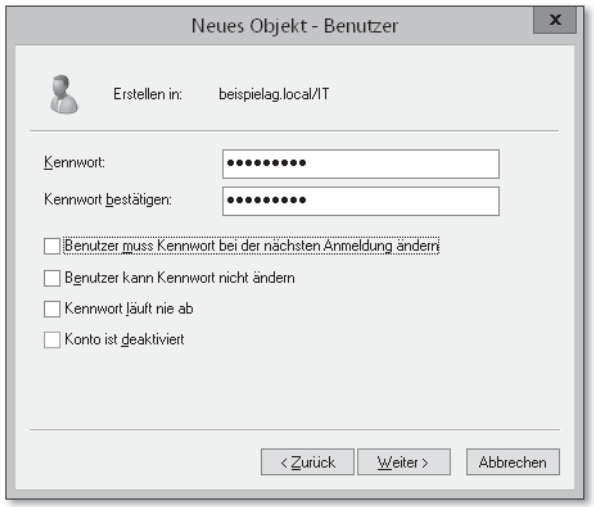

Abbildung 4.7 Anlegen eines neuen Benutzers

Wurde beim Anlegen des Benutzerkontos die Option Benutzer muss Kennwort bei der nächsten Anmeldung ändern nicht ausgewählt (siehe Abbildung 4.7), entspricht das Kennwort des Office 365-Benutzerkontos unmittelbar nach der Synchronisierung dem lokalen Kennwort. Ist die Option dagegen ausgewählt, muss sich der Anwender zunächst lokal anmelden, sein Kennwort ändern, und erst dann erfolgt die Synchronisierung zu Office 365.

- Anwender ändert das Kennwort seines lokalen Active-Directory-Benutzerkontos

  Die Änderung wird zu seinem Office 365-Benutzerkonto übertragen.

- Anwender ändert das Kennwort seines Office 365-Benutzerkontos

  Die Änderung wird nicht zu seinem lokalen Active-Directory-Benutzerkonto übertragen. Ändert er später sein Kennwort lokal, wird das Office 365-Kennwort überschrieben. Änderungen des Kennworts in Office 365 sind dann nicht mehr möglich.

- Kennwort des lokalen Active-Directory-Benutzerkontos ist abgelaufen

  Aktivieren Sie die Kennwortsynchronisierung, werden die betroffenen Office 365-Benutzerkonten automatisch so konfiguriert, dass deren Kennwörter nicht mehr ablaufen. Läuft nun das Kennwort eines lokalen Active-Directory-Benutzerkontos ab, wirkt sich das nicht auf das Office 365-Benutzerkonto aus. Der Anwender kann sich mit seinem abgelaufenen Kennwort weiterhin an Office 365 anmelden.

- Helpdesk setzt Kennwort eines lokalen Active-Directory-Benutzerkontos zurück

  Hierbei muss unterschieden werden, ob der Helpdesk-Mitarbeiter die Option Benutzer muss Kennwort bei der nächsten Anmeldung ändern aktiviert hat (siehe Abbildung 4.8). Ist die Option nicht ausgewählt, wird das Kennwort sofort an Office 365 übermittelt. Ist die Option dagegen ausgewählt, muss sich der Anwender zunächst mit seinem lokalen Active-Directory-Benutzerkonto anmelden. Dabei wird er zur Änderung seinen Kennworts aufgefordert, und das neue Kennwort wird dann zu Office 365 übertragen.

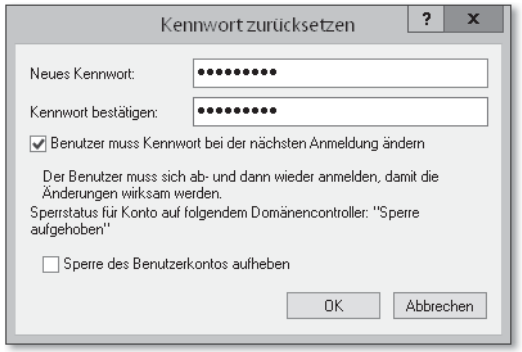

Abbildung 4.8 Kennwort zurücksetzen

4.2.3 Planung und Vorbereitung

Die Einrichtung der Synchronisierung ist ein wichtiger Schritt bei der Anbindung Ihres Office 365-Mandanten an das lokale Active Directory. Dabei müssen Sie aber einige Punkte berücksichtigen, die ich Ihnen in diesem Abschnitt erläutern werde.

Einschränkungen

- Anzahl Active-Directory-Objekte

  Beim AADSync gibt es zwei Grenzwerte bei der Anzahl von Active-Directory-Objekten. Keine Probleme treten auf bei bis zu 300.000 Objekten (Benutzer, Gruppen, Kontakte). Vorausgesetzt, Sie haben in Ihrem Office 365-Mandanten eine eigene Domäne verifiziert – ansonsten gilt hier eine Grenze von 50.000 Objekten.

  Werden mehr als 300.000 Objekte synchronisiert, kontaktieren Sie den Office 365-Kundendienst für eine entsprechende Freischaltung Ihres Office 365-Mandanten (siehe Abschnitt 2.11, »Problembehebung«).

  Werden weniger als 100.000 Objekte synchronisiert, kann das Verzeichnissynchronisierungstool den automatisch mit installierten *Microsoft SQL Server Express LocalDB* verwenden. Bei mehr Objekten ist eine Instanz der »großen« SQL Server erforderlich, die dann gesondert konfiguriert werden muss.

- Administration von Benutzerkonten

  Es ist zwar nicht wirklich eine Einschränkung, aber Sie sollten es dennoch beachten: Sobald die Synchronisierung aktiviert ist, können Sie viele Eigenschaften der Benutzerkonten nur noch über die lokalen Active-Directory-Tools und nicht mehr im Office 365 Admin Center bearbeiten (siehe Abbildung 4.9).

  Es dürfte zunächst eher eine Erleichterung sein, mit den gewohnten Werkzeugen einfach weiterarbeiten zu können. Etwas problematischer wird die Sache, wenn Sie Exchange Online einsetzen. In diesem Fall können von Office 365-Seite aus viele Exchange-Attribute der Benutzerkonten nicht geändert werden, beispielsweise die E-Mail-Adressen. Solche Attribute müssen dann ebenfalls mit lokal vorhandenen Tools verwaltet werden, was sich schwierig gestalten kann, wenn Sie lokal keinen Exchange Server (mehr) haben. Lesen Sie hierzu auch den Abschnitt 6.2.3, »Ändern von Exchange-Attributen mit aktivierter Verzeichnissynchronisierung«. [«]

  Neue Benutzerkonten legen Sie nach der Aktivierung der Synchronisierung auch nur noch lokal im Active Directory an und nicht mehr im Office 365 Admin Center. Benutzerkonten, die Sie dennoch direkt in Office 365 erstellen, werden nicht auch automatisch in Ihrem Active Directory angelegt.

  Dennoch kann es Sinn machen, einzelne Benutzer direkt im Office 365 Admin Center anzulegen, beispielsweise für administrative Benutzer, für externe Anwender, die nur Zugriff auf Office 365, aber nicht auf das lokale Netzwerk bekommen sollen etc.

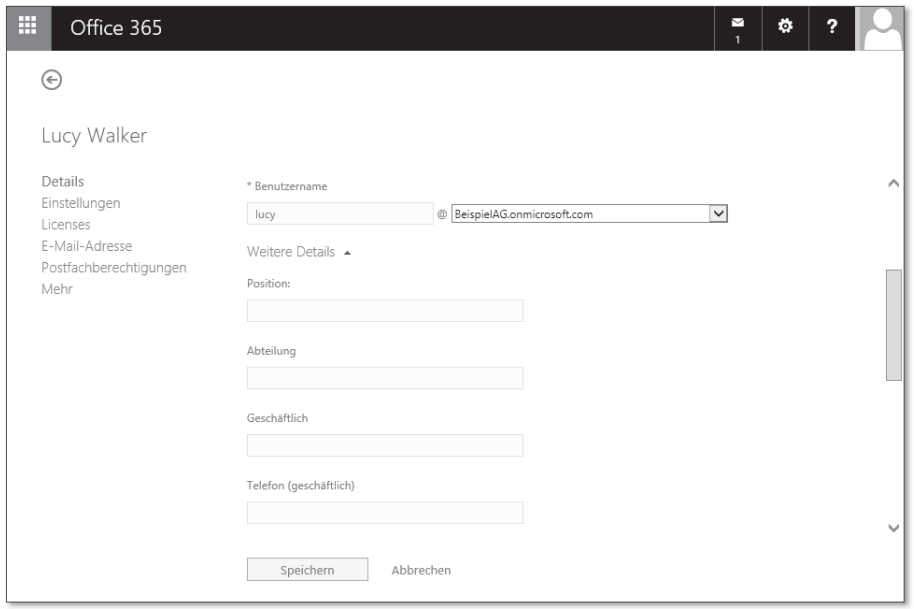

Abbildung 4.9 Eingeschränkte Bearbeitung von Benutzerkonten im Office 365 Admin Center

- Exchange Online-Lizenzierung
  Angenommen, Sie verfügen über einen lokalen Exchange Server und verwenden die Verzeichnissynchronisierung. Weisen Sie dann einem synchronisierten Benutzer eine Lizenz zu, die Exchange Online umfasst, wird für diesen nicht mehr automatisch ein Postfach angelegt, sofern er bereits über ein lokales Postfach verfügt. Stattdessen erscheint die Meldung aus Abbildung 4.10.

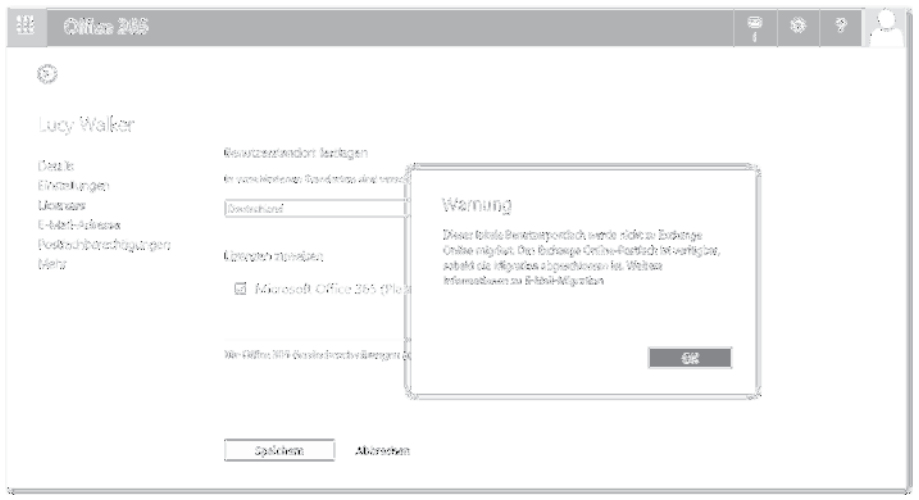

Abbildung 4.10 Meldung beim Zuweisen einer Exchange Online-Lizenz

Das hat auch seinen Grund: Wollten Sie später das lokale Postfach zu Exchange Online verschieben, ginge das nicht mehr, da dort für den Benutzer bereits ein Postfach vorhanden wäre.

Vorbereitungen

Bevor Sie die Active-Directory-Synchronisierung einrichten, sollten Sie einige Dinge überprüfen:

- Active-Directory-Attribute lokaler Benutzerkonten
  Vor der Aktivierung der Synchronisierung sollten Sie sicherstellen, dass die Benutzerprinzipalnamen (UPN) der lokalen Benutzerkonten geeignet gesetzt sind, das heißt, sie erfüllen idealerweise folgende Voraussetzungen:
  - Der Benutzerprinzipalname muss vergeben sein.
  - Die Domänen der Benutzerprinzipalnamen sind in Ihrem Office 365-Mandanten verifiziert (siehe Abschnitt 2.4.2). Das schließt Domänen aus, die im Internet nicht routbar sind, beispielsweise solche mit der Endung *.local* und *.intra*.

  Sollte aus irgendeinem Grund diese Voraussetzung nicht zu erfüllen sein, beispielsweise weil Sie intern eine Anwendung einsetzen, die den Benutzerprinzipalnamen mit einer für Office 365 ungeeigneten Domäne voraussetzt, können Sie für die Office 365-Benutzernamen auch ein anderes Active-Directory-Attribut einsetzen. Mehr dazu lesen Sie in Abschnitt 4.3.9, »Alternative Benutzernamen mit AD FS«. [«]

  Benötigen Sie ein alternatives Benutzerprinzipalnamen-Suffix (beispielsweise, weil Ihre Domäne *beispielag.local* heißt und Sie jetzt bei den Benutzerprinzipalnamen *beispielag.de* verwenden wollen), gehen Sie wie folgt vor:
- Öffnen Sie die Managementkonsole Active Directory-Domänen und -Vertrauensstellungen (siehe Abbildung 4.11). Diese finden Sie im Zweifelsfall auf einem Domänencontroller.

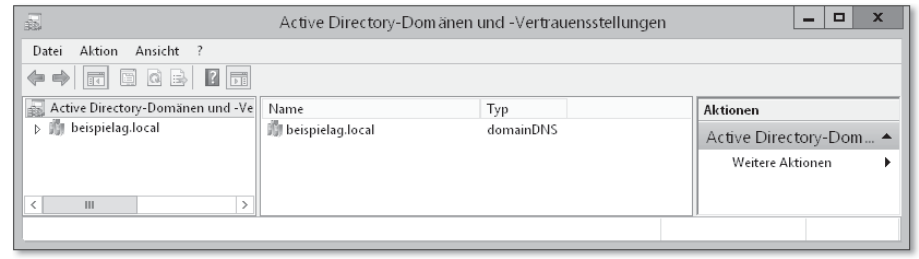

Abbildung 4.11 Active Directory-Domänen und -Vertrauensstellungen

- Klicken Sie mit der rechten Maustaste in der linken Navigation auf Active Directory-Domänen und -Vertrauensstellungen, und wählen Sie im Kontextmenü die Eigenschaften (siehe Abbildung 4.12).

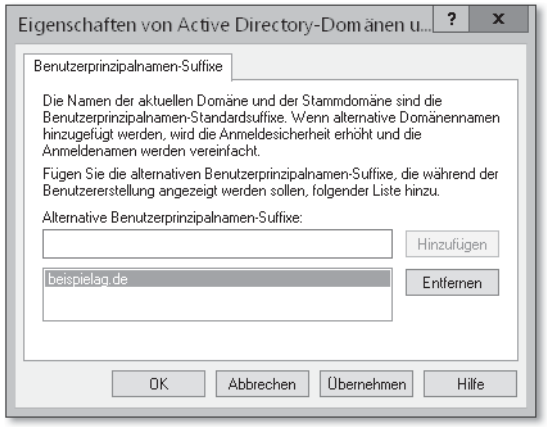

Abbildung 4.12 Hinzufügen eines neuen Benutzerprinzipalnamen-Suffixes

- Fügen Sie im erscheinenden Fenster ein alternatives Benutzerprinzipalnamen-Suffix hinzu. Dieses können Sie dann bei den Benutzerkonten auswählen.

Daneben gelten die Voraussetzungen aus Tabelle 4.3.

Wie Sie die Benutzerprinzipalnamen mithilfe der PowerShell automatisiert vergeben, lesen Sie in Abschnitt 3.17.3, »Anwendung«.

Attribut	Voraussetzungen
displayname	▶ Ist nicht länger als 256 Zeichen. ▶ Enthält keines der folgenden Zeichen: ? @ +
givenName	▶ Ist nicht länger als 64 Zeichen. ▶ Enthält keines der folgenden Zeichen: ? @ +
mail	▶ Ist nicht länger als 256 Zeichen. ▶ Enthält keines der folgenden Zeichen: [! # $ % & * + / = ? ^ ` { }] ▶ Muss eindeutig sein.
mailNickname	▶ Ist nicht länger als 64 Zeichen. ▶ Enthält weder das Leerzeichen noch eines der folgenden Zeichen: " \ [ ] : > < ;
proxyAddresses	▶ Ist nicht länger als 256 Zeichen. ▶ Enthält keines der folgenden Zeichen:) (; > <] [\ ,

Tabelle 4.3 Voraussetzungen Active-Directory-Attribute

Attribut	Voraussetzungen
sAMAccountName	▶ Ist nicht länger als 20 Zeichen. ▶ Enthält keines der folgenden Zeichen: ! # $ % ^ & { } ` ~ " , \ / [ ] : @ < > + = ; ? * ▶ Ist der sAMAccountName ungültig, der userPrincipalName jedoch gültig, wird das Benutzerkonto in Office 365 angelegt.
en	▶ Ist nicht länger als 64 Zeichen. ▶ Enthält keines der folgenden Zeichen: ? @ +
targetAddress	▶ Ist erforderlich für E-Mail-aktivierte Objekte. ▶ Ist nicht länger als 256 Zeichen. ▶ Enthält keines der folgenden Zeichen: [! # $ % & * + / = ? ^ ` { }]
userPrincipalName	▶ Benutzername ist nicht länger als 64 Zeichen. ▶ Domänenname ist nicht länger als 256 Zeichen. ▶ Enthält keines der folgenden Zeichen: }{ #‹* +) (> < / \ = ? ` ▶ @ muss vorhanden sein, darf aber nicht erstes Zeichen sein. ▶ Benutzername endet nicht mit einem der folgenden Zeichen: . & @ ▶ Benutzername hat kein Leerzeichen. ▶ Muss eindeutig sein.

Tabelle 4.3 Voraussetzungen Active-Directory-Attribute (Forts.)

Was sind Benutzerprinzipalnamen (UPNs)?

Benutzerkonten im Active Directory haben potenziell zwei Benutzernamen, wie in Abbildung 4.13 ersichtlich:

- Benutzeranmeldename (= Benutzerprinzipalname, User Principal Name/UPN)

  Dieser Benutzerprinzipalname ist optional und hat die Form einer E-Mail-Adresse: *Benutzer@Domäne*, also beispielsweise *lucy@beispielag.de*. Oftmals ist die E-Mail-Adresse des Benutzers auch identisch mit diesem Benutzerprinzipalnamen – das muss aber nicht so sein. Der Teil hinter dem Klammeraffen wird auch allgemein als Benutzerprinzipalnamen-Suffix bezeichnet, da er nicht identisch mit dem eigentlichen Domänennamen sein muss.

- Benutzeranmeldename (Prä-Windows 2000) (= SAM Account Name)

  Jedes Benutzerkonto im Active Directory verfügt über einen SAM Account Name. Er hat die Form *Domäne\Benutzer*, also beispielsweise *BeispielAG\Lucy*.

Für Office 365 spielt der zweite Anmeldename, also der SAM Account Name, keine Rolle. Legen Sie in Office 365 ein Benutzerkonto an, vergeben Sie auch nur den Benutzerprinzipalnamen als Benutzernamen.

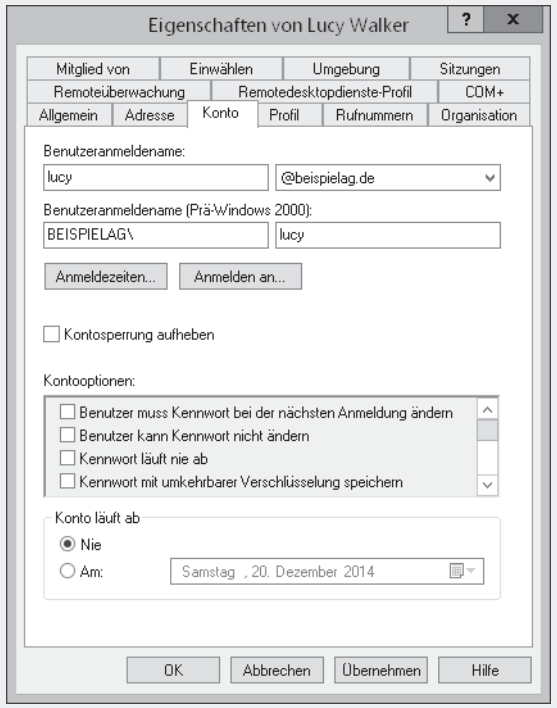

Abbildung 4.13 Benutzerkontoeigenschaften im Active Directory

4.2.4 Überprüfen der lokalen Umgebung

Für die Einrichtung der Active-Directory-Synchronisierung muss Ihre lokale Umgebung einige Voraussetzungen erfüllen. Microsoft stellt für die Überprüfung der lokalen Umgebung ein Tool bereit, mit dem Sie ohne großen Aufwand Ihre lokale Umgebung schon vor Konfigurationsänderungen auf mögliche Problemstellen hin untersuchen können. So erhalten Sie rechtzeitig Hinweise, was Sie zunächst noch ändern sollten, bevor Sie mit der eigentlichen Konfiguration beginnen.

IdFix DirSync Error Remediation Tool

Speziell für das Überprüfen des Active Directorys und der darin enthaltenen Objekte bietet sich das *IdFix DirSync Error Remediation Tool* an. Es zeigt Ihnen Objekte, die bei der Synchronisierung Probleme verursachen würden und schlägt auch entsprechende Abhilfe vor (siehe Abbildung 4.14).

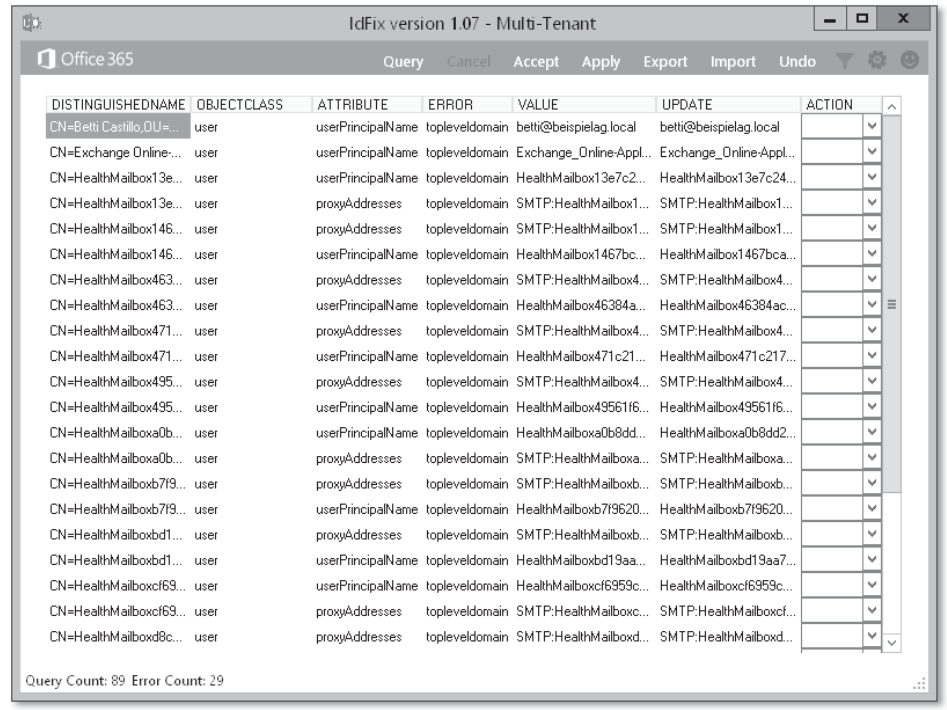

Abbildung 4.14 IdFix hat Probleme erkannt.

Zur Ausführung von IdFix müssen folgende Voraussetzungen erfüllt sein:

- Betriebssystem: ab Windows 7 bzw. ab Windows Server 2008 R2
- .NET Framework 4

IdFix können Sie hier herunterladen:

http://www.microsoft.com/en-us/download/details.aspx?id=36832

4.2.5 Installation

Bevor Sie mit der Installation des Verzeichnissynchronisierungstools loslegen, müssen Sie sich über die Voraussetzungen im Klaren sein.

Voraussetzungen

AADSync muss auf einem Server installiert werden, der folgende Voraussetzungen erfüllt:

- Hardware
  Tabelle 4.4 gibt Ihnen Hilfestellung bei der Auswahl geeigneter Hardware. Der Einsatz einer entsprechenden virtuellen Maschine ist auch möglich.

Anzahl Active-Directory-Objekte	CPU	RAM	Freie Festplatten-kapazität
< 10.000	1,6 GHz	4 GB	70 GB
10.000–50.000	1,6 GHz	4 GB	70 GB
50.000–100.000	1,6 GHz	16 GB	100 GB
100.000–300.000	1,6 GHz	32 GB	300 GB
300.000–600.000	1,6 GHz	32 GB	450 GB
> 600.000	1,6 GHz	32 GB	500 GB

Tabelle 4.4 Hardwarevoraussetzungen

- Windows-Version
  Das Verzeichnissynchronisierungstool ist eine 64-Bit-Anwendung und setzt entsprechend einen 64-Bit-Windows-Server (ab Windows Server 2008 SP1) voraus. Die Installation auf einem Domänencontroller ist möglich, aber nicht für Produktivumgebungen empfohlen. Das Verzeichnissynchronisierungstool installiert im Standardfall einen SQL Server Express LocalDB mit und erzeugt während der Synchronisierung einiges an Last, die auf einem Domänencontroller stören könnte.
- .NET Framework 4.5
  Vor der Installation des Verzeichnissynchronisierungstools muss das .NET Framework in der Version 4.5 installiert sein. Führen Sie die Installation gegebenenfalls mit dem Server Manager aus, oder laden Sie die Installationspakete hier herunter:
  http://www.microsoft.com/de-de/download/details.aspx?id=40773
- PowerShell ab 3
  Vor der Installation des Verzeichnissynchronisierungstools muss die PowerShell ab Version 3 installiert sein (beim Windows Server 2012 ist Version 3 bereits standardmäßig vorhanden, bei Windows Server 2012 R2 sogar Version 4). Die Installationspakete finden Sie hier:
  - PowerShell 3 (Windows Server 2008): *http://www.microsoft.com/en-us/download/details.aspx?id=34595*
  - PowerShell 4 (Windows Server 2008 R2): *http://www.microsoft.com/de-de/download/details.aspx?id=40855*
- Firewall
  Das Verzeichnissynchronisierungstool kommuniziert in der ausgehenden Richtung mit Office 365 über HTTPS 443/TCP. Die Firewall muss dies zulassen.

In jedem Forest der Active-Directory-Umgebung benötigen Sie für AADSync ein Dienstbenutzerkonto. Dieses benötigt für die Pushsynchronisierung keine speziellen Berechtigungen, ein normaler Domänenbenutzer ist ausreichend. Soll allerdings die Kennwortsynchronisierung zum Einsatz kommen, benötigt das Benutzerkonto besondere Berechtigungen. Welche das sind und wie diese gesetzt werden, lesen Sie im nächsten Abschnitt.

Es gibt übrigens keine Hochverfügbarkeitskonfiguration von AADSync. Sie installieren das Tool genau einmal, egal, wie viele Domänen und Active-Directory-Forests vorhanden sind.

Verwenden Sie bereits DirSync und wollen zu AADSync wechseln, deinstallieren Sie vor der Installation von AADSync DirSync. [«]

Berechtigungen für die Kennwortsynchronisierung

Wollen Sie die Kennwortsynchronisierung einsetzten, muss das Benutzerkonto, mit dem AADSync auf den Active-Directory-Forest zugreift, einige zusätzliche Berechtigungen erhalten:

1. Öffnen Sie die Verwaltungskonsole ADSI-Editor.
2. Stellen Sie bei Bedarf eine Verbindung zum standardmäßigen Namenskontext her (Aktion • Verbindung herstellen).
3. Öffnen Sie über das Kontextmenü die Eigenschaften der Root-Domäne, beispielsweise von DC=beispielag, DC=local (siehe Abbildung 4.15).

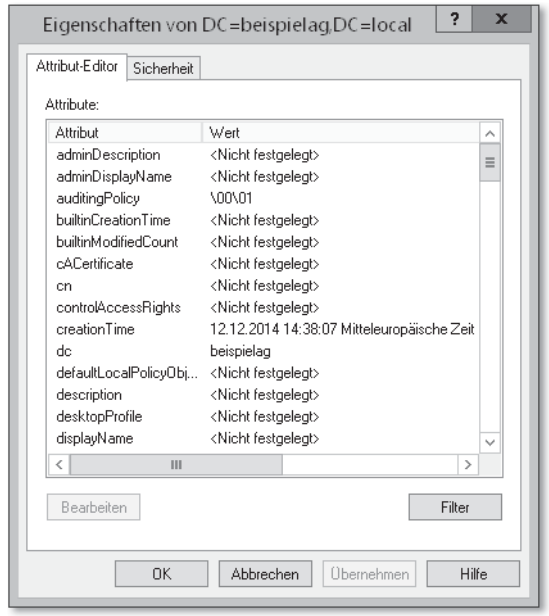

Abbildung 4.15 Domäneneigenschaften

4. Wechseln Sie zur Registerkarte Sicherheit (siehe Abbildung 4.16).

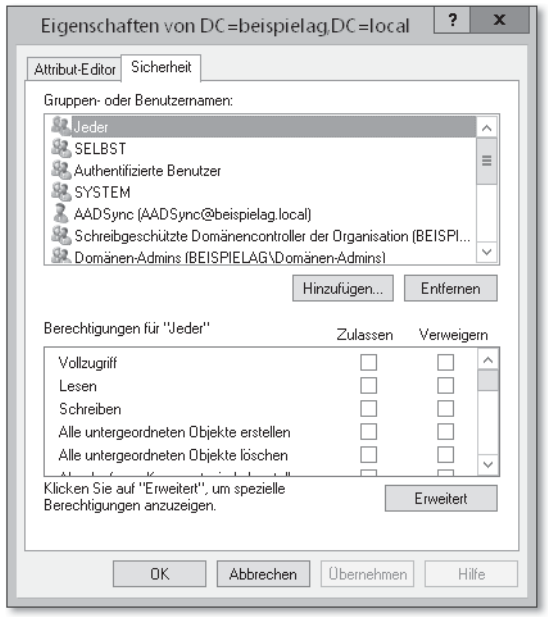

Abbildung 4.16 Sicherheitseinstellungen

5. Fügen Sie zur oberen Liste das Benutzerkonto für AADSync hinzu und geben ihm dann zusätzlich die folgenden Berechtigungen:
   - Alle Verzeichnisänderungen replizieren
   - Verzeichnisänderungen replizieren

Sollten Sie eine Exchange-Hybridbereitstellung einrichten wollen (siehe Abschnitt 6.13) sind zusätzlich noch weitere Rechte für das AADSync-Benutzerkonto zum Schreiben bestimmter Active-Directory-Attribute erforderlich. Erteilen Sie in diesem Fall folgende Berechtigungen:

1. Klicken Sie auf die Schaltfläche ERWEITERT (siehe Abbildung 4.17).
2. Klicken Sie auf die Schaltfläche HINZUFÜGEN (siehe Abbildung 4.18).
3. Klicken Sie auf PRINZIPAL AUSWÄHLEN und geben dann das Benutzerkonto für AADSync an.
4. Wählen Sie unter ANWENDEN AUF die Option UNTERGEORDNETE "BENUTZER"-OBJEKTE und erteilen die folgenden Berechtigungen:
   - `msExchArchiveStatus` schreiben
   - `msExchBlockedSendersHash` schreiben
   - `msExchSafeRecipientsHash` schreiben
   - `msExchSafeSendersHash` schreiben
   - `msExchUCVoiceMailSettings` schreiben

   - `msExchUserHoldPolicies` schreiben
   - `proxyAddresses` schreiben

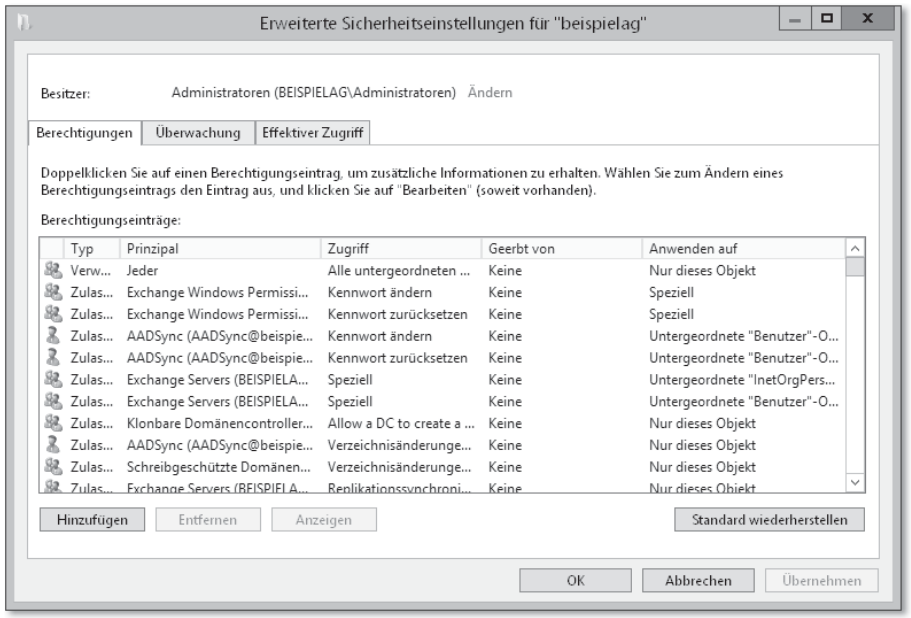

Abbildung 4.17 Erweiterte Einstellungen

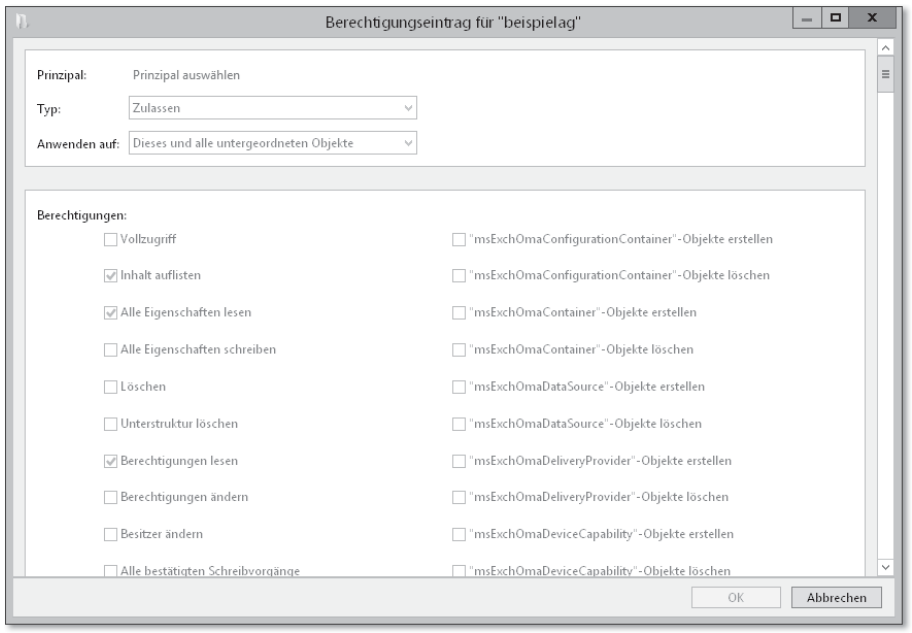

Abbildung 4.18 Hinzufügen

5. Wiederholen Sie den Schritt für Untergeordnete "InetOrgPerson"-Objekte:
   - `msExchArchiveStatus` schreiben
   - `msExchBlockedSendersHash` schreiben
   - `msExchSafeRecipientsHash` schreiben
   - `msExchSafeSendersHash` schreiben
   - `msExchUCVoiceMailSettings` schreiben
   - `msExchUserHoldPolicies` schreiben
   - `proxyAddresses` schreiben
6. Wiederholen Sie den Schritt für Untergeordnete "Kontakt"-Objekte:
   `proxyAddresses` schreiben
7. Wiederholen Sie den Schritt für Untergeordnete "Gruppe"-Objekte:
   `proxyAddresses` schreiben

Wie Sie bei der Konfiguration noch sehen werden, können Sie die Option *Kennwort zurückschreiben* aktivieren. Dabei werden Kennwortänderungen in AAD in das lokale Active Directory übertragen. Dabei handelt es nicht um die schon angesprochene Kennwortsynchronisierung, denn es geht um die umgedrehte Richtung ausgehend vom AAD. Um diese Funktion nutzen zu können, benötigen Sie AAD Premium (was außerhalb von Office 365 eingekauft werden muss). Sollten Sie diese Option nutzen wollen, sind noch weitere Konfigurationsschritte erforderlich:

1. Ausgehend von Abbildung 4.16 klicken Sie auf die Schaltfläche Erweitert.
2. Klicken Sie auf die Schaltfläche Hinzufügen.
3. Klicken Sie auf Prinzipal auswählen und geben dann das Benutzerkonto für AADSync an.
4. Wählen Sie unter Anwenden auf die Option Untergeordnete "Benutzer"-Objekte.
5. Aktivieren Sie zusätzlich die folgenden Optionen:
   - Kennwort ändern
   - Kennwort zurücksetzen

Aktivieren der Active-Directory-Synchronisierung

Standardmäßig ist die Active-Directory-Synchronisierung im Office 365-Mandanten deaktiviert. Sie müssen sie aktivieren, bevor Sie AADSync installieren und konfigurieren. Dafür gibt es zwei Möglichkeiten: das Office 365 Admin Center und die PowerShell.

Im Office 365 Admin Center wechseln Sie im Bereich Benutzer zum Abschnitt Aktive Benutzer. Klicken Sie dann auf Active Directory-Synchronisierung einrichten (siehe Abbildung 4.19).

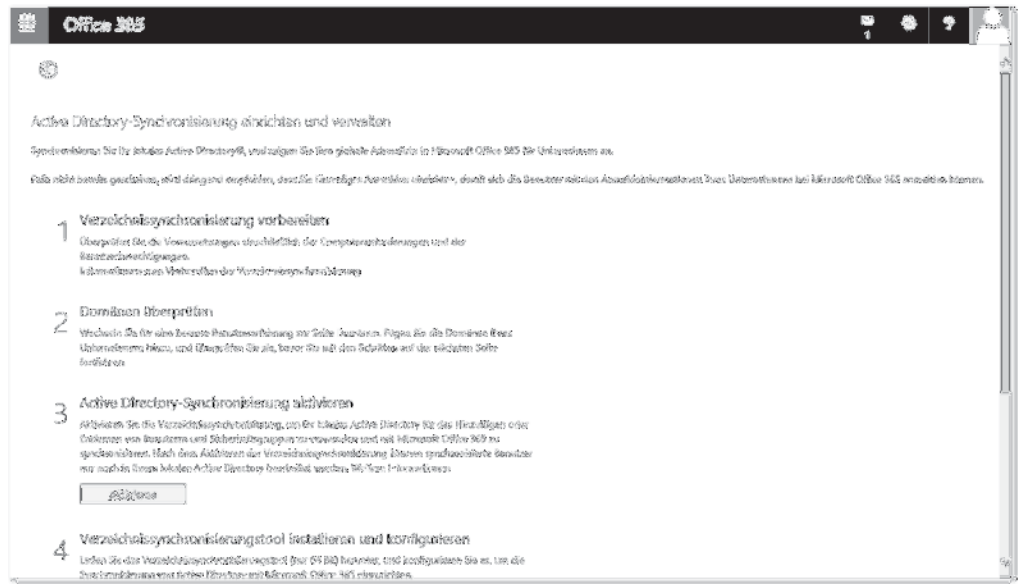

Abbildung 4.19 Einrichtung der Active-Directory-Synchronisierung

Dort klicken Sie auf die Schaltfläche Aktivieren. Die direkte URL lautet: *https://portal.office.com/default.aspx#@/DirSync/DirectorySynchronization.aspx*

Über die PowerShell erledigen Sie mithilfe des Cmdlets `Set-MsolDirSyncEnabled` diesen Schritt. Melden Sie sich zunächst in der PowerShell an Ihrem Office 365-Mandanten an (siehe Abschnitt 3.16.1, »Azure Active Directory-Modul für Windows PowerShell«), und geben Sie dann folgenden Befehl:

```
Set-MsolDirSyncEnabled -EnableDirSync $true
```

Listing 4.4 Aktivierung der Active-Directory-Synchronisierung

An denselben Stellen bzw. mit demselben Cmdlet können Sie die Synchronisierung auch wieder deaktivieren. Bei einer guten Planung im Vorfeld der Aktivierung sollte dies aber nicht nötig sein und kann zu unerwünschten Nebeneffekten führen. Beispiel: Sie setzen bisher die Synchronisierung ein, deaktivieren Sie dann aber. Dadurch bleiben die Benutzerkonten im Office 365-Verzeichnisdienst erhalten. Nach der Deaktivierung nehmen Sie Änderungen sowohl an den lokalen Benutzerkonten als auch an den Office 365-Benutzerkonten vor. Anschließend aktivieren Sie die Synchronisierung wieder. Da die Zuordnung der Objekte erhalten geblieben ist, werden die Office 365-Benutzerkonten mit den Angaben aus den Active-Directory-Benutzerkonten überschrieben. Die Änderungen an den Office 365-Benutzerkonten gehen verloren. [«]

Installation und Konfiguration

Das aktuelle Installationspaket von AADSync finden Sie unter folgender URL:

http://aka.ms/aadsync

[»] Im Office 365 Admin Center finden Sie auf derselben Seite, auf der Sie auch die Active-Directory-Synchronisierung aktivieren können, derzeit noch das alte Verzeichnissynchronisierungstool DirSync. Es ist zu erwarten, dass Microsoft dort zukünftig AADSync zum Download anbietet.

Führen Sie die dort heruntergeladene Datei aus. Danach startet automatisch der Konfigurationsassistent (siehe Abbildung 4.20).

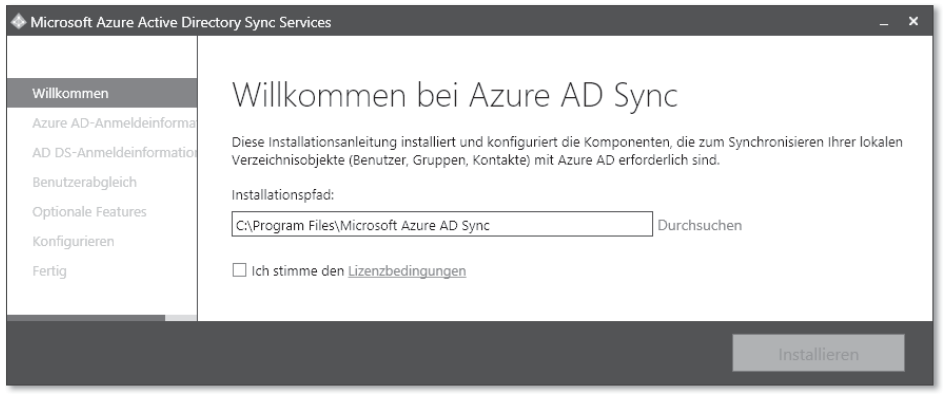

Abbildung 4.20 AADSync-Konfigurationsassistent

Möchten Sie statt des mitgelieferten SQL Server Express LocalDB eine der größeren SQL Server (ab 2008) einsetzen, brechen Sie den Konfigurationsassistenten ab und führen die Installation manuell über die Kommandozeile durch. Anschließend starten Sie den Konfigurationsassistenten über das Symbol auf dem Desktop wieder. Hier ein Beispiel:

```
DirectorySyncTool.exe /sqlserver SERVERNAME
   /sqlserverinstance INSTANZNAME
   /serviceAccountDomain DOMÄNE
   /serviceAccountName DIENSTBENUTZERNAME
   /serviceAccountPassword DIENSTBENUTZERKONTO
```

Listing 4.5 AADSync-Installation mit eigenem SQL-Server

Danach geht es mit folgenden Schritten weiter:

1. Akzeptieren Sie gegebenenfalls die Lizenzbedingungen.
2. Im Schritt AZURE AD-ANMELDEINFORMATIONEN geben Sie einen Office 365-Benutzer an, mit dem AADSync auf Ihren Mandanten zugreifen soll (siehe Abbildung 4.21).

Sie sollten hier kein Benutzerkonto angeben, das einem Anwender zugeordnet ist. [«] Erstellen Sie lieber ein zusätzliches Konto, und weisen Sie ihm die Rolle »Globaler Administrator« zu. Eine Lizenz benötigt das neue Konto nicht, sodass auch keine Kosten verursacht werden. Denken Sie in Zukunft aber daran, das Kennwort, wenn es sich einmal ändern sollte, auch hier im Konfigurationstool zu aktualisieren. Dieser Umstand ist besonders problematisch, wenn das Kennwort nach einer gewissen Zeitspanne abläuft. Denn dann kann auch die Synchronisierung nicht mehr durchgeführt werden. Wie Sie das Ablaufen des Kennworts verhindern können, lesen Sie in Abschnitt 3.16.3, »Benutzer anlegen«.

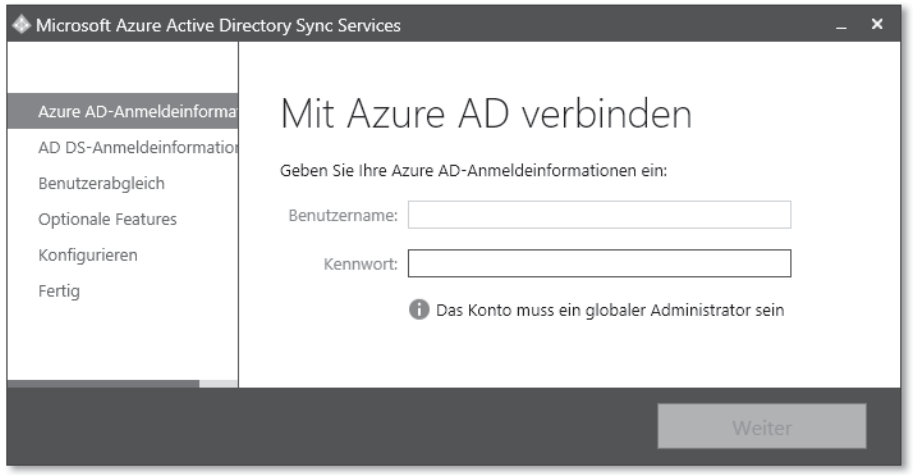

Abbildung 4.21 Azure AD-Anmeldeinformationen

3. Im Schritt AD DS-ANMELDEINFORMATIONEN geben Sie den Benutzer an, unter dem AADSync auf Ihr lokales Active Directory zugreifen soll (siehe Abbildung 4.22).

Abbildung 4.22 AD DS-Anmeldeinformationen

Diesen Vorgang können Sie bei Bedarf für weitere Active-Directory-Forests wiederholen.

4. Im Schritt Benutzerabgleich sind zwei Angaben erforderlich (siehe Abbildung 4.23).

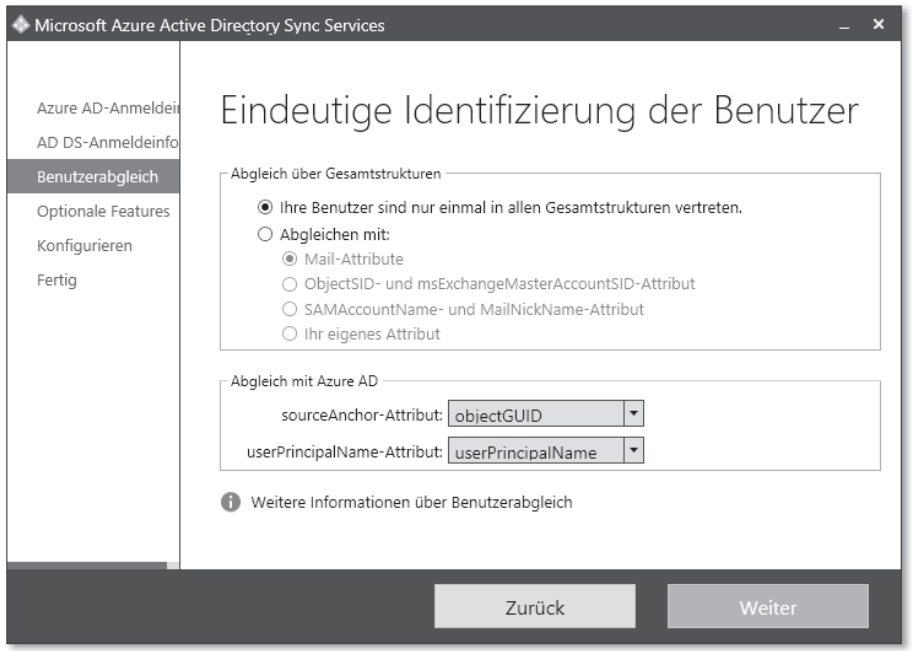

Abbildung 4.23 Benutzerabgleich

- Abgleich über Gesamtstrukturen: Wählen Sie aus, wie Benutzer aus den Active-Directory-Forests in Office 365 repräsentiert werden sollen. Tabelle 4.5 erläutert die Optionen.
- Abgleich mit Azure AD: Wählen Sie unter sourceAnchor-Attribut ein Attribut, dessen Wert sich während der gesamten Lebenszeit des Objekts nicht ändert. Die vorausgewählte `objectGUID` ist potenziell eine gute Wahl – dabei wird davon ausgegangen, dass die Benutzerkonten in Zukunft nicht in einen anderen Forest verschoben werden. Unter userPrincipalName-Attribut geben Sie ein Attribut an, mit dessen Wert sich die Benutzer an Office 365 anmelden sollen. Typischerweise mit dem Attribut `userPrincipalName`.

  Soll dieses Attribut hier aber nicht zum Einsatz kommen, beispielsweise weil es für Office 365 ungeeignet gesetzt ist, können Sie ein anderes wählen, wie `mail`. Beachten Sie dabei aber auch Abschnitt 4.3.9, »Alternative Benutzernamen mit AD FS«.

Einstellung	Bedeutung
Ihre Benutzer sind nur einmal in allen Gesamtstrukturen vertreten	Alle Benutzerkonten werden als separate Benutzer in Office 365 angelegt. Eine Zusammenlegung von Benutzerkonten aus unterschiedlichen Active-Directory-Forests findet nicht statt. Dies ist auch für Umgebungen mit einem einzelnen Active-Directory-Forest die richtige Wahl. Bei mehreren Forests darf keine Synchronisation der GAL (*Global Adress List* = globale Adressliste) zwischen mehreren Exchange-Organisationen konfiguriert sein.
Mail-attribut	Alle Benutzerkonten der lokalen Active-Directory-Forests mit demselben Wert im Attribut `mail` werden in Office 365 als einzelner Benutzer angelegt. Dies ist beispielsweise in einer Umgebung mit zwei Active-Directory-Forests mit jeweils einer separaten Exchange-Organisation gegeben. Zwischen den beiden Forests ist eine Zwei-Wege-Vertrauensstellung eingerichtet. Dort werden meist mithilfe der Synchronisation der GAL in einem Forest vorhandene Benutzerkoten im anderen Forest als Kontakte angelegt. Über das Attribut `mail` kann eine Zuordnung vorgenommen werden, und die Benutzer werden im AAD als einzelne Benutzer ohne den jeweils zugehörigen Kontakt angelegt.
ObjectSID- und msExchangeMasterAccountSID-Attribut	Diese Option ist für Umgebungen gedacht, in denen es einen oder mehrere Active-Directory-Forests für Benutzerkonten und einen separaten Forest für Ressourcen gibt. Der Ressourcen-Forest vertraut dabei den Benutzerkonten-Forest. Mit dieser Option wird für ein aktiviertes Benutzerkonto aus einem Benutzerkonten-Forest mit einem deaktivierten Benutzerkonto aus einem Resource-Forest zusammengelegt (Stichwort *Linked Mailbox* bei einer lokalen Exchange-Umgebung).
SAMAccountName- und MailNickName attribute	Benutzerkonten mit entsprechenden Werten aus unterschiedlichen Active-Directory-Forests werden in Office 365 als einzelne Benutzerkonten angelegt.

Tabelle 4.5 Benutzerabgleich-Optionen

Einstellung	Bedeutung
Ihr eigenes Attribut	Auswahl eines eigenen Attributs zur Zusammenlegung von Benutzerkonten aus unterschiedlichen Active-Directory-Forests

Tabelle 4.5 Benutzerabgleich-Optionen (Forts.)

5. Im Schritt Optionale Features aktivieren Sie die Unterstützung bestimmter Dienste (siehe Abbildung 4.24):

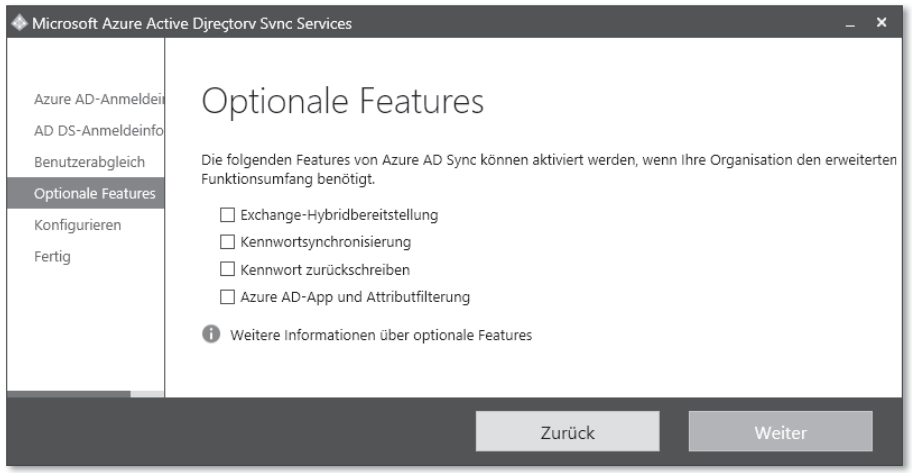

Abbildung 4.24 Optionale Features

- Exchange-Hybridbereitstellung: Diese Option muss aktiv sein, wenn Sie eine Exchange-Hybridbereitstellung einrichten wollen (siehe Abschnitt 6.13).
- Kennwortsynchronisierung: Setzen Sie diese Option, um die Kennwortsynchronisierung von lokalen Benutzern zu den zugehörigen AAD-Benutzern zu aktivieren.
- Kennwort zurückschreiben: Mit dieser Option werden Kennwortänderungen in Office 365 in das lokale Active Directory übertragen. Achtung: Es handelt sich dabei nicht um die schon angesprochene Kennwortsynchronisierung, denn es geht um die umgedrehte Richtung ausgehend vom AAD. Um diese Funktion nutzen zu können, benötigen Sie AAD Premium (was außerhalb von Office 365 eingekauft werden muss).
- Azure AD-App und Attributfilterung: Aktivieren Sie diese Option, können Sie im nächsten Schritt bestimmte Anwendungen auswählen (siehe Abbildung 4.25). Nur die für die ausgewählten Anwendungen erforderlichen Active-Directory-Attribute werden dann von AADSync synchronisiert. Selbst die manuelle Auswahl von zu synchronisierenden Attributen ist möglich

(siehe Abbildung 4.26). Doch Achtung: Wählen Sie zu viele Attribute ab, besteht die Gefahr, dass manche Dienste nicht mehr richtig funktionieren.

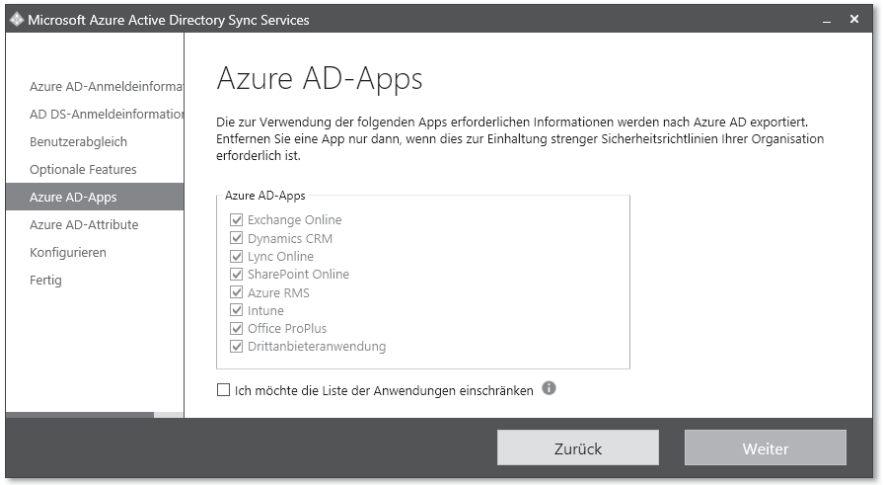

Abbildung 4.25 Azure AD-Apps

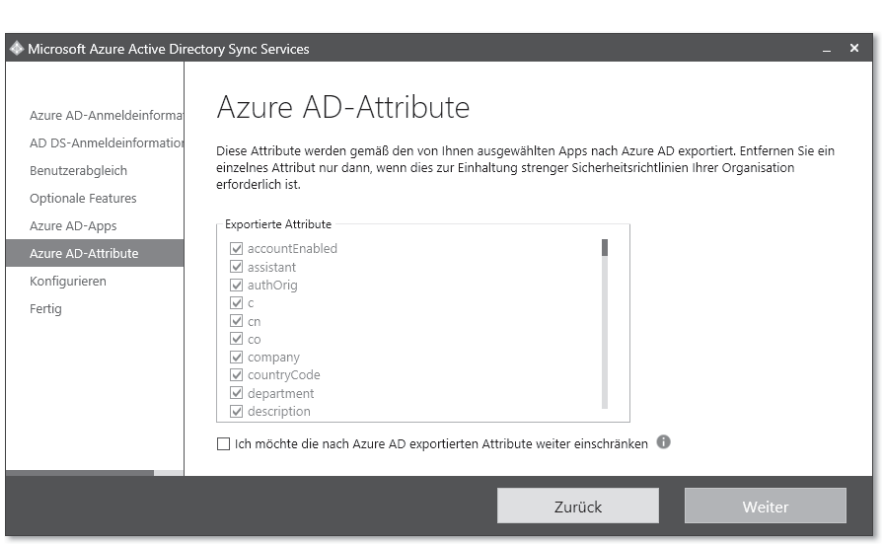

Abbildung 4.26 Azure AD-Attribute

6. Überprüfen Sie im Schritt Konfigurieren die ausgewählten Optionen, und lassen Sie anschließend die Konfiguration durchsetzen und gegebenenfalls die initiale Synchronisierung durchführen. Sollen allerdings nicht alle Benutzerkonten, Gruppen und Kontakte synchronisiert werden, müssen Sie vorher (!) einen Filter konfigurieren. Lesen Sie hierzu Abschnitt 4.2.6, »Filtern von Active-Directory-Objekten«.

Die Synchronisierung dauert pro 5.000 zu synchronisierender Objekte rund eine Stunde.

[»] Nach der Konfiguration sollten Sie sich ab- und dann neu anmelden.

Nach der Installation

Nach Abschluss der Installation finden Sie verschiedene Komponenten von AADSync auf dem Server:

- Anwendung *DirectorySyncTool* (auf dem Desktop)

  Das Symbol führt zum Konfigurationsassistenten, mit dem Sie Ihre lokale Active-Directory-Umgebung mit dem Azure Active Directory koppeln.

- Anwendung *Synchronization Service* (auf der Startseite bzw. im Startmenü)

  AADSync basiert auf dem FIM. Das Symbol führt Sie zur FIM-Verwaltungskonsole, dem *MIISClient*.

- Anwendung *Synchronization Rules Editor* (auf der Startseite bzw. im Startmenü)

  Mit dem Synchronization Rules Editor haben Sie – wie der Name schon sagt – Zugriff auf die von AADSync angewandten Synchronisierungsregeln (siehe Abbildung 4.27).

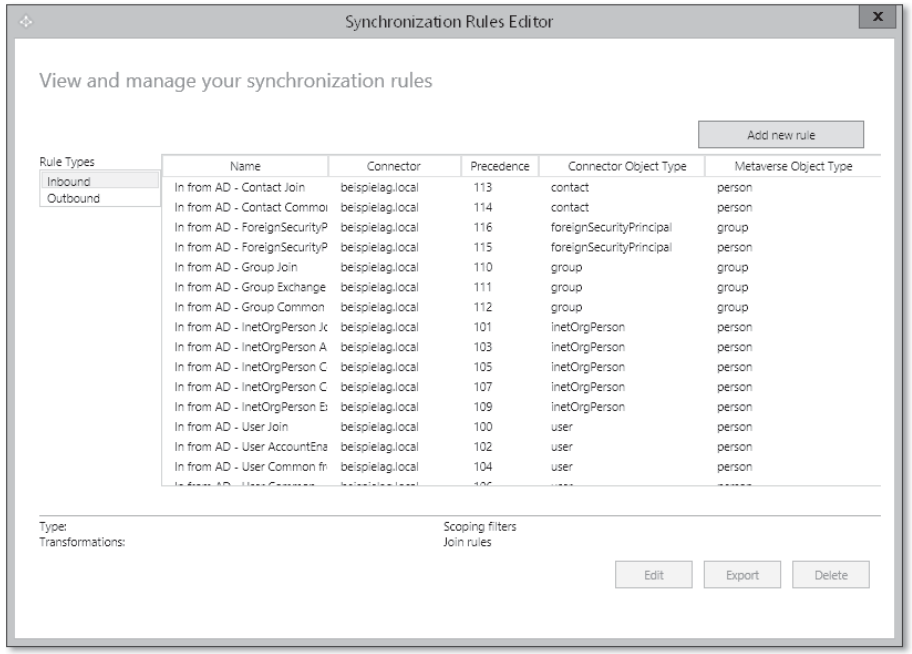

Abbildung 4.27 Synchronization Rules Editor

Abhängig vom lokalen Active-Directory-Schema und von der Präsenz einer Exchange- oder Lync-Umgebung sind hier unterschiedliche Regeln angelegt. Bei den

Outbound Rules finden Sie nur solche, die für ausgewählte Office 365-Dienste von Bedeutung sind.

Mit diesem Tool könnten Sie an dem Regelwerk auch Änderungen vornehmen. Die ist beispielsweise erforderlich, wenn Sie bestimmte lokale Objekte nicht mit dem AAD synchronisieren lassen wollen (siehe Abschnitt 4.2.6, »Filtern von Active-Directory-Objekten«).

- Anwendung *Synchronization Service Key Management* (auf der Startseite bzw. im Startmenü)

  Das Tool ermöglicht es Ihnen, die Schlüssel zu verwalten, mit denen AADSync sensible Daten verschlüsselt, beispielsweise die Zugangsdaten. Wollten Sie die Synchronisationsdatenbank von AADSync sichern und AADSync selbst auf einem anderen Server wiederherstellen, ist das nur möglich, wenn Sie über die Schlüssel verfügen.

  Ein Backup der Datenbank macht nur Sinn, wenn Sie sehr viele Objekte synchronisieren. Richten Sie AADSync beispielsweise nach einem SQL-Serverausfall neu ein, wird ohne Datenbankbackup mit einer vollständigen Synchronisierung begonnen, die pro 5.000 zu synchronisierender Objekte wieder rund eine Stunde in Anspruch nimmt. [«]

- Windows-Dienst *Microsoft Azure AD Sync*

  Dieser Dienst ist für die eigentliche Synchronisierung zuständig und läuft unter dem bei der Installation angelegten Benutzer *AAD_<ID>*, wobei die ID und das Kennwort automatisch gewählt werden. Dieser Benutzer ist außerdem Mitglied der bei der Installation angelegten Gruppe *ADSyncAdmins*.

4.2.6 Filtern von Active-Directory-Objekten

Standardmäßig synchronisiert das Verzeichnissynchronisierungstool alle vorhandenen Benutzerkonten, E-Mail-aktivierte Gruppen, Sicherheitsgruppen und Kontakte. Der Konfigurationsassistent zur Einrichtung dieser Synchronisierung erlaubt dabei keine Auswahl, welche Objekte synchronisiert werden sollen und welche nicht. Es werden einfach grundsätzlich alle Objekte der beschriebenen Typen synchronisiert. Wie bereits erwähnt, wird die eigentliche Synchronisierung über FIM vorgenommen. Über dessen Verwaltungskonsole können Sie eine Filterung einrichten, mit der bestimmt wird, welche Objekte synchronisiert werden sollen.

Grundsätzlich werden dabei drei unterschiedliche Verfahren zur Filterkonfiguration unterstützt:

- Organisationseinheiten filtern
- Domänen filtern
- eigenschaftsbasierte Filterung

Organisationseinheiten filtern

Ein einfaches Vorgehen beim Ausschluss von Objekten aus der Synchronisierung ist die Abwahl von Organisationseinheiten, die bei weiteren Synchronisationsläufen nicht mehr berücksichtigt werden sollen.

[»] Achtung: Schließen Sie eine Organisationseinheit von der Synchronisierung aus, nachdem diese bereits früher einmal synchronisiert wurde, werden die darin enthaltenen Objekte aus dem Office 365-Verzeichnisdienst gelöscht. Das ist besonders bei Benutzerkonten problematisch.

Zur Konfiguration, welche Organisationseinheiten bei der Synchronisierung berücksichtigt werden sollen, gehen Sie wie folgt vor:

1. Melden Sie sich an dem Server an, auf dem das Verzeichnissynchronisierungstool ausgeführt wird. Verwenden Sie dabei ein Benutzerkonto, das Mitglied der lokalen Sicherheitsgruppe *ADSyncAdmins* ist, beispielsweise der lokale Benutzer, den Sie bei der Konfiguration der Verzeichnissynchronisierung angegeben haben.
2. Führen Sie die Anwendung *Synchronization Service* über die Startseite bzw. das Startmenü aus. Dabei handelt es sich um die Verwaltungskonsole des Forefront Identity Managers.
3. Wechseln Sie zum Bereich CONNECTORS (siehe Abbildung 4.28).

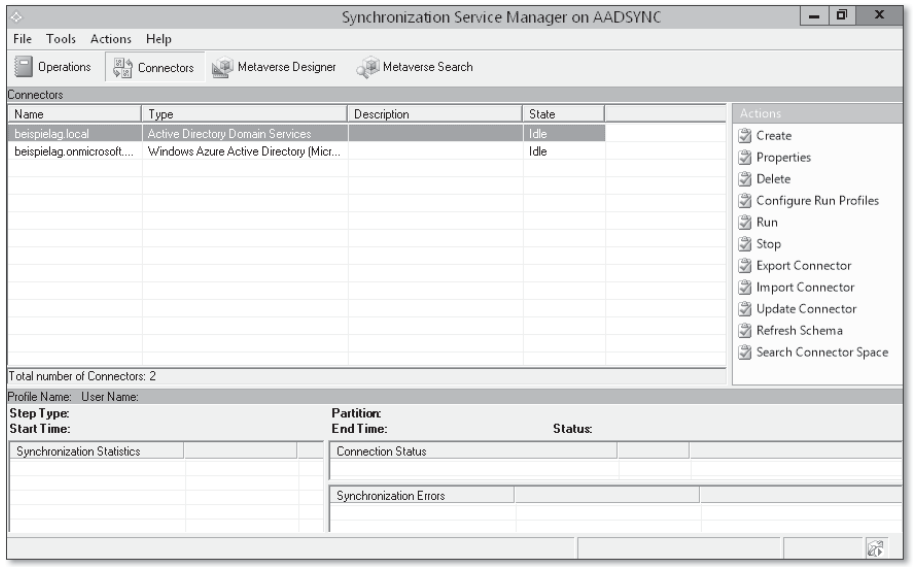

Abbildung 4.28 Synchronization Service

4. Klicken Sie doppelt auf die Zeile für Ihren lokalen Active-Directory-Forest.
5. Wählen Sie den Bereich CONFIGURE DIRECTORY PARTITIONS (siehe Abbildung 4.29). Markieren Sie dann gegebenenfalls unter SELECT DIRECTORY PARTITIONS

die Domäne, die die auszuschließende Organisationseinheit enthält, und klicken Sie dann auf die Schaltfläche CONTAINERS.

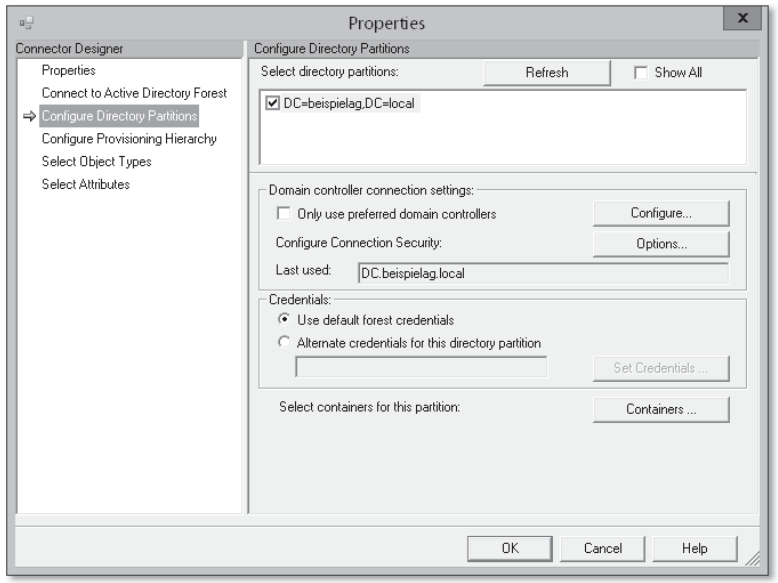

Abbildung 4.29 Partitionseigenschaften

6. Geben Sie die Benutzerdaten eines Domänenadministrators an.
7. Deaktivieren Sie alle Organisationseinheiten, deren Elemente während des Synchronisierungsvorgangs nicht berücksichtigt werden sollen (siehe Abbildung 4.30).

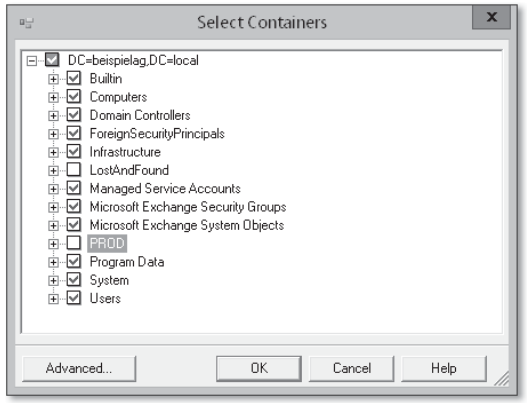

Abbildung 4.30 Containerauswahl

8. Schließen Sie alle Fenster mit OK.
9. Öffnen Sie das Kontextmenü der Zeile Ihres lokalen Active-Directory-Forests, und wählen Sie den Befehl RUN.

10. Markieren Sie das RUN PROFILE mit dem Namen FULL IMPORT, und klicken Sie auf OK.
11. Warten Sie, bis der STATE der Zeile Ihres lokalen Active-Directory-Forests auf IDLE steht.
12. Markieren Sie das RUN PROFILE mit dem Namen DELTA SYNCHRONIZATION, und klicken Sie auf OK.
13. Warten Sie, bis der STATE der Zeile Ihres lokalen Active-Directory-Forests auf IDLE steht.

Die Änderungen werden dann beim nächsten Synchronisierungsintervall berücksichtigt. Starten Sie gegebenenfalls wie in Abschnitt 4.2.7, »Manueller Start der Synchronisierung«, beschrieben direkt einen Synchronisierungsvorgang.

Benutzerkonten, die nun nicht mehr synchronisiert werden, markiert das Verzeichnissynchronisierungstool automatisch als gelöscht. Damit sind diese Konten und auch die Daten, beispielsweise das Postfach, aber noch nicht endgültig verloren. Innerhalb von 30 Tagen können Sie diese Konten wiederherstellen. Lesen Sie hierzu Abschnitt 2.5.4, »Gelöschte Benutzer wiederherstellen«.

Domänen filtern

Der Vorgang zur Filterung bestimmter Domänen ist sehr ähnlich wie bei der Filterung von Organisationseinheiten. Im Fenster von Abbildung 4.30 markieren Sie nur die Domäne (oberster Eintrag). Alle darin enthaltenen Container müssen abgewählt werden.

[»] Die Domäne selbst dürfen Sie nicht abwählen, sonst erhalten Sie den Fehler *missing-partition-for-run-setup*.

Eigenschaftsbasierte Filterung

Den Ausschluss von Objekten aus der Synchronisierung können Sie auch über eine eigenschaftsbasierte Filterung konfigurieren, um damit beispielsweise alle Benutzerkonten mit bestimmten Eigenschaften von der Synchronisierung auszuschließen. In einem Beispiel sollen alle Benutzer, deren Wohnort (Active-Directory-Attribut `City`) Berlin lautet, nicht synchronisiert werden. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich an dem Server an, auf dem das Verzeichnissynchronisierungstool ausgeführt wird. Verwenden Sie dabei ein Benutzerkonto, das Mitglied der lokalen Sicherheitsgruppe *ADSyncAdmins* ist, beispielsweise der lokale Benutzer, den Sie bei der Konfiguration der Verzeichnissynchronisierung angegeben haben.
2. Führen Sie die Anwendung *Synchronization Rules Editor Service* über die Startseite bzw. das Startmenü aus (siehe Abbildung 4.31).
3. Markieren Sie unter RULE TYPES den Eintrag INBOUND.
4. Klicken Sie auf ADD NEW RULE, um eine neue Regel anzulegen (siehe Abbildung 4.32).

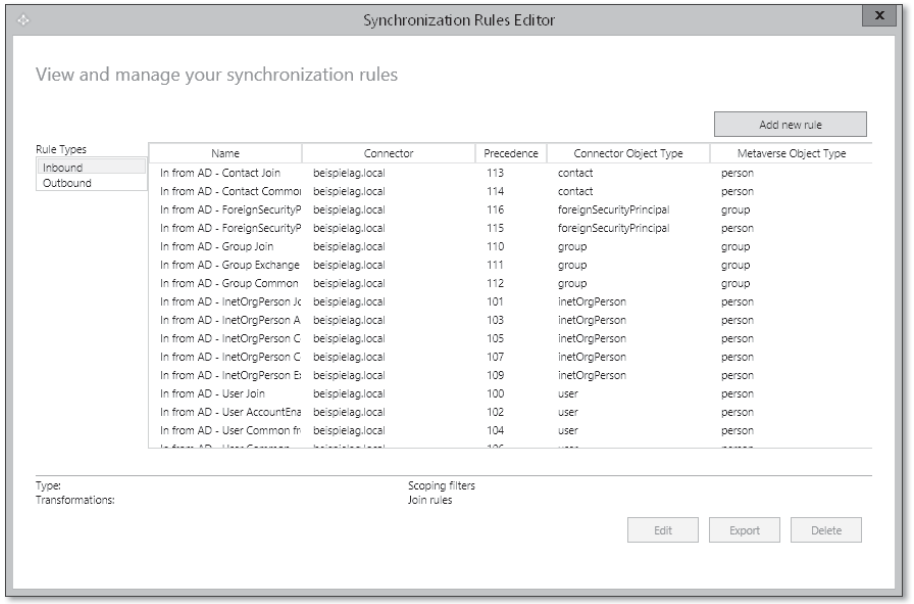

Abbildung 4.31 Synchronization Rules Editor

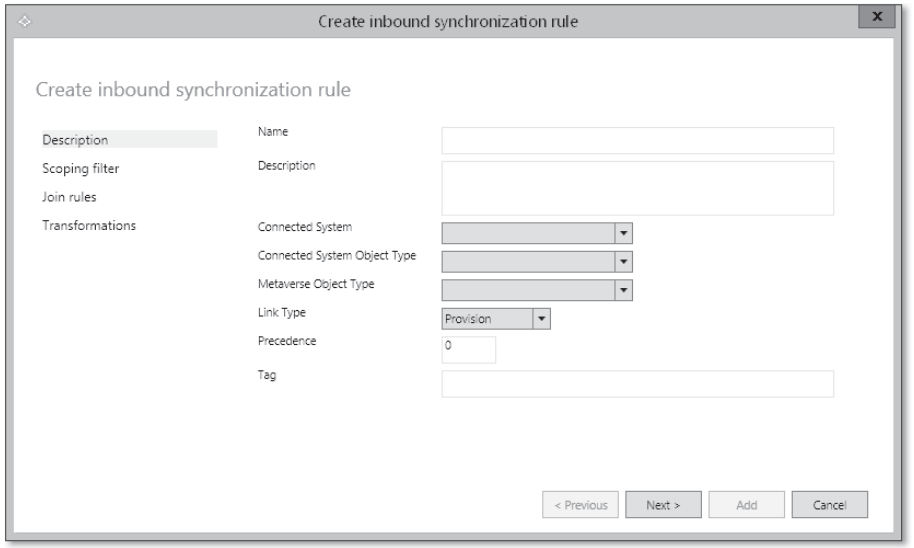

Abbildung 4.32 Anlegen einer neuen Regel

5. Legen Sie die Regel wie folgt an:
   - NAME: ein aussagekräftiger Name für die neue Regel
   - CONNECTED SYSTEM: der betroffene Active-Directory-Forest
   - CONNECTED SYSTEM OBJECT TYPE: USER (für Benutzerkonten)

- Metaverse Object Type: person
- Link Type: Join
- Precedence: Die Regeln werden in der Reihenfolge der Precedence ausgeführt. Wählen Sie einen Wert, der von anderen Regeln noch nicht belegt ist (beispielsweise 1.000).

6. Im nächsten Schritt Scoping filter (siehe Abbildung 4.33) legen Sie mit Add group eine neue Gruppe für eine Klausel an. Für unser Beispiel muss die Klausel wie folgt lauten:
   - `l EQUAL Berlin`
   - `l` steht dabei im Active-Directory-Schema für *Locality name*, also für den Wohnort.

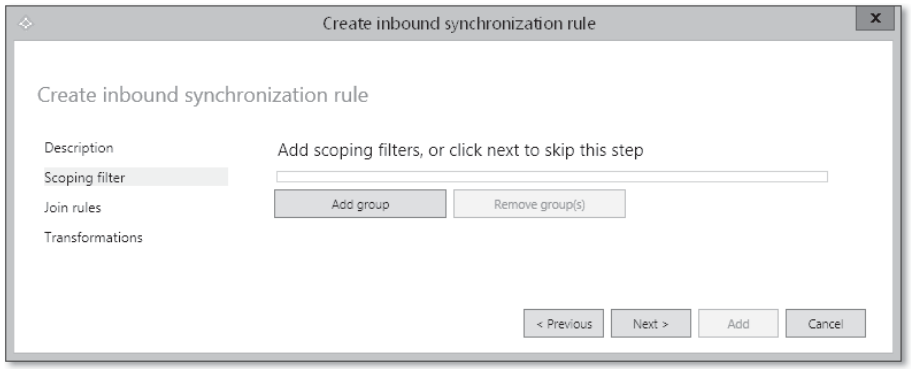

Abbildung 4.33 Filterkonfiguration

7. Den nächsten Schritt Join rule übergehen Sie.
8. Im Schritt Transformations (siehe Abbildung 4.34) machen Sie folgende Angaben:
   - FlowType: Constant
   - Target Attribute: cloudFiltered
   - Source: `True`
   - Apply Once: nicht ausgewählt
   - Merge Type: Update
9. Klicken Sie auf Add, um die Regel anzulegen.
10. Führen Sie die Anwendung *Synchronization Service* über die Startseite bzw. das Startmenü aus.
11. Wechseln Sie zum Bereich Connectors.
12. Öffnen Sie das Kontextmenü der Zeile Ihres lokalen Active-Directories-Forests, und wählen Sie den Befehl run.
13. Markieren Sie das Run profile mit dem Namen Full Synchronization, und klicken Sie auf OK.

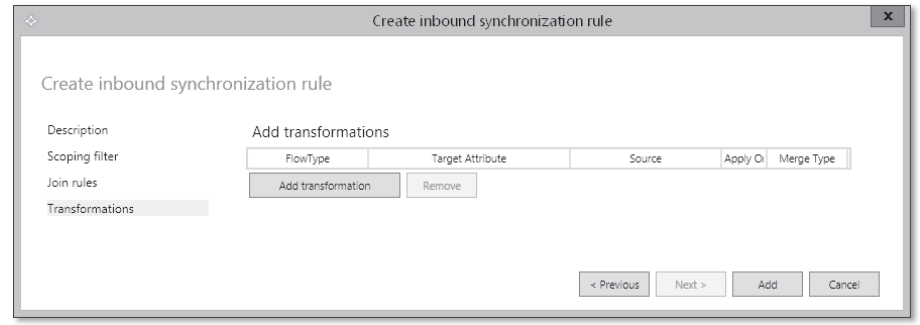

Abbildung 4.34 Transformationskonfiguration

14. Warten Sie, bis der State der Zeile Ihres lokalen Active-Directory-Forests auf Idle steht.

Mit dem nächsten Synchronisierungsintervall werden die Änderungen im AAD übernommen. Starten Sie gegebenenfalls wie in Abschnitt 4.2.7, »Manueller Start der Synchronisierung«, beschrieben direkt einen Synchronisierungsvorgang.

4.2.7 Manueller Start der Synchronisierung

Die regelmäßige Synchronisierung im Drei-Stunden-Intervall regelt bei AADSync eine Aufgabe in der Windows-Aufgabenverwaltung mit dem Namen Azure AD Sync Scheduler (siehe Abbildung 4.35).

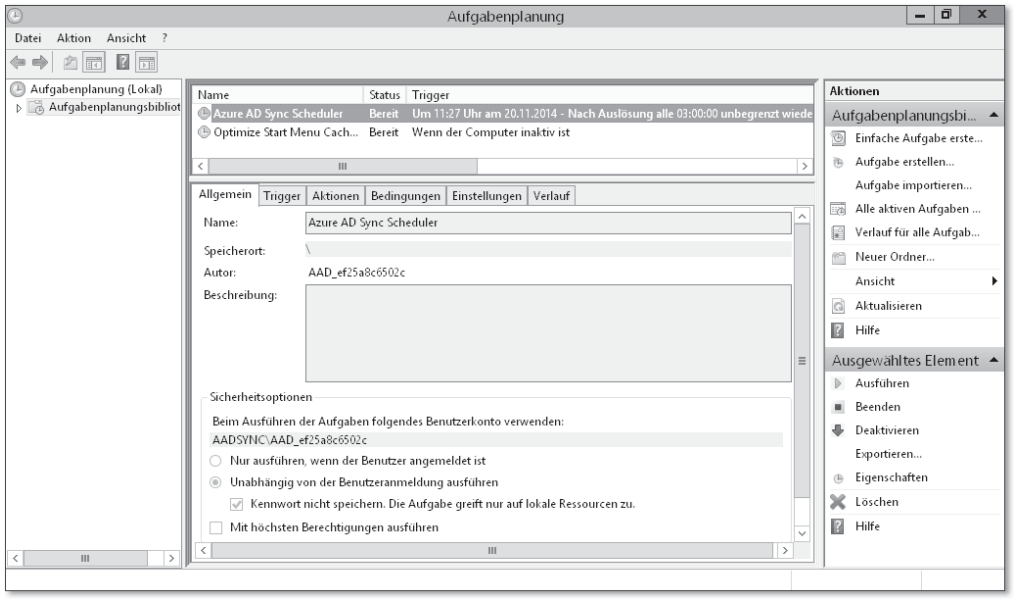

Abbildung 4.35 Aufgabe zum Start der Synchronisierung

Diese Aufgabe führt das Kommandozeilentool *DirectorySyncClientCmd.exe* aus dem Ordner *\Program Files\Microsoft Azure AD Sync\Bin* aus. Dieses Kommandozeilentool können Sie auch direkt ausführen, um die Synchronisierung manuell zu starten. In diesem Fall erhalten Sie in der Konsole auch einige Statusmeldungen (siehe Abbildung 4.36).

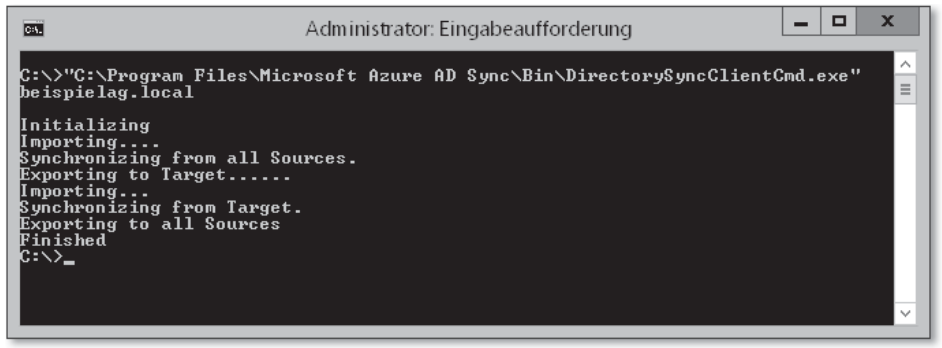

Abbildung 4.36 Statusmeldungen während der Synchronisierung

Haben Sie noch nie eine Synchronisierung durchgeführt, müssen Sie das Kommandozeilentool zusammen mit dem Parameter `initial` aufrufen.

Über die Windows-Ereignisanzeige können Sie den Verlauf der Synchronisierung verfolgen (siehe Abschnitt 4.2.9, »Fehlerbehandlung«).

4.2.8 Synchronisierung von Benutzerkonten

Bei der Synchronisierung von Benutzerkonten sind einige Besonderheiten zu beachten:

- Vergabe von *Net-IDs*
  Jedes über AADSync neu angelegte Benutzerkonto in Office 365 erhält eine Net-ID. Mit dieser wird die Zuordnung zum ursprünglichen lokalen Benutzerkonto erkannt. Außerdem spielt sie beim Anmeldevorgang eines Identitätsverbunds eine wichtige Rolle (siehe Abschnitt 4.3.4, »Anmeldevorgang«).
- bereits vorhandene Benutzerkonten in Office 365
  Sollten Sie vor der Aktivierung der Active-Directory-Synchronisierung bereits in Office 365 Benutzer anmpgelegt haben, versucht das Verzeichnissynchronisierungstool eine Zuordnung vorzunehmen. Als Grundlage verwendet das Tool dabei GUIDs und die primäre SMTP-Adresse, mit der ein Abgleich zwischen lokalen Active-Directory-Benutzerkonten und den im Office 365-Verzeichnisdienst vorhandenen Benutzerkonten erfolgt (siehe Abschnitt 4.2.1, »Synchronisierungsvorgang«).
- Deaktivieren von lokalen Benutzerkonten
  Deaktivieren Sie ein Benutzerkonto in Ihrem Active Directory, wird das zugehörige Office 365-Benutzerkonto ebenfalls deaktiviert. Der Anwender kann sich also nicht mehr an den Office 365-Diensten anmelden.

- Löschen von lokalen Benutzerkonten
  Löschen Sie ein Benutzerkonto in Ihrem Active Directory, wird das zugehörige Office 365-Benutzerkonto ebenfalls gelöscht.
- Lizenzierung
  Durch das automatische Anlegen von Office 365-Benutzerkonten durch die Active-Directory-Synchronisierung wird nicht auch automatisch eine Office 365-Lizenz vergeben. Bei der Lizenzierung der neuen Benutzerkonten handelt es sich um einen separaten Prozess, den Sie entweder über das Office 365 Admin Center oder über die PowerShell erledigen können.

Benutzerlizenzierung über das Office 365 Admin Center

Die Benutzerverwaltung im Office 365 Admin Center bietet einen speziellen Filter, mit dem Sie nicht lizenzierte Benutzerkonten anzeigen lassen können, um sie dann zu lizenzieren. Gehen Sie dazu wie folgt vor:

1. Öffnen Sie im Office 365 Admin Center den Bereich Benutzer und Gruppen.
2. Als Filter (Trichter-Symbol) wählen Sie Nicht lizenzierte Benutzer (siehe Abbildung 4.37).

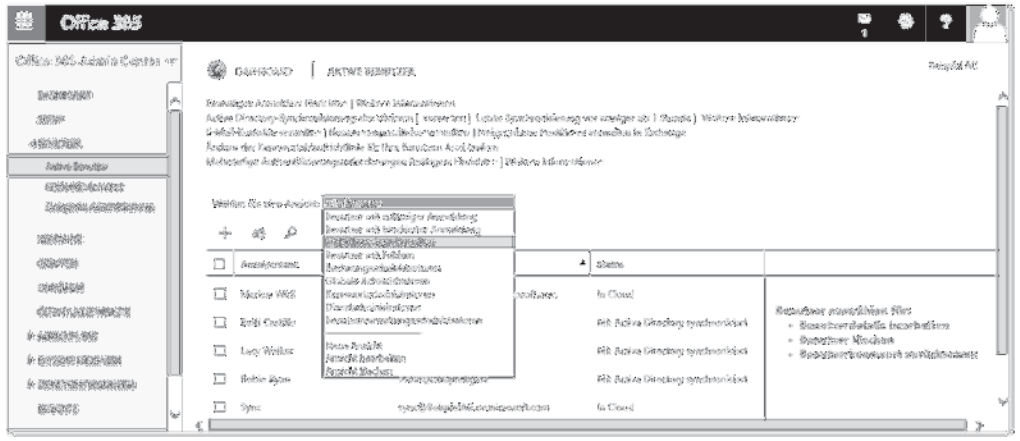

Abbildung 4.37 Filter für nicht lizenzierte Benutzer

3. Markieren Sie dann den oder die zu lizenzierenden Benutzer, und geben Sie den Befehl Synchronisierte Benutzer aktivieren.

Office 365 verlangt dann von Ihnen die Angabe des Benutzerstandorts sowie der gewünschten Lizenz (siehe Abbildung 4.38). Haben Sie keinen Domänenverbund konfiguriert, wird für die Benutzer automatisch ein Kennwort generiert. Bei einem Domänenverbund verbleibt die Kennwortverwaltung bei Ihrem lokalen Active Directory.

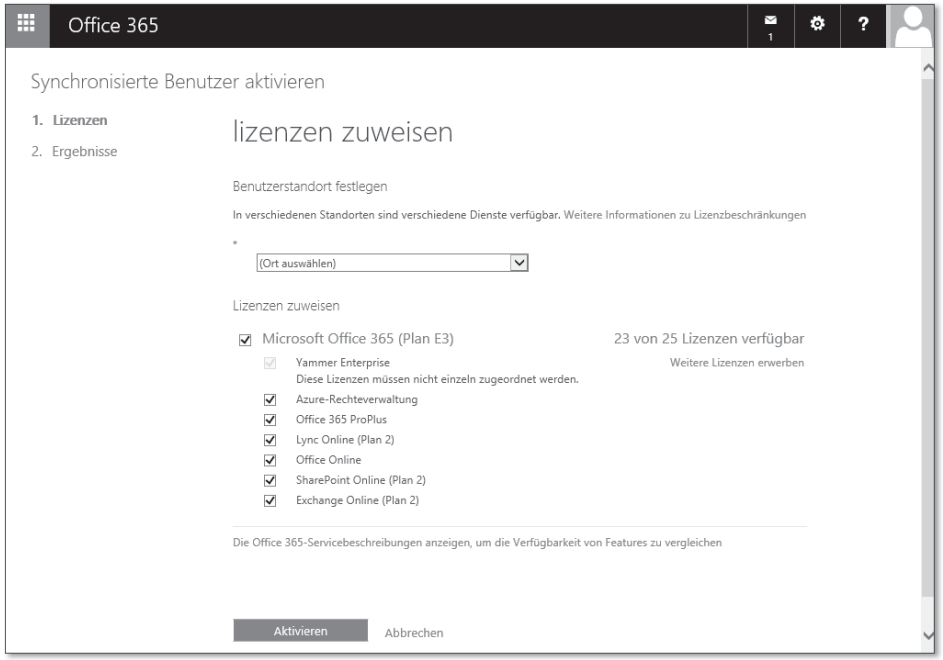

Abbildung 4.38 Synchronisierte Benutzer aktivieren

Benutzerlizenzierung über die PowerShell

In Abschnitt 3.16.1, »Azure Active Directory-Modul für Windows PowerShell«, habe ich bereits gezeigt, wie Sie mit der PowerShell eine Verbindung zu Ihrem Office 365-Mandanten herstellen. Nachdem Sie sich mit `Connect-MsolService` angemeldet haben, können Sie mit folgendem Kommando alle nicht lizenzierten Benutzer ausfindig machen:

```
Get-MsolUser -UnlicensedUsersOnly
```

Listing 4.6 Nicht lizenzierte Benutzer auflisten

Diese Benutzer können Sie nun beispielsweise mit einer E3-Lizenz versorgen, indem Sie die Objekte an ein `Set-MsolUser` weiterleiten, um den Standort anzugeben. Anschließend können Sie mit `Set-MsolUserLicense` eine Lizenz vergeben:

```
$benutzer = Get-MsolUser -UnlicensedUsersOnly
$benutzer |
   Set-MsolUser -UsageLocation "DE"
$benutzer |
   Set-MsolUserLicense -AddLicenses "BEISPIELAG:ENTERPRISEPACK"
```

Listing 4.7 Benutzer lizenzieren

Hierbei sollten Sie aber beachten, dass der Code sämtlichen nicht lizenzierten Benutzer eine Lizenz verpasst. Doch nicht alle Benutzer benötigen auch tatsächlich eine. Beispielsweise wird beim Anlegen eines Websitepostfachs (siehe Abschnitt 7.6, »Websitepostfächer«) automatisch auch ein Benutzer angelegt. Dieser benötigt aber keine Lizenz. Weitere Vorgehensweisen bei der Lizenzierung bespreche ich in Abschnitt 2.5.2, »Benutzer anlegen«.

4.2.9 Fehlerbehandlung

Haben Sie die Verzeichnissynchronisierung aktiviert, sollten Sie sie auch überwachen, um frühzeitig auf Probleme aufmerksam zu werden. Office 365 unterstützt Sie dabei mit Fehlermeldungen, die per E-Mail versandt werden, und AADSync mit Einträgen in der Windows-Ereignisanzeige.

Fehlermeldungen per E-Mail

Office 365 sendet bei Problemen automatisch eine E-Mail an den als technischen Ansprechpartner hinterlegten Kontakt Ihres Mandanten. So werden Sie frühzeitig darauf hingewiesen, dass die Synchronisierung nicht wie gewünscht durchgeführt werden konnte.

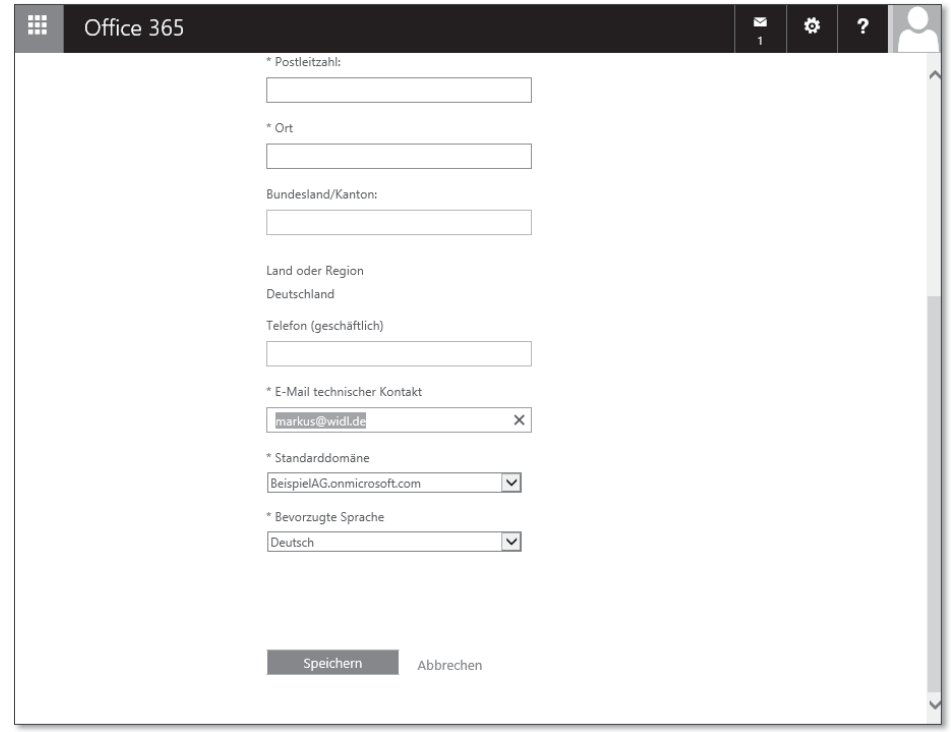

Abbildung 4.39 Anpassung des technischen Kontakts

Den technischen Kontakt können Sie anpassen, indem Sie im Office 365 Admin Center im Bereich DASHBOARD rechts oben auf Ihren Unternehmensnamen klicken (siehe Abbildung 4.39).

Es bietet sich an, als E-Mail-Adresse für den technischen Kontakt eine Verteilerliste anzugeben, die nicht nur eine einzelne Person enthält.

Statusinformationen in der Windows-Ereignisanzeige

Das Verzeichnissynchronisierungstool schreibt im *Ereignisprotokoll* »Anwendung« der Windows-Ereignisanzeige Statusinformationen über den Verlauf der Synchronisierung (siehe Abbildung 4.40).

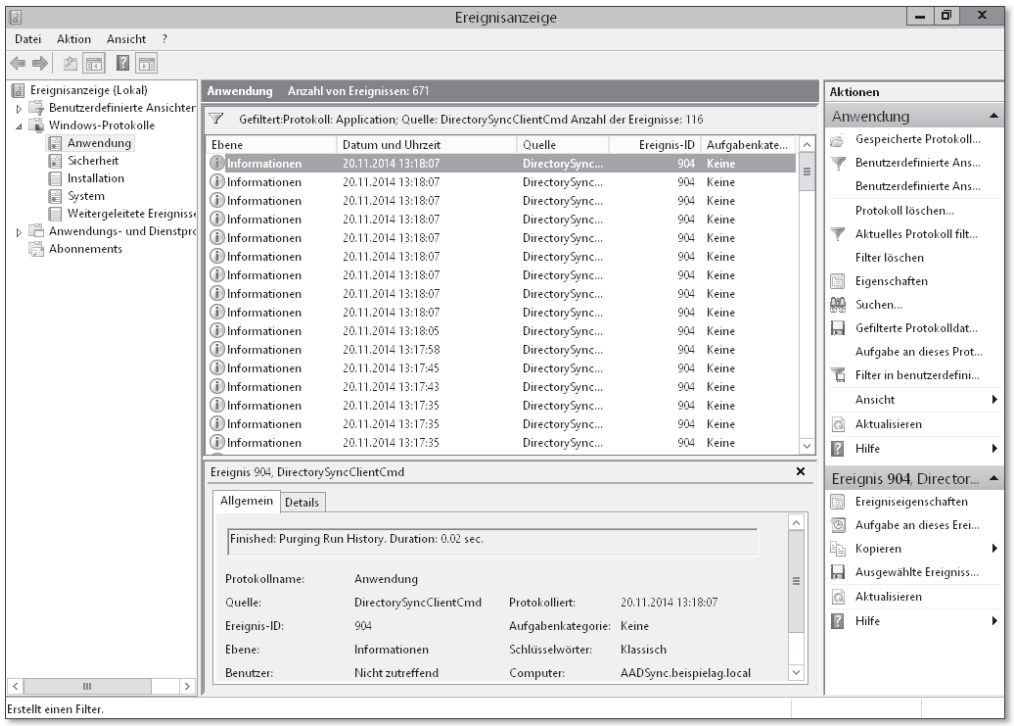

Abbildung 4.40 Windows-Ereignisanzeige

Die Einträge werden mit der Quelle *Directory Synchronization* angelegt. Tabelle 4.6 listet einige wichtige Ereignisse auf.

[»] Die Einträge enthalten manchmal die `ImmutableId`, mit der das betroffene Office 365-Benutzerkonto referenziert wird (siehe Abschnitt 4.2.1, »Synchronisierungsvorgang«). Die Ereignisanzeige können Sie auch wieder mit der PowerShell auswerten. Sehen wir uns einige Beispiele an.

Ereignis-ID	Bedeutung
3	Export wurde gestartet.
4	Export wurde abgeschlossen.
5	Anzahl exportierter Objekte
656	Kennwortänderung erkannt
657	Ergebnis der Kennwortsynchronisierung

Tabelle 4.6 Synchronisierungsereignisse

Zunächst sollen alle Ereignisse bezüglich der Synchronisierung aufgelistet werden:

```
Get-EventLog -LogName Application `
   -Source "Directory Synchronization"
```

Listing 4.8 Anzeige von Synchronisierungsereignissen

Wollen Sie die Ereignisse von einem anderen Computer aus aufrufen als von dem, auf dem das Synchronisierungstool läuft, hängen Sie den Computernamen an:

```
Get-EventLog -LogName Application `
   -Source "Directory Synchronization" `
   -ComputerName "AADSYNC"
```

Listing 4.9 Anzeige von Synchronisierungsereignissen auf einem bestimmten Computer

Möchten Sie nur die Fehler haben, filtern Sie die Objekte auf den Typ des Eintrags:

```
Get-EventLog -LogName Application `
   -Source "Directory Synchronization" `
   -EntryType Error
```

Listing 4.10 Anzeige von Synchronisierungsereignissen vom Typ Fehler

Und zu guter Letzt sollen nur die Fehler der vergangenen sieben Tage ausgegeben werden:

```
Get-EventLog -LogName Application `
   -Source "Directory Synchronization" `
   -EntryType Error `
   -After (Get-Date).AddDays(-7)
```

Listing 4.11 Anzeige von Synchronisierungsereignissen vom Typ Fehler aus den vergangenen sieben Tagen

Kapitel 9

Lync Online

Im neunten Kapitel nutzen Sie Lync Online für Chat, halten Audio- und Videokonferenzen, lernen eine Vielzahl von Clients kennen und richten die Kommunikation mit Skype- und anderen Lync-Anwendern ein.

Mit *Lync* decken Sie die Bereiche *Chat,* Anwesenheitsinformationen, Konferenzen über Audio und Video und – möglicherweise – die herkömmliche Telefonie bis hin zu einem Ersatz der Telefonanlage ab. Das »möglicherweise« hängt von der Konfiguration ab und erfordert gegebenenfalls eine *Lync Server-Infrastruktur* im eigenen Netzwerk.

Zugriff auf Lync erhalten Sie als Anwender nicht nur über diverse Clients, sondern auch direkt integriert in den Office-Anwendungen, insbesondere in Outlook und der Outlook Web App sowie in SharePoint. Dort werden zu den jeweiligen Personenangaben jeweils auch deren Anwesenheitsstatus angezeigt. Sie sehen damit sofort, ob eine Person gerade verfügbar ist, und können unmittelbar eine Lync-Besprechung aufbauen. Der Anwesenheitsstatus wird dabei automatisch mithilfe der Termine des Kalenders und der Abwesenheitsinformationen aus dem Anwenderpostfach gesetzt.

Über einen *Domänenverbund* (auch *Lync Federation* genannt, nicht zu verwechseln mit einem Identitätsverbund) können Sie darüber hinaus eine Verbindung zwischen Ihrer Office 365-Umgebung und anderen Lync-Organisationen herstellen, damit die beteiligten Personen sich untereinander in ihrer Kontaktliste pflegen und ihren Anwesenheitsstatus austauschen können. Auch organisationsübergreifende Lync-Sitzungen sind dann möglich.

In diesem Kapitel werde ich auch mehrfach auf den *Lync Server 2013* verweisen. Dabei handelt es sich um die Lync-Variante, die im eigenen Netzwerk auf eigener Hardware installiert wird.

Microsoft hat angekündigt, Lync im ersten Halbjahr 2015 in *Skype for Business* umzubenennen. [«]

9.1 Was ist Lync Online?

Beginnen wir mit einer kurzen Einführung zu Lync Online. Ich beschreibe verschiedene Einsatzszenarien und die Arbeit mit Lync.

9.1.1 Einsatzszenarien

Um einen ersten Eindruck der Lync-Funktionalität zu bekommen, finden Sie hier einige mögliche Einsatzszenarien:

- Anwesenheitsstatus
  Im Lync-Client sehen Sie den *Anwesenheitsstatus* der eigenen Kontakte. Aber nicht nur dort, sondern in vielen weiteren Microsoft-Anwendungen wie SharePoint und Outlook ist der Status neben den Namen der Anwender zu sehen. Ein Blick genügt, um zu sehen, ob der Anwender an seinem Rechner sitzt (siehe Abbildung 9.1).

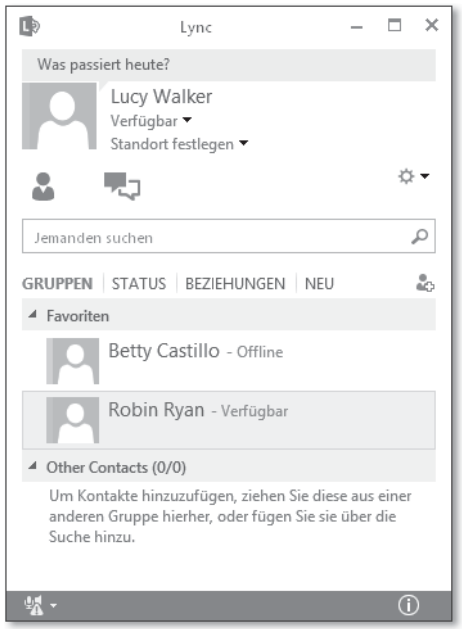

Abbildung 9.1 Anwesenheitsstatus der eigenen Lync-Kontakte

Der Anwesenheitsstatus wird automatisch auf Basis des Kalenders und der Abwesenheitsinformationen im Postfach der Anwender gepflegt. Er ist aber auch manuell in den diversen Clients konfigurierbar.

[»] An dem Anwesenheitsstatus reiben sich gern Datenschützer und Betriebsräte, die hier eine Nachverfolgung wittern, weil angezeigt wird, wie lange ein Anwender offline oder abwesend ist. Deaktivieren lässt sich diese Zeitangabe bei Lync Online derzeit leider nicht.

- Chat
  Chat beschreibt die Kommunikation mithilfe von Sofortnachrichten in Textform *(Instant Messaging)*. In den diversen Lync-Clients können Sie eine Kontaktliste pflegen und mit den Mitgliedern daraus ad hoc eine Chatsitzung beginnen, was oftmals schneller zu einer Antwort führt als eine E-Mail, aber das Gegenüber in seinem Arbeitsablauf nicht so stört wie ein Telefonat (siehe Abbildung 9.2).

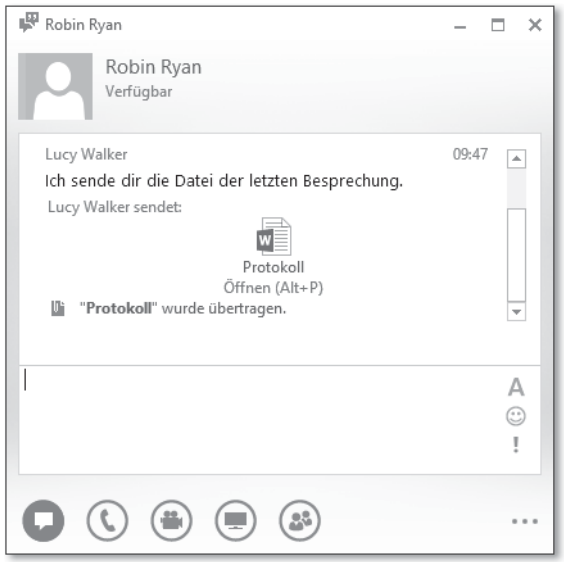

Abbildung 9.2 Chat

- Audio- und Videokonferenzen
  Reicht Chat nicht aus, können Sie mit Ihrem Kommunikationspartner auch eine Audio- und/oder Videokonferenz ad hoc beginnen. Sie kommunizieren dann über ein Mikrofon oder eine Webcam mit Ihrem Gegenüber (siehe Abbildung 9.3).

  An den Besprechungen können bis zu 250 Personen teilnehmen. Während einer solchen Sitzung kann auch eine PowerPoint-Präsentation samt Animationen gezeigt werden. Für das Rendering der Folien ist dabei Lync Online aus Office Online zuständig. Schulungen und Präsentationen sind somit bis zu einem gewissen Grad denkbar.

  Möchte jemand an einer Besprechung teilnehmen, der aber gerade keinen Zugang zu einem Rechner mit einem Lync-Client hat – etwa weil er im Auto unterwegs ist –, kann er zur Einwahl stattdessen ein Telefon verwenden (siehe Abschnitt 9.2.3, »Benutzerverwaltung«). Dazu ist aber ein separater Partner erforderlich, der diese Funktionalität bereitstellt. Lync Online liefert diese nicht automatisch mit.

Abbildung 9.3 Audio-/Videokonferenz

- Desktop-/Anwendungsfreigabe
  In einer Lync-Sitzung können Sie ein bestimmtes Anwendungsfenster oder auch den kompletten Desktop mit anderen teilen. Auch eine Steuerungsweitergabe ist denkbar. So können Sie beispielsweise einem Kollegen unmittelbar bei einem Problem helfen, indem dieser Ihnen seinen Bildschirminhalt überträgt (siehe Abbildung 9.4). Das ist sogar betriebssystemübergreifend möglich.

Abbildung 9.4 Bildschirmübertragungen

- Whiteboard
  Sind während einer Lync-Sitzung schnelle Skizzen erforderlich, können Sie diese mithilfe eines Whiteboards erstellen (siehe Abbildung 9.5).

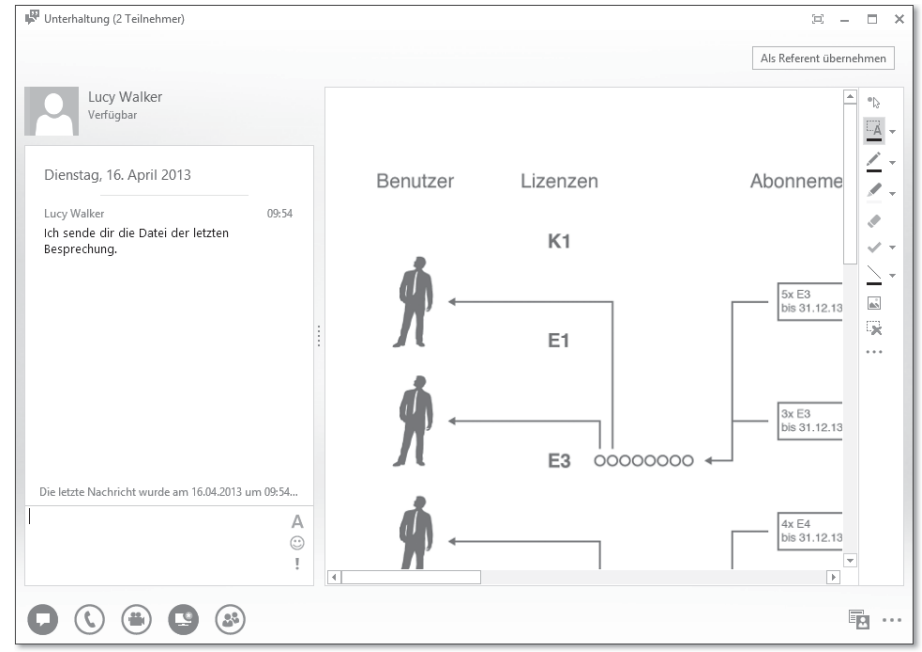

Abbildung 9.5 Whiteboard

- Dateiübertragung
  An Sitzungsteilnehmer der eigenen Lync-Organisation können Sie Dateien übertragen. Damit können Sie möglicherweise den E-Mail-Versand mit großen Anhängen ein wenig einschränken (siehe Abbildung 9.6).

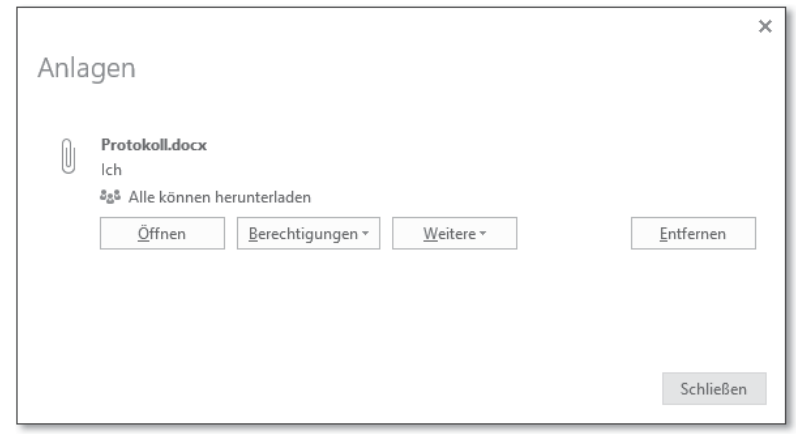

Abbildung 9.6 Dateiübertragung

- Telefonie
  Telefonanrufe in das »normale« Telefonnetz und der Empfang von Anrufen daraus sind zum jetzigen Zeitpunkt mit Lync Online noch nicht möglich, wohl aber mit einer lokal bereitgestellten Lync Server-Infrastruktur.
- Telefonanlagenfunktionalität
  Lync an sich enthält Funktionen, die zum Ersatz einer Telefonanlage eingesetzt werden können. Doch sind diese Funktionen in Lync Online selbst nicht enthalten. Wollen Sie das erreichen, müssen Sie im eigenen Netzwerk einen Lync Server einrichten (siehe Abschnitt 9.5, »Telefonie«).

9.1.2 Lizenzüberblick

Tabelle 9.1 zeigt einen groben Überblick der von den verschiedenen Lizenzpaketen und Einzellizenzen abgedeckten Funktionen.

Funktion	Lync Online in Business Essentials	Lync Online in Business Premium	Lync Online Plan 1	Lync Online Plan 2 (einzeln oder in E1/3/4)
Lync 2013-Client	nein	nein	nein	nur innerhalb von E3/E4
Lync Basic 2013-Client	ja	ja	ja	ja
Lync Windows Store- App	ja	ja	ja	ja
Lync Web App	ja	ja	ja	ja
Lync Mobile Clients	ja	ja	ja	ja
Chat (Sofortnachrichten und Präsenzinformationen)	ja	ja	ja	ja
Lync-zu-Lync-Audio-/Videokonferenzen	ja	ja	ja	ja
Freigabe von Bildschirm, Anwendung	ja	ja	nur Teilnahme	ja
Einwahlkonferenzen (über Partner)	ja	ja	nein	ja

Tabelle 9.1 Lync Online-Funktionsvergleich

Lizenztypen im Detail und im Vergleich mit Lync Server 2013

Die abgedeckten Funktionen der einzelnen Lizenztypen finden Sie detailliert in der offiziellen Dienstbeschreibung unter folgender URL beschrieben:

http://technet.microsoft.com/library/lync-online-service-description.aspx

Dort finden Sie auch einen Vergleich zwischen Lync Online und dem Lync Server 2013.

9.1.3 Arbeiten mit Lync

Je nach Konfiguration finden Sie als Office 365-Anwender an vielen Stellen Lync:

- Clients
  Für unterschiedliche Einsatzzwecke gibt es verschiedene Lync-Clients. Diese reichen von der Unterstützung verschiedener Betriebssysteme über Web- und mobile Clients bis hin zu richtigen Telefonen.
- Outlook
  Mit der Installation des Lync 2013-Clients wird Outlook (ab 2007) um ein spezielles Add-in erweitert. Dadurch finden Sie im Menüband eines neuen Termins die Schaltfläche ONLINEBESPRECHUNG. Klicken Sie auf diese, wird im Textbereich des Termins ein Link zur Online-Besprechung eingefügt. Die Empfänger des Termins können so einfach per Mausklick an der Besprechung teilnehmen (siehe Abbildung 9.7).

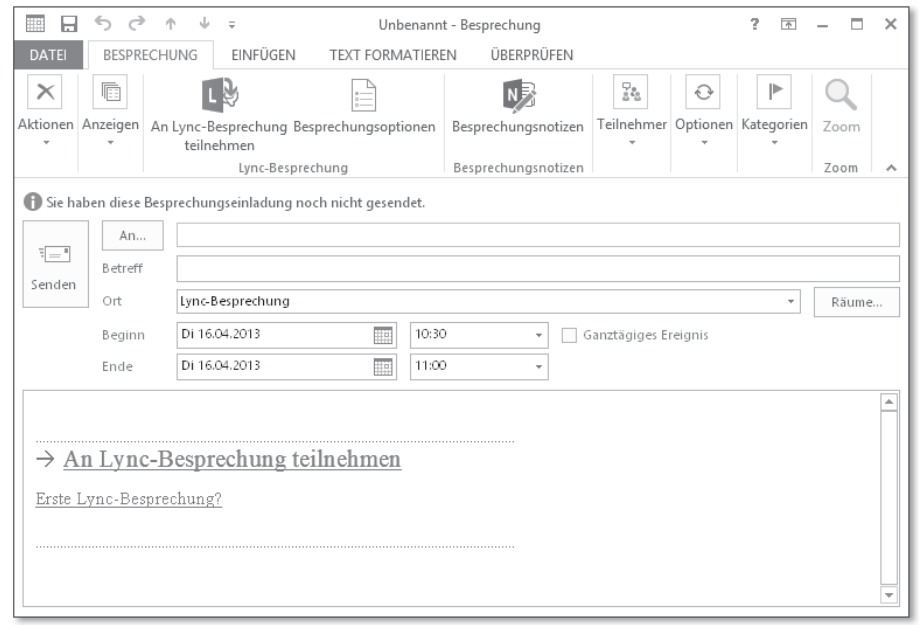

Abbildung 9.7 Outlook-Termin für eine Online-Besprechung

Wie Sie auch ohne Outlook eine Online-Besprechung planen, erläutere ich im Kasten »Lync Online-Besprechungen ohne Outlook planen« unter Abbildung 9.11.

Als Organisator des Termins werden Sie gleichzeitig zum Organisator der Besprechung und können über die Menüband-Registerkarte LYNC-BESPRECHUNG unter BESPRECHUNGSOPTIONEN weitere Einstellungen vornehmen:

– BERECHTIGUNGEN
  In Online-Besprechungen können Sie einen *Wartebereich* nutzen, in den neue Teilnehmer zunächst gelangen, ohne an der Besprechung selbst teilnehmen zu können. Von dort aus kann der Organisator die Teilnehmer in die Besprechung aufnehmen. Der Bereich enthält Einstellungen, ob und wann der Wartebereich zum Einsatz kommt. Daneben konfigurieren Sie hier, wer Referent der Besprechung sein soll und damit Inhalte freigeben und Personen zulassen kann.
– EINLADUNGSSPRACHE
  Die Einladungssprache kann auf Englisch umgestellt werden.
– INFO
  Versionsinformationen zum Outlook-Add-in

Neben der Lync-Besprechungsplanung finden Sie in Outlook 2013 im Bereich PERSONEN links die LYNC-KONTAKTE. Auch darüber können Sie den Anwesenheitsstatus der Kontakte einsehen und direkt eine Besprechung starten (siehe Abbildung 9.8).

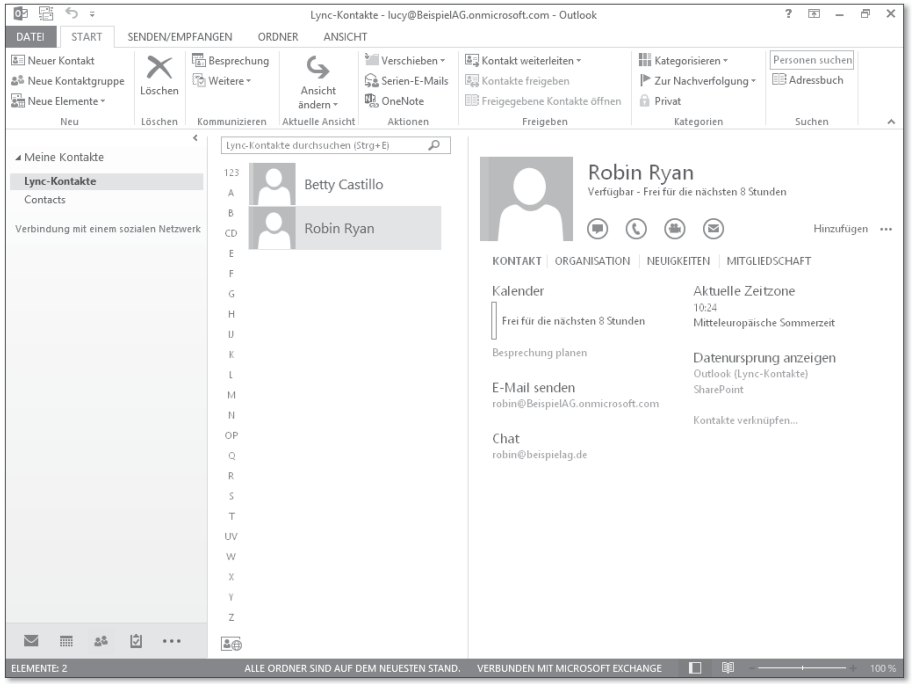

Abbildung 9.8 Lync-Kontakte in Outlook 2013

Vorausgesetzt wird hier allerdings, dass der Lync 2013-Client auf dem lokalen Rechner installiert ist (siehe Abschnitt 9.4.1, »Lync 2013-Client«).

- Outlook Web App

  In der Outlook Web App ist Lync von sich aus bereits an mehreren Stellen integriert:

  – In der Navigation rechts oben, kombiniert mit dem Namen des Anwenders. Der Name fungiert als Menü, über das Sie Ihren Lync-Anwesenheitsstatus ändern können (siehe Abbildung 9.9).
  – Fahren Sie mit der Maus auf einen Kontakt, können Sie mit der Person eine Lync-Instant-Messaging-Sitzung aufbauen, sofern diese an Lync angemeldet ist.

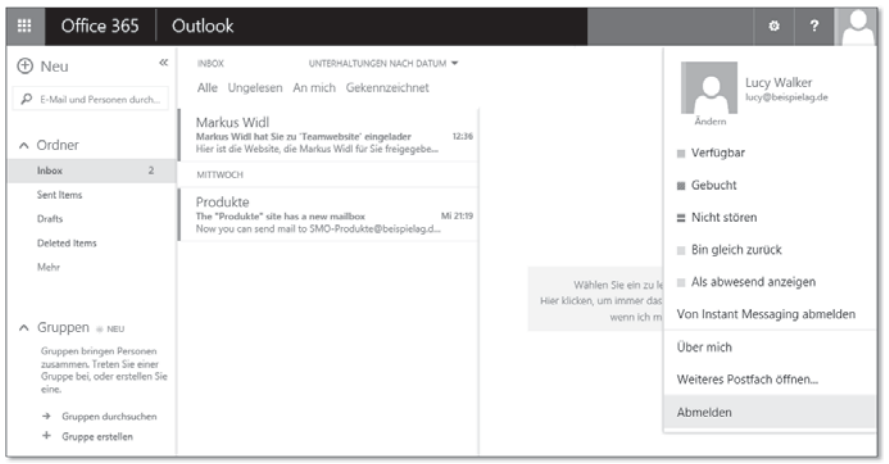

Abbildung 9.9 Lync in der Outlook Web App

- Office-Anwendungen

  Mit der Installation des Lync-Clients werden auch die Office-Anwendungen Word, PowerPoint und Excel (jeweils ab Version 2007) um ein Plug-in erweitert, das einige Lync-Funktionen einführt. Beispiel: Klicken Sie in Word auf DATEI • FREIGEBEN • ALS CHATNACHRICHT SENDEN, können Sie direkt aus der Anwendung heraus eine Instant-Messaging-Besprechung mit bestimmten Teilnehmern starten (siehe Abbildung 9.10). Dabei wird die gerade geöffnete Datei an alle Teilnehmer versandt. Die Besprechung selbst findet dann im Lync-Client statt.

- SharePoint Online

  Zuletzt finden Sie auch im Browser bei der Ansicht Ihrer SharePoint-Online-Umgebung den Anwesenheitsstatus der Lync-Anwender bei den jeweiligen Namen, etwa in der Spalte GEÄNDERT VON. Auch von dort aus können Sie ad hoc eine Lync-Besprechung starten. Führen Sie den Mauszeiger auf den Personennamen, erscheint ein Lync-Fenster (siehe Abbildung 9.11).

Wie beim Outlook-Add-in muss auch hier für die SharePoint-Integration auf dem Computer der Lync 2013-Client installiert sein.

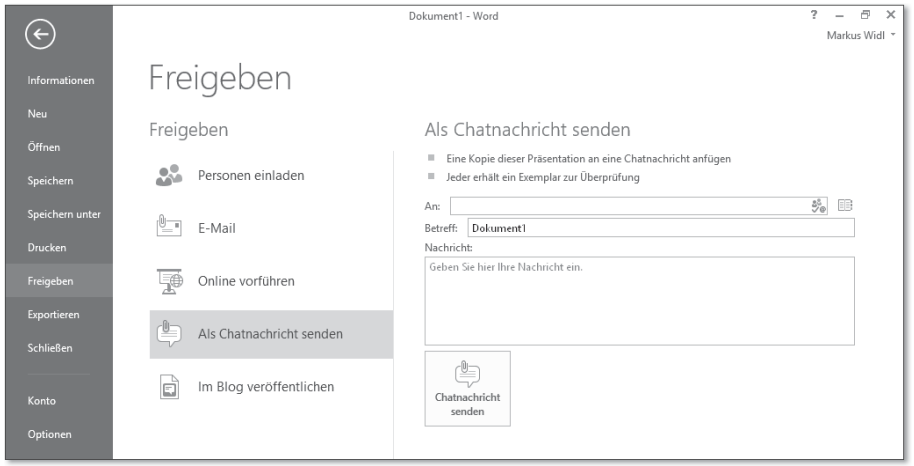

Abbildung 9.10 Lync-Integration in Word 2013

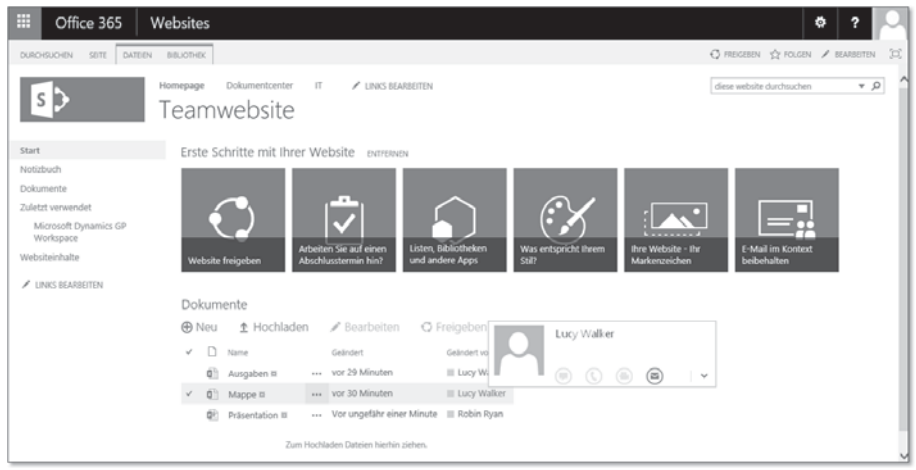

Abbildung 9.11 SharePoint-Integration

Lync Online-Besprechungen ohne Outlook planen

Wie Sie mithilfe von Outlook eine Lync Online-Besprechung planen, habe ich bereits erläutert. Doch auch ohne Outlook können Sie Besprechungen anlegen, und zwar über den *Lync Web Scheduler*. Dabei handelt es sich um eine spezielle Website, die Sie unter folgender URL erreichen:

https://sched.lync.com/

Melden Sie sich dort mit einem Office 365-Mandanten an, der auch über eine Lync-Lizenz verfügt, ist dort das Anlegen von Besprechungen möglich (siehe Abbildung 9.12).

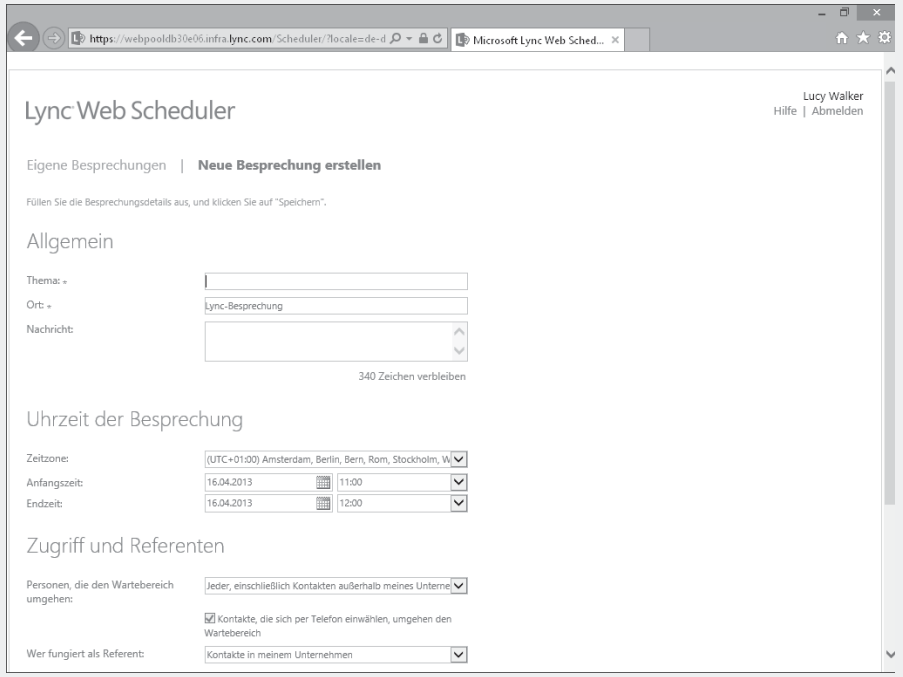

Abbildung 9.12 Website zur Planung von Online-Besprechungen

Die Website liefert Ihnen auch eine URL zur Besprechung, die Sie wiederum in eine E-Mail einbetten können. Ein Zwang zur Verwendung von Outlook bei der Planung von Lync Online-Besprechungen ist also nicht gegeben.

9.2 Administration

Im Vergleich zu den »großen« Anwendungen Exchange Online und SharePoint Online ist die Administration von Lync Online weit weniger umfangreich und komplex.

9.2.1 Voraussetzungen

Um einen einwandfreien Betrieb von Lync Online zu gewährleisten, müssen verschiedene Voraussetzungen erfüllt sein. Dazu gehören Domäneneinstellungen, Firewallausnahmen und die Benutzerkonfiguration.

Domäneneinstellungen

Die für Lync Online verwendeten Domänen müssen im DNS-Server entsprechend konfiguriert sein. Lesen Sie dazu in Abschnitt 2.4, »Domänenverwaltung«, nach.

Firewallausnahmen

Damit die Kommunikation zwischen den Teilnehmern einer Lync Online-Besprechung uneingeschränkt funktioniert, muss die externe Firewall mit einigen Ausnahmen konfiguriert werden. Sind diese nicht vorhanden, äußert sich das oftmals in der nicht funktionierenden Audio- und Videoübertragung und anderen Freigabeproblemen.

Tabelle 9.2 zeigt eine Übersicht der erforderlichen Ausnahmen.

Port	Protokoll	Richtung	Verwendung
443	STUN/TCP	ausgehend	Audio- und Videoübertragung sowie Anwendungs- und Desktopfreigabe
443	PSOM/TLS	ausgehend	Dateiübertragung
3478	STUN/UDP	ausgehend	Audio- und Videoübertragung
5223	TCP	ausgehend	Lync Mobile-Pushbenachrichtigungen
50000–59999	RTP/UDP	ausgehend	Audio- und Videoübertragung

Tabelle 9.2 Lync Online-Firewallausnahmen

Außerdem müssen ausgehende Verbindungen zu folgenden Zielen zugelassen werden:

- **.microsoftonline.com*
- **.microsoftonline-p.de*
- **.sharepoint.com*
- **.outlook.com*
- **.lync.com*
- *osub.microsoft.com*

Diese Ausnahmen gelten jeweils für die Protokolle TCP und HTTPS, und das SSL-Timeout sollte auf acht Stunden festgelegt werden.

Weitere Informationen zur Firewallkonfiguration wie die von Lync Online verwendeten IP-Adressbereiche und URLs finden Sie unter folgender URL:

http://support.microsoft.com/kb/2409256/de

Auch auf den Clients werden Firewallausnahmen benötigt, die mit der Installation des Lync 2013-Clients automatisch erfolgen.

Benutzerkonfiguration

Zur Anmeldung an Lync Online benötigt jeder Office 365-Benutzer eine Lync Online-Lizenz. Dem Benutzer wird automatisch eine SIP-Adresse (*SIP = Session Initiation Protocol*) zugewiesen. Standardmäßig entspricht diese dem Anmeldenamen (Benutzerprinzipalname). Ändern Sie den Anmeldenamen des Benutzers, ändert sich seine SIP-Adresse automatisch mit.

Einen Nachteil bei der Änderung der SIP-Adresse sollten Sie beachten: Anwender, die die Person mit neuer SIP-Adresse in ihrer Kontaktliste haben wollen, müssen die Person unter der neuen SIP-Adresse erneut eintragen. [«]

SIP-Adresse ändern

Um nur die SIP-Adresse zu ändern, stehen Ihnen zwei Wege offen:

Im Exchange Admin Center von Exchange Online öffnen Sie im Bereich Empfänger den Abschnitt Postfächer. Bearbeiten Sie eines der angezeigten Postfächer, können Sie unter E-Mail-Adresse auch die SIP-Adresse anpassen (siehe Abbildung 9.13).

Das setzt allerdings voraus, dass dem Benutzer auch eine Exchange Online-Lizenz zugewiesen wurde.

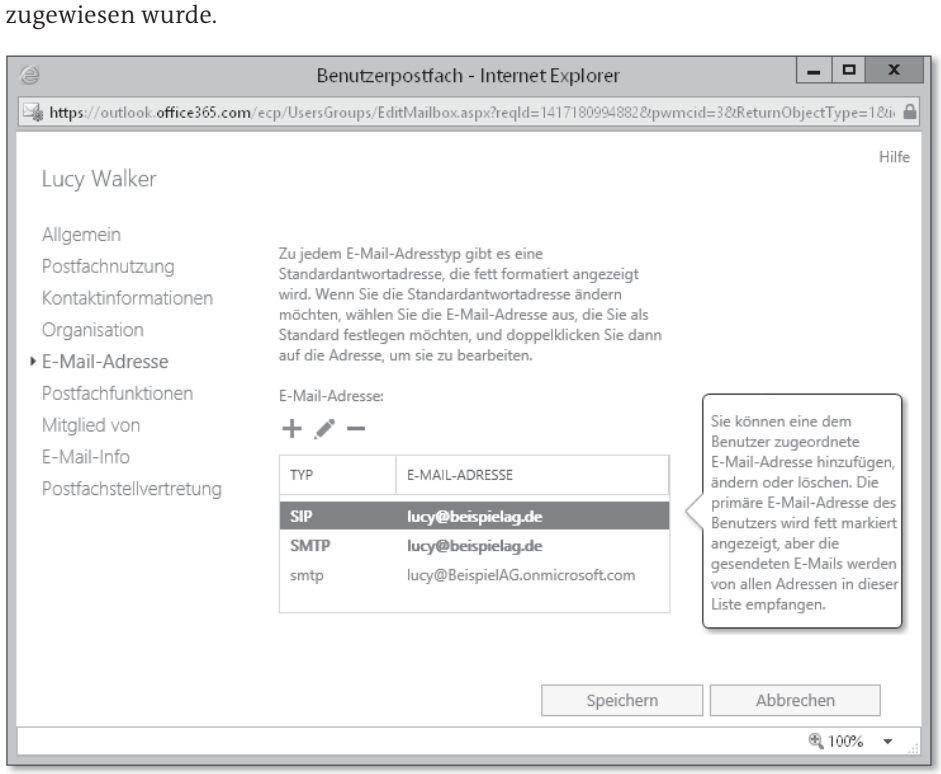

Abbildung 9.13 Änderung der SIP-Adresse über das EAC

Die Änderung der SIP-Adresse eines Benutzers mithilfe der PowerShell nehmen Sie wieder über Exchange vor:

1. Haben Sie die Active-Directory-Verzeichnissynchronisierung aktiviert und betreiben einen lokalen Exchange Server, starten Sie die *Exchange Management Shell (EMS)*. Ansonsten starten Sie die PowerShell und stellen über das Kommando aus Listing 9.1 eine Verbindung mit Exchange Online her. Vorausgesetzt wird auch hier, dass der betroffene Benutzer über eine Exchange Online-Lizenz verfügt.

```
#Office 365-Administratorbenutzer abfragen
$cred = Get-Credential
$session = New-PSSession `
   -ConfigurationName Microsoft.Exchange `
   -ConnectionUri https://outlook.office365.com/powershell-liveid/ `
   -Credential $cred `
   -Authentication Basic `
   -AllowRedirection
Import-PSSession $session
```

Listing 9.1 Verbindungsaufbau mit Exchange Online

2. Über das Cmdlet `Get-Mailbox` ermitteln Sie die E-Mail-Adressen (Eigenschaft `EmailAddresses`) des Benutzers. Dort ist auch die SIP-Adresse enthalten. Passen Sie die Liste entsprechend an, und schreiben Sie sie dann über `Set-Mailbox` zurück. Ein Beispiel liefert Listing 9.2.

```
#Benutzername
$identity = "lucy@beispielag.de"
#Alte SIP-Adresse
$alt_sip = "sip:lucy@beispielag.de"

#Neue SIP-Adresse
$neu_sip = "sip:lucyneu@beispielag.de"

#Adressen ermitteln
$mail = (Get-Mailbox -Identity $identity).EmailAddresses

#Alte SIP-Adresse ersetzen
$mail = $mail -replace $alt_sip, $neu_sip

#Adressen schreiben
Set-Mailbox -Identity $identity -EmailAddresses $mail
```

Listing 9.2 SIP-Adresse ändern

[»] Für Lync Online gibt es zwar auch eine PowerShell-Erweiterung (siehe Abschnitt 9.3), jedoch ist damit eine Änderung der SIP-Adresse nicht möglich.

9.2.2 Lync Admin Center

Die Lync-Administration finden Sie im Office 365 Admin Center unter ADMINISTRATOR • LYNC. Es erscheint das *Lync Admin Center* aus Abbildung 9.14.

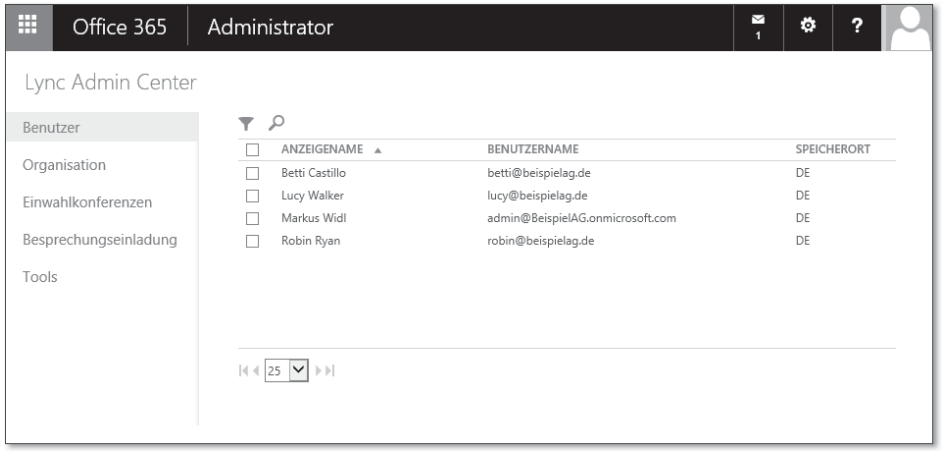

Abbildung 9.14 Lync Admin Center

Tabelle 9.3 führt die Hauptbereiche der Systemsteuerung auf und erläutert kurz deren jeweilige Aufgabe.

Bereich	Aufgabe
BENUTZER	Anzeige von Benutzern mit Lync Online-Lizenz. Zu jedem Benutzer werden die aktivierten Lync-Funktionen aufgeführt (siehe Abschnitt 9.2.3, »Benutzerverwaltung«).
ORGANISATION	Konfiguration, an welche Anwender die Anwesenheitsinformationen übertragen werden, Einstellungen, welche Pushbenachrichtigungsdienste für mobile Clients zum Einsatz kommen sollen (siehe Abschnitt 9.4.4, »Mobile Lync-Clients«), sowie die Konfiguration eines Domänenverbunds, um die Kommunikation mit Lync-Benutzern außerhalb der eigenen Office 365-Umgebung zuzulassen (siehe Abschnitt 9.2.5, »Externe Kommunikation«)
EINWAHLKONFERENZEN	Konfiguration von Einwahlkonferenzen, mit denen Anwender über ein Telefon an Lync-Besprechungen teilnehmen können (siehe Abschnitt 9.2.6, »Einwahlkonferenzen«)
BESPRECHUNGS-EINLADUNG	Planen von und Einladen zu Besprechungen (siehe Abschnitt 9.2.7, »Besprechungseinladungen«)

Tabelle 9.3 Administrationsbereiche

Im Folgenden werden wir die Konfigurationsoptionen durchgehen und ihre Auswirkungen besprechen.

9.2.3 Benutzerverwaltung

Im letzten Bereich Benutzer des Lync Admin Centers finden Sie eine Liste der Lync Online-Benutzer (siehe Abbildung 9.14).

[»] Achtung: Die Spalte Benutzername enthält nicht zwangsläufig die SIP-Adresse, sondern grundsätzlich den allgemeinen Office 365-Benutzernamen. Benötigen Sie eine Liste mit Name und SIP-Adresse, können Sie das PowerShell-Skript aus Listing 9.6 ausprobieren.

In der Benutzerverwaltung schränken Sie für Ihre Anwender manche Funktionalität ein, indem Sie den Benutzer markieren und auf Bearbeiten (Stift-Symbol) klicken (siehe Abbildung 9.15).

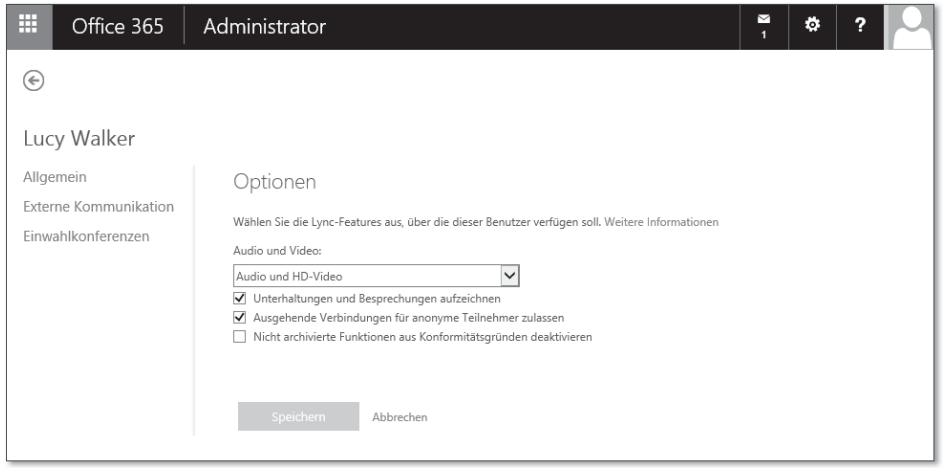

Abbildung 9.15 Benutzereinstellungen

Bei den Benutzereinstellungen aktivieren und deaktivieren Sie die folgenden Optionen:

- Allgemein
  Darunter fallen beispielsweise die Verwendung von Audio und/oder Video und das Aufzeichnen von Besprechungen.
- Externe Kommunikation
  Dazu gehört die Kommunikation mit Benutzern aus anderen Lync-Organisationen und mit Skype.
- Einwahlkonferenzen
  Konfiguration der Zugangsdaten für eine Teilnahme an einer Lync-Besprechung per Telefon

Standardmäßig sind mit Ausnahme der Einwahlkonferenz alle Optionen aktiviert, sodass der Anwender nicht eingeschränkt wird.

9.2.4 Organisationsverwaltung

Der Anwesenheitsstatus eines Anwenders steht automatisch allen zur Verfügung, die potenziell mit dem Anwender kommunizieren könnten, also beispielsweise auch den über einen Domänenverbund angebundenen Anwendern. Ist das für Ihr Unternehmen zu öffentlich, können Sie die Anzeige dieser Anwesenheitsinformationen auf Kontakte eines Benutzers einschränken. Wählen Sie dazu im Lync Admin Center im Bereich Organisation unter Vertraulicher Anwesenheitsmodus die Option Anwesenheitsinformationen nur für Kontakte eines Benutzers anzeigen (siehe Abbildung 9.16).

Abbildung 9.16 Vertraulicher Anwesenheitsmodus

Der Anwesenheitsstatus kann vom Anwender selbst über die Lync-Clients gesetzt werden und wird gegebenenfalls automatisch mit den Einträgen des Kalenders und den Abwesenheitsinformationen aus dem Exchange-Postfach abgeglichen. Der Status kann einen der folgenden Werte annehmen:

- Verfügbar
- Beschäftigt
- Nicht stören
- Bin gleich zurück
- Nicht bei der Arbeit
- Als abwesend anzeigen

Neben der Konfiguration des Anwesenheitsmodus können Sie in diesem Bereich auswählen, welche Pushbenachrichtigungsdienste verwendet werden sollen, um

mobile Clients über Chat, Voicemailnachrichten und Anrufe in Abwesenheit zu informieren. Zur Auswahl stehen die Pushbenachrichtigungsdienste von Microsoft (für Windows Phone-Geräte) sowie von Apple (für Apple iOS-Geräte). Standardmäßig sind beide aktiviert. Für Android-Geräte ist ein solcher Pushbenachrichtigungsdienst nicht erforderlich, da dort der Lync-Client über Multitasking ständig läuft und dauerhaft mit dem Server verbunden ist.

9.2.5 Externe Kommunikation

Zu den Einstellungen der externen Kommunikation gehören die Einrichtung eines *Domänenverbunds* sowie die Anbindung an öffentliche Chatdienstanbieter.

Domänenverbund

Mit einem Domänenverbund koppeln Sie Ihre eigene Lync Online-Umgebung mit einer anderen Lync Online- oder auch Lync Server-Umgebung. Der Vorteil dabei ist die Kommunikation über Unternehmensgrenzen hinweg. So können an einer Besprechung Teilnehmer aus unterschiedlichen Unternehmen teilhaben, der Anwesenheitsstatus ist übergreifend verfügbar etc. Für die Personen der anderen Unternehmen werden in Ihrer eigenen Office 365-Umgebung keine zusätzlichen Lync Online-Lizenzen benötigt.

Wählen Sie im Lync Admin Center im Bereich ORGANISATION den Abschnitt EXTERNE KOMMUNIKATION (siehe Abbildung 9.17).

Abbildung 9.17 Externe Kommunikation

Unter EXTERNER ZUGRIFF haben Sie die Auswahl zwischen folgenden Optionen:

- AKTIVIEREN MIT AUSNAHME DER BLOCKIERTEN DOMÄNEN
  Damit öffnen Sie Ihre eigene Lync Online-Umgebung für alle nach außen, mit Ausnahme der blockierten Domänen. Lync-Benutzer aus den blockierten Domänen

  erhalten keinen Anwesenheitsstatus übermittelt und können auch keine Lync-Sitzung initiieren.

  Das ist eine eher weitgehende Freigabe. Möglicherweise werden Ihre Anwender dadurch von unliebsamen Gästen gestört. Deshalb ist die zweite Option zu überlegen.

- NUR FÜR ZULÄSSIGE DOMÄNEN AKTIVIEREN
  Hier wird die Öffnung der eigenen Lync Online-Umgebung auf einzelne Domänen beschränkt, beispielsweise die Domänen von Partnerunternehmen, mit denen Sie zusammenarbeiten.
- VOLLSTÄNDIG DEAKTIVIEREN
  Lync-Sitzungen sind nur mit Benutzern aus der eigenen Lync-Organisation möglich, Anwesenheitsinformationen werden nicht nach außen weitergegeben.

  Hierbei handelt es sich um die Standardeinstellung.

Aktivieren Sie den Domänenverbund, sollten Sie Geduld haben. Lync Online benötigt möglicherweise einen Tag, bis der Verbund aufgebaut ist.

Eine Beschreibung, was Administratoren eines Lync Servers 2013 tun müssen, um einen Domänenverbund mit einer Lync Online-Umgebung aufzubauen, finden Sie unter folgender URL: [«]

http://technet.microsoft.com/de-de/library/hh202193.aspx

Öffentliche Chatdienste

Der im Lync Admin Center verwendete Begriff *Öffentliche Chatdienste* ist etwas zu weit gefasst (siehe Abbildung 9.17). Es geht hier nur um Skype-Anwender. Also nicht etwa um den *AOL Instant Messenger (AIM)*, *Yahoo! Messenger* oder ähnliche Produkte.

Standardmäßig ist diese Verbindung deaktiviert.

Aktivieren Sie die Verbindung zu Skype, sind folgende Funktionen derzeit schon möglich:

- Austausch des Anwesenheitsstatus
- Chat
- Audioanrufe
- Videoanrufe
- Suchen und Hinzufügen von Lync-Kontakten zu Skype

Dagegen sind die folgenden Funktionen noch nicht möglich:

- Videokonferenzen mit mehr als zwei Teilnehmern
- Audiokonferenzen mit mehr als zwei Teilnehmern

- Chat mit mehreren Teilnehmern
- Desktop- und Anwendungsfreigabe

Auch hier müssen Sie nach der Aktivierung möglicherweise einen Tag warten, bis die Verbindung funktionsfähig hergestellt wird. Vermutlich wird Microsoft auch hier den Funktionsumfang mit Skype in Zukunft erweitern.

Damit die Kommunikation zwischen Lync und Skype funktioniert, ist es erforderlich, dass sich die Skype-Anwender mit einem Microsoft-Konto an Skype anmelden. Derzeit haben Skype Anwender bei der Anmeldung die Auswahl zwischen einem Skype-Namen, Facebook und einem Microsoft-Konto.

9.2.6 Einwahlkonferenzen

Einwahlkonferenzen sind für Sie und Ihre Anwender dann von Vorteil, wenn Personen an einer Lync-Besprechung teilnehmen wollen, die jedoch während der Besprechung keinen Zugriff auf einen der zahlreichen Lync-Clients haben. Das gilt beispielsweise für jemanden, der gerade mit dem Auto unterwegs ist oder sich im Urlaub befindet. In diesem Fall können die Personen mit einem herkömmlichen Telefon oder Handy bei einer Einwahlnummer anrufen und dem Audioteil der Besprechung folgen.

Einwahlkonferenzen sind allerdings nicht im Produktumfang von Lync Online enthalten. Diese Funktionalität können Sie nur mit einem dazu geeigneten Lync Online-Partner nutzen, der sich für die Bereitstellung der Infrastruktur natürlich separat bezahlen lässt. Derzeit sind die folgenden Partner als Bereitsteller von Einwahlkonferenzen möglich:

- PGi: *http://www.pgi.com/de/de/*
- Intercall: *http://de.intercalleurope.com*
- BT Conferencing *http://www.btconferencing.com*

Voraussetzung für die Konfiguration einer Einwahlkonferenz ist die Lizenzierung Ihrer Office 365-Benutzer mit einer Lync Online-Lizenz. Dann können Sie im Lync Admin Center im Bereich EINWAHLKONFERENZEN im Abschnitt BENUTZER MIT EINGEHENDEN VERBINDUNGEN für jeden Benutzer separat die Daten eines der Lync Online-Partner angeben (siehe Abbildung 9.18).

Die Einwahlkonferenzeinstellungen für jeden Benutzer umfassen die Auswahl eines Anbieters, einer gebührenpflichtigen Nummer, einer optionalen gebührenfreien Nummer und einer Kennung (einem Kennwort), anhand derer der Anrufer authentifiziert wird.

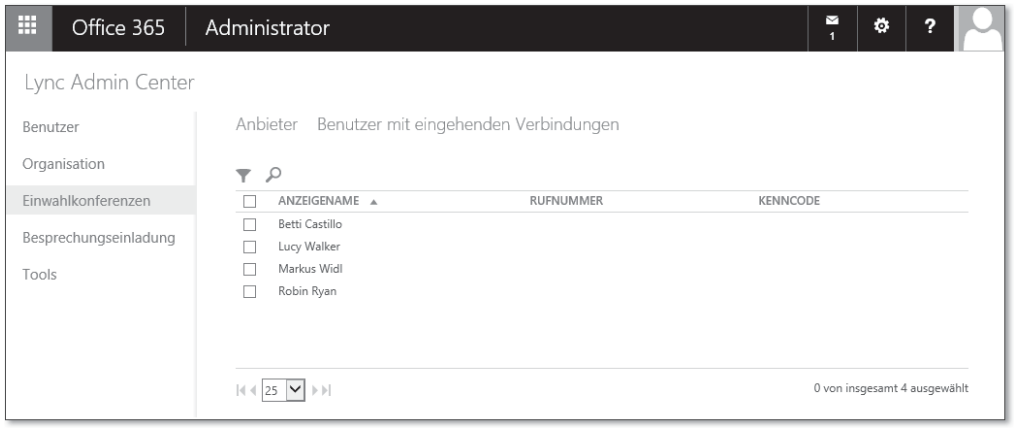

Abbildung 9.18 Benutzerinformationen für Einwahlkonferenzen

Die Einstellungen für die Einwahlkonferenz können Sie im Bereich EINWAHLKONFERENZEN im Abschnitt ANBIETER auch ex- und importieren. Das Austauschformat ist dabei eine CSV-Datei, mit der Sie die jeweiligen Daten für die Anwender pflegen können, was sicher etwas schneller geht, als für jeden Benutzer einzeln im Lync Admin Center die Daten zu erfassen – vorausgesetzt, Sie verfügen über eine nennenswerte Benutzeranzahl.

Konferenzeinwahl

Möchten Sie dann tatsächlich per Einwahl an einer Konferenz teilnehmen, gehen Sie wie folgt vor:

1. Sie rufen die gebührenpflichtige oder die kostenfreie Telefonnummer an.
2. Über die Telefontastatur geben Sie Ihre Kennung ein.

Über die Telefontastatur können Sie außerdem die Kommandos aus Tabelle 9.4 eingeben.

Kommando	Beschreibung
*1	private Ansage der verfügbaren Kommandos
*3	private Ansage der Namen der Konferenzteilnehmer
*4	Teilnehmer stumm schalten
*6	eigenes Mikrofon stumm schalten bzw. öffnen

Tabelle 9.4 Telefonkommandos

Kommando	Beschreibung
*7	Sperren bzw. Freigeben der Konferenz
*8	Alle Personen des Wartebereichs freigeben. Neue Teilnehmer werden automatisch freigegeben.
*9	Aktivieren bzw. Deaktivieren der Ankündigung neuer Konferenzteilnehmer

Tabelle 9.4 Telefonkommandos (Forts.)

9.2.7 Besprechungseinladungen

Im Bereich Besprechungseinladung haben Sie die Möglichkeit, ebendiese ein klein wenig zu individualisieren. Es geht dabei um die Besprechungseinladungen, die Sie über Outlook verwenden, sofern der Lync 2013-Client installiert ist, und den Lync Web Scheduler:

https://sched.lync.com/

Zur Auswahl stehen Logo, URLs für weitere Informationen und ein Fußzeilentext (siehe Abbildung 9.19).

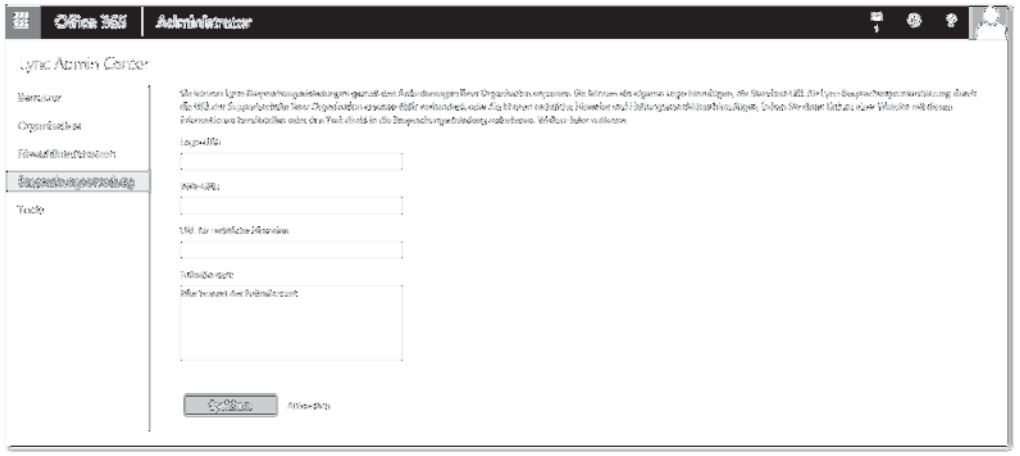

Abbildung 9.19 Besprechungseinladungen

9.3 PowerShell mit Lync Online

Für die Lync Online-Administration mit PowerShell benötigen Sie ein Modul, das rund 50 Befehle umfasst.

9.3.1 Voraussetzungen

Ähnlich wie beim Windows Azure Active Directory und bei SharePoint Online müssen Sie ein Modul auf dem lokalen Computer installieren, mit dem Sie die erforderlichen Befehle nachrüsten. Um mit dem Lync-Modul arbeiten zu können, müssen lokal die folgenden Voraussetzungen erfüllt sein:

- Windows ab 7 bzw. Windows Server ab 2008 R2 (jeweils in einer 64-Bit-Ausgabe)
- Windows PowerShell 3
- Die PowerShell-Ausführungsrichtlinie darf nicht auf `Restricted` stehen. Ändern Sie den Wert gegebenenfalls mit `Set-ExecutionPolicy`.
- .NET Framework 4.5
- Microsoft Online Services-Anmelde-Assistent

  http://www.microsoft.com/download/details.aspx?id=41950

Das Installationspaket des Lync Online-Moduls erhalten Sie unter der folgenden URL: *http://www.microsoft.com/en-us/download/details.aspx?id=39366*

9.3.2 Verbindungsaufbau

Das Lync Online-Modul trägt den internen Namen `LyncOnlineConnector`. Sie können es mit dem folgenden Kommando explizit in eine PowerShell-Sitzung importieren:

```
Import-Module LyncOnlineConnector
```

Listing 9.3 Import des Lync-Moduls

Das Modul enthält nur die Funktion `New-CsOnlineSession`, mit der Sie eine Verbindung zu Lync Online aufbauen. Alle weiteren Befehle werden dann über das PowerShell-Remoting in die lokale PowerShell-Sitzung importiert.

Führen Sie zum Verbindungsaufbau folgendes Kommando aus:

```
$cred = Get-Credential
$session = New-CsOnlineSession -Credential $cred
$module = Import-PSSession -Session $session
```

Listing 9.4 Lync Online-Verbindungsaufbau

Nach dem erfolgreichen Import können Sie eine Liste der Lync-Befehle abfragen (siehe Abbildung 9.20):

```
Get-Command -Module $module |
   Sort-Object -Property Noun
```

Listing 9.5 Abfrage der Lync-Befehle

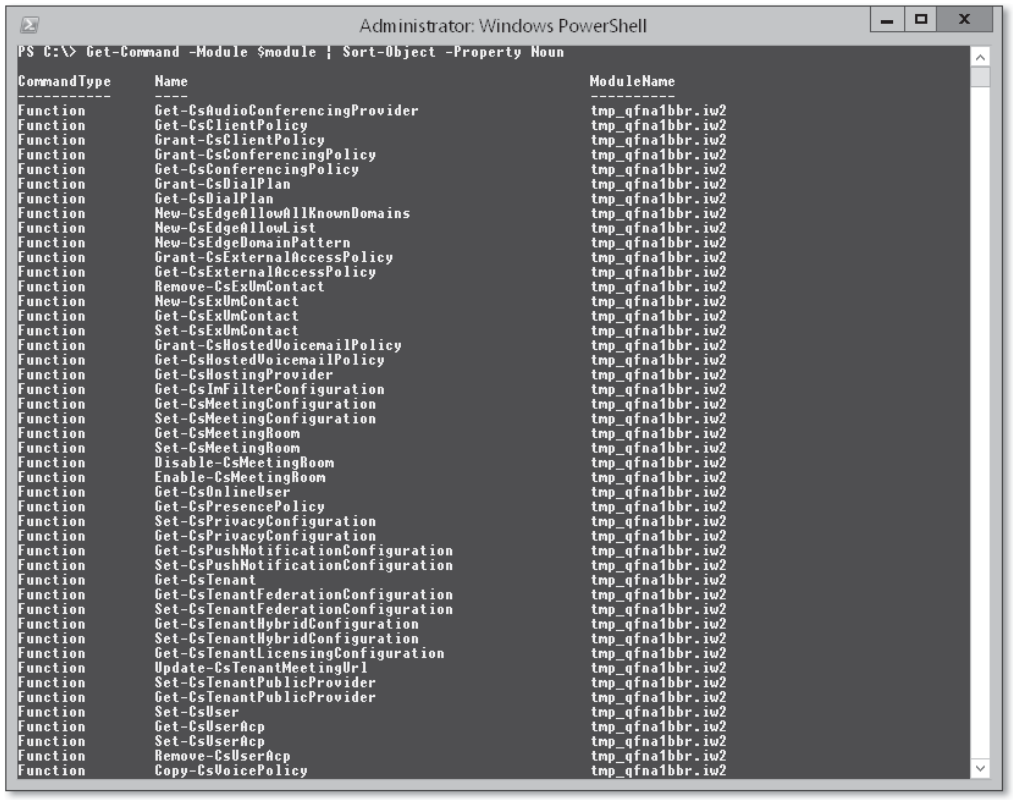

Abbildung 9.20 Abfrage der Lync-Befehle

9.3.3 Anwendung

In diesem Abschnitt sehen wir uns einige Anwendungsbeispiele des Lync Online-Moduls an, um die Arbeitsweise zu demonstrieren.

Erstellen einer Benutzerliste

Zunächst erstellen wir eine Liste aller Benutzer mit dem jeweiligen Benutzerprinzipalnamen sowie den zugehörigen SIP-Adressen (siehe Abbildung 9.21):

```
Get-CsOnlineUser |
   Select-Object UserPrincipalName,SipAddress
```

Listing 9.6 Erstellen einer Benutzerliste mit SIP-Adressen

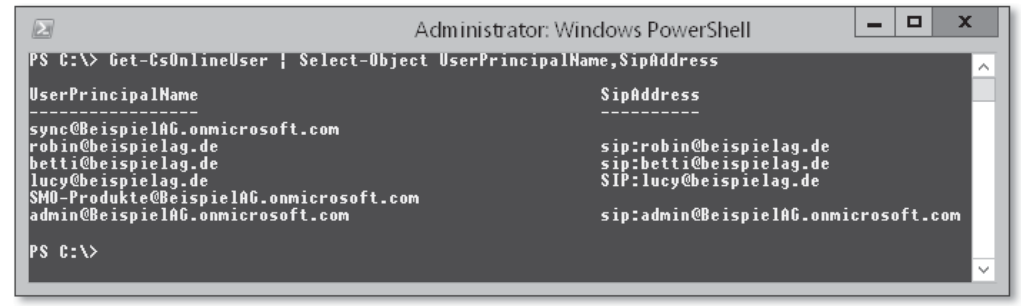

Abbildung 9.21 Erstellen einer Benutzerliste mit SIP-Adressen

Externe Kommunikation

Wollen Sie die Kommunikation über Lync mit einer anderen Domäne zulassen (beispielsweise bei einem Partnerunternehmen), müssen Sie dies erst entsprechend konfigurieren.

Ob die externe Kommunikation mit anderen Domänen grundsätzlich erlaubt ist, ermitteln Sie mit folgendem Kommando:

```
Get-CsTenantFederationConfiguration
```

Listing 9.7 Abfrage der Einstellungen für externe Kommunikation

Steht dabei die Eigenschaft `AllowFederatedUsers` auf `False`, ist die externe Kommunikation nicht erlaubt.

Bei der Aktivierung der externen Kommunikation haben wir nun die Auswahl zwischen zwei Strategien:

- Externe Kommunikation aktivieren mit Ausnahme der blockierten Domänen
- Externe Kommunikation nur für zulässige Domänen aktivieren

Mehr zur externen Kommunikation mit Lync lesen Sie in Abschnitt 9.2.5, »Externe Kommunikation«. [«]

Sehen wir uns nun die PowerShell-Konfiguration für beide Strategien an.

Externe Kommunikation aktivieren mit Ausnahme der blockierten Domänen

Bei dieser Strategie öffnen wir unsere Lync-Domäne grundsätzlich nach außen, blockieren aber die Kommunikation mit bestimmten Domänen. Hier ein Beispiel:

```
#Externe Kommunikation aktivieren
Set-CsTenantFederationConfiguration -AllowFederatedUsers $true `
   -AllowedDomains (New-CsEdgeAllowAllKnownDomains)
```

```
#Liste blockierter Domänen leeren
Set-CsTenantFederationConfiguration -BlockedDomains $null

#Domäne zur Liste blockierter Domänen hinzufügen
$pattern = New-CsEdgeDomainPattern -Domain "beispielag.de"
Set-CsTenantFederationConfiguration `
   -BlockedDomains @{Add=$pattern}

#Domäne von der Liste blockierter Domänen entfernen
$pattern = New-CsEdgeDomainPattern -Domain "beispielag.de"
Set-CsTenantFederationConfiguration `
   -BlockedDomains @{Remove=$pattern}
```

Listing 9.8 Externe Kommunikation aktivieren mit Ausnahme der blockierten Domänen

Externe Kommunikation nur für zulässige Domänen aktivieren

Bei dieser Strategie lassen wir die Kommunikation nur mit einzelnen Domänen zu. Auch hier ein Beispiel:

```
#Federation nur für zulässige Domänen aktivieren
Set-CsTenantFederationConfiguration -AllowFederatedUsers $true

#Liste zugelassener Domänen erstellen
$list = New-CsEdgeAllowList
$list.AllowedDomain.Add(
   (New-CsEdgeDomainPattern -Domain "beispielag1.de"))
$list.AllowedDomain.Add(
   (New-CsEdgeDomainPattern -Domain "beispielag2.de"))
$list.AllowedDomain.Add(
   (New-CsEdgeDomainPattern -Domain "beispielag3.de"))

Set-CsTenantFederationConfiguration -AllowedDomains $list
```

Listing 9.9 Externe Kommunikation nur für zulässige Domänen aktivieren

Externe Kommunikation nicht zulassen

Zu guter Letzt können wir die externe Kommunikation mit dem folgenden Kommando auch wieder deaktivieren:

```
Set-CsTenantFederationConfiguration -AllowFederatedUsers $false
```

Listing 9.10 Externe Kommunikation nicht zulassen

Konferenzaufzeichnungen

Das Aufzeichnen von Lync-Konferenzen wird standardmäßig erlaubt. Sie können das aber auch mit dem folgenden Kommando deaktivieren:

```
Set-CsMeetingConfiguration -AllowConferenceRecording $False
```

Listing 9.11 Deaktivieren von Konferenzaufzeichnungen

Und mit diesem Kommando erlauben Sie die Aufzeichnung wieder, aktivieren sie also:

```
Set-CsMeetingConfiguration -AllowConferenceRecording $True
```

Listing 9.12 Aktivieren von Konferenzaufzeichnungen

9.4 Lync-Clients

Lync Online-Anwendern steht eine Vielzahl unterschiedlicher Clients zur Verfügung. In diesem Abschnitt stelle ich diese kurz vor.

9.4.1 Lync 2013-Client

Der umfangreichste Client ist der Lync 2013-Client (siehe Abbildung 9.22). Er ist Bestandteil der folgenden Lizenzen (über das darin enthaltene Office 365 ProPlus):

- E3
- E4

Damit fehlt er bei Office 365 Business Essentials und Premium, E1 sowie bei Lync Online Plan 1 und 2 sowie bei den K(iosk)-Lizenzen. Mit Ausnahme der K-Lizenzen sind sie zwar auch mit dem Lync 2013-Client kompatibel, enthalten den Client selbst aber nicht. Hier müssen Sie mit dem Lync Basic 2013-Client vorliebnehmen (siehe Abschnitt 9.4.3, »Lync Basic 2013 und Lync Web App-Client«). Beim Basic-Client stehen dann OneNote-Besprechungsnotizen, Aufzeichnungen und Kalenderfunktionen nicht zur Verfügung.

Installation

Der Lync 2013-Client wird zusammen mit dem Office-Paket installiert (siehe Abschnitt 5.1, »Welches Office-Paket?«).

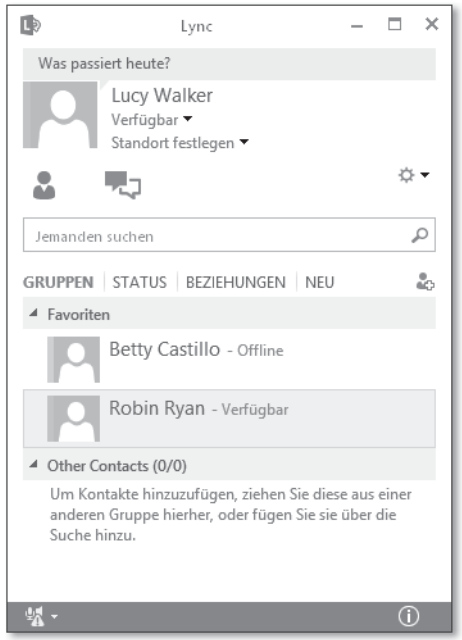

Abbildung 9.22 Lync 2013-Client

Anwendung

Nach der Anmeldung am Client erscheint ein Fenster mit der anfänglich leeren Kontaktliste. Über das Suchfeld können Sie dort bis zu 250 Kontakte eintragen. Diese können aus der eigenen Umgebung, dem Domänenverbund und von Skype (sofern die Anwender dort Microsoft-Konten verwenden) stammen. Um einen Lync-Anwender zur Kontaktliste hinzufügen, geben Sie Ihre SIP-Adresse ein. Im Normalfall ist diese identisch mit der E-Mail-Adresse.

Um im Lync-Client einen Skype-Anwender zu den Kontakten hinzuzufügen, wählen Sie den Befehl Neuer Kontakt • Externen Kontakt hinzufügen • Skype (siehe Abbildung 9.23).

Sollte der Benutzername des Microsoft-Kontos auf die Domänen *live.com*, *hotmail.com* oder *outlook.com* lauten, geben Sie den Benutzernamen direkt ein. Bei anderen Domänen ist jedoch ein bestimmtes Format erforderlich:

```
Benutzer(Domänenname)@msn.com
```

Heißt der Benutzername beispielsweise *lucy@beispielag.de*, müssen Sie Folgendes eingeben:

```
lucy(beispielag.de)@msn.com
```

Im Skype-Client geben Sie dagegen die SIP-Adresse des Lync-Anwenders ein.

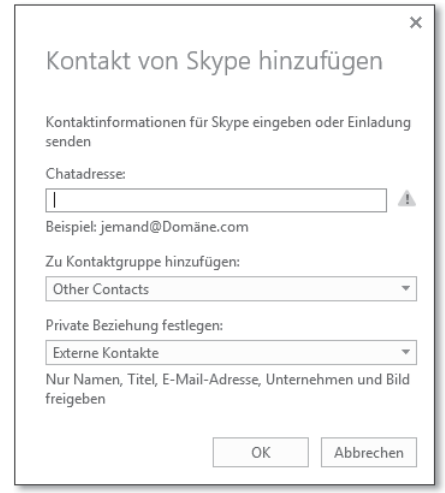

Abbildung 9.23 Skype-Benutzer hinzufügen

Eine Ad-hoc-Besprechung starten Sie nach einem Doppelklick auf einen Eintrag der Kontaktliste (siehe Abbildung 9.24). Das dann erscheinende Fenster dient zunächst dem Chat.

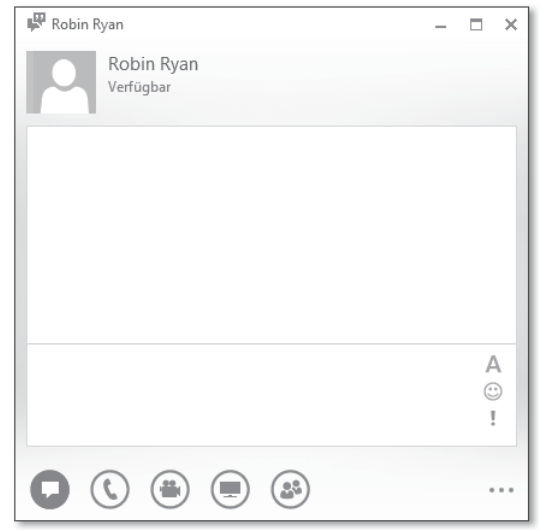

Abbildung 9.24 Besprechungsfenster

Von hier aus können Sie über die Symbole am unteren Fensterrand eine Telefon- oder Videokonferenz beginnen, über das Freigabesymbol Anwendungen freigeben und Dateien hochladen und über das Teilnehmersymbol weitere Teilnehmer zur Besprechung hinzufügen. Der spannendste Punkt dabei ist aber die Freigabe. Tabelle 9.5 zeigt eine Übersicht, was freigegeben werden kann.

Option	Bedeutung
Monitor	Der komplette Desktop eines oder beider Monitore wird an alle Besprechungsteilnehmer übertragen. Die Steuerung des Desktops kann an andere Teilnehmer übergeben werden (siehe Abbildung 9.25).
Programm	Die Darstellung einer beliebigen, bereits gestarteten Anwendung wird an alle Besprechungsteilnehmer übertragen. Auch hier kann die Steuerung an andere Teilnehmer übergeben werden.
PowerPoint	Eine PowerPoint-Präsentation wird an alle Besprechungsteilnehmer übertragen. Dabei werden auch Animationen ausgeführt. Der Präsentierende kann auf den Folien Markierungen setzen.
Whiteboard	Ein Whiteboard wird mit allen Besprechungsteilnehmern geteilt. Alle Teilnehmer können parallel auf dem Whiteboard Skizzen eintragen.
Umfrage	Eine neue Umfrage mit bis zu sieben möglichen Antworten wird an alle Teilnehmer übertragen. Die Ergebnisse können öffentlich sein oder geheim gehalten werden (siehe Abbildung 9.26).

Tabelle 9.5 Freigabeoptionen

Abbildung 9.25 Desktopfreigabe bei einem Besprechungsteilnehmer

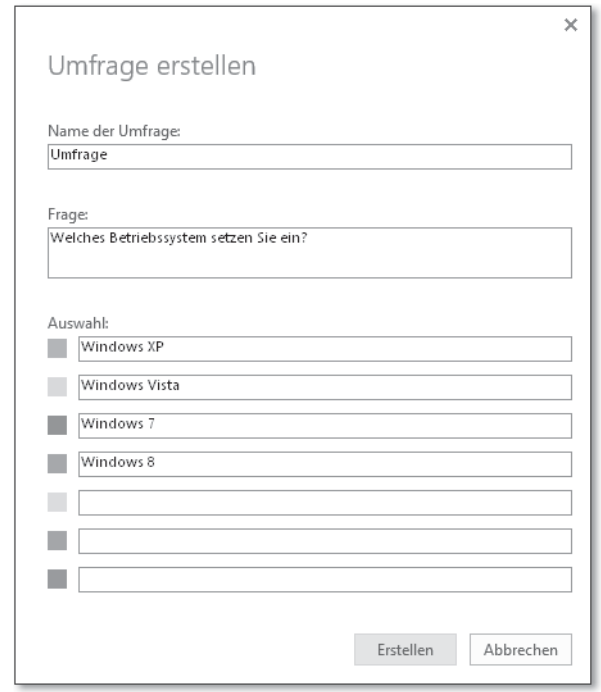

Abbildung 9.26 Umfrage

Konferenzen können Sie auch aufzeichnen und später wieder abspielen. Dabei werden Audio, Video, Sofortnachrichten, die Anwendungsfreigabe, PowerPoint-Präsentationen, das Whiteboard und Umfragen berücksichtigt. Wählen Sie zum Aufzeichnen im Kontextmenü (Aufruf über das Symbol mit den drei Punkten) den Befehl Aufzeichnung beginnen. Aufgezeichnete Konferenzen können Sie dann im Kontextmenü über Aufzeichnungen verwalten wieder abspielen (siehe Abbildung 9.27).

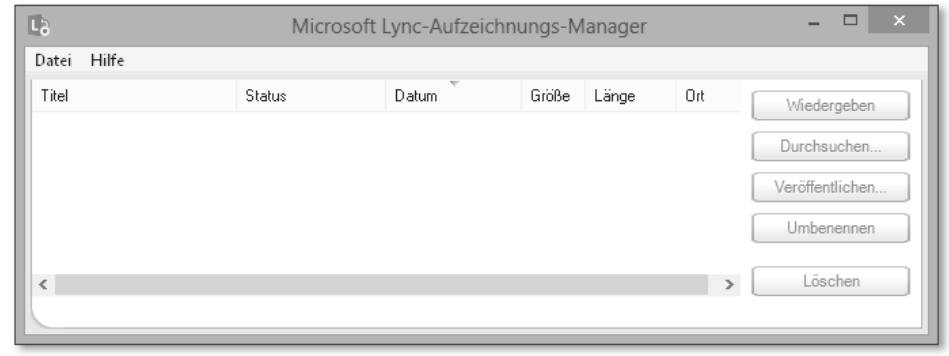

Abbildung 9.27 Aufzeichnungs-Manager

9.4.2 Lync Windows Store-App

Auch für die neue Oberfläche Modern UI von Windows 8 und Windows RT gibt es von Microsoft einen besonderen Lync-Client, der insbesondere für die Fingerbedienung ausgelegt ist (siehe Abbildung 9.28).

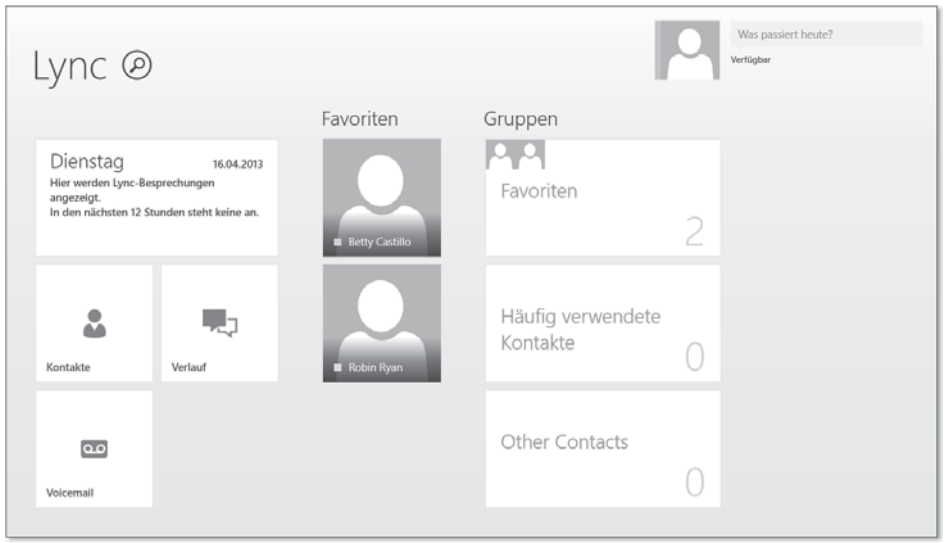

Abbildung 9.28 Lync Windows Store-App

Sie finden ihn im Windows Store unter folgender URL: *http://apps.microsoft.com/windows/de-de/app/lync/ba4b9485-8712-41ff-a9ea-6243a3e07682*

Der Lync-Client bietet Ihnen Zugriff auf Ihre Kontaktliste, die Sie auch modifizieren können. Außerdem sind Chat, Audio- und Videokonferenzen sowie das Darstellen der Anwendungs- und Desktopfreigabe des Kommunikationspartners möglich.

9.4.3 Lync Basic 2013 und Lync Web App-Client

Die Clients *Lync Basic 2013* und *Lync Web App* sind insbesondere für Anwender gedacht, die nicht über den Lync 2013-Client verfügen, weil sie sich beispielsweise zum Zeitpunkt der Konferenz nicht an ihrem regulären Arbeitsplatz befinden. Auch Gäste können damit an Ihren Konferenzen teilnehmen, benötigen also keinen Zugang zu Ihrer Office 365-Umgebung. Beide Clients sind kostenfrei erhältlich.

Lync Basic 2013 ist auch für Benutzer mit den Lizenzen Office 365 Business Essentials und Premium, E1 sowie Lync Online Plan 1 und 2 gedacht, denen der voll funktionsumfängliche Lync 2013-Client nicht zur Verfügung steht.

Abbildung 9.29 und Abbildung 9.30 zeigen die Oberflächen der beiden Clients.

Abbildung 9.29 Lync Basic 2013

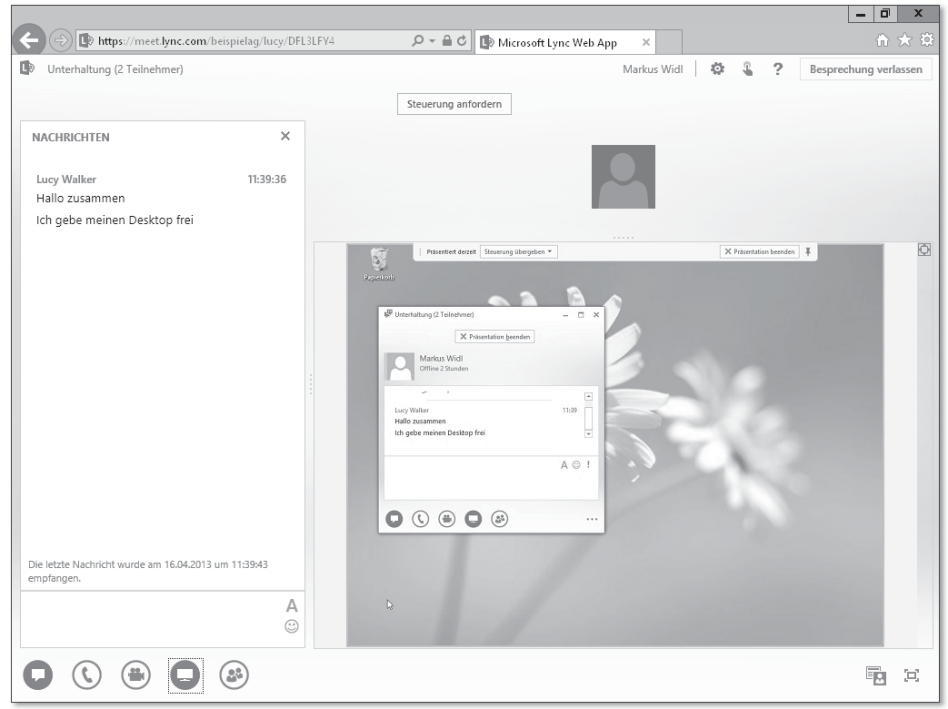

Abbildung 9.30 Lync Web App

Tabelle 9.6 vergleicht die beiden Clients miteinander.

Funktion	Lync Basic 2013	Lync Web App
kostenfrei erhältlich	ja	ja
lokale Installation erforderlich	ja	nein
Status veröffentlichen und anzeigen	ja	nein
Kontaktliste anzeigen und ändern	ja	nein
Chatunterhaltung mit einem Kontakt initiieren	ja	nein
mehrere Unterhaltungen in einem einzigen Fenster	ja	nein
Audio bei Konferenzen	ja	ja (mit Plug-in)
Video bei Konferenzen	ja	ja (mit Plug-in)
Desktop- und Anwendungs-freigabe	ja	ja (mit Plug-in)
PowerPoint vorführen	ja	ja
Whiteboard	ja	ja
Dateiupload	ja	ja
Besprechung einleiten	ja	nein
Anrufe initiieren	ja (zu Lync-Client)	nein

Tabelle 9.6 Vergleich Lync Basic 2013 und Lync Web App

Bei der Lync Web App entfällt zwar eine separate Clientinstallation, da die Ausführung im Browser erfolgt, doch für die volle Funktionalität (inklusive Audio, Video, Anwendungsfreigabe) ist die (automatische) Installation eines ActiveX-Plug-ins unter Windows erforderlich. Auf Mac OS X-Geräten ist das Plug-in dagegen nicht erforderlich. Tabelle 9.7 gibt Auskunft, was genau unterstützt wird.

Zur Verwendung des Lync Basic 2013-Clients benötigen Sie Windows 7 SP1 oder Windows 8. Die Installationspakete erhalten Sie unter folgenden URLs:

- 32 Bit: *www.microsoft.com/de-de/download/details.aspx?id=35451*
- 64 Bit: *www.microsoft.com/de-de/download/details.aspx?id=35450*

Betriebssystem	Audio, Video, Anwendungsfreigabe	IE 11 32 Bit	IE 11 64 Bit	IE 10 32 Bit	IE 10 64 Bit	IE 9 32 Bit	IE 9 64 Bit	IE 8 32 Bit	IE 8 64 Bit	Firefox 12.x 32 Bit	Safari 5.x 64 Bit	Chrome 18.x 32 Bit
Windows 8.1	ja	ja	ja	–	–	–	–	–	–	ja	–	ja
Windows 8 (nicht RT)	nein	–	–	ja	ja	–	–	–	–	ja	–	ja
Windows 7 SP1	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja	nein	ja
Windows Vista SP2	nein	–	–	ja	nein	ja	nein	ja	nein	ja	nein	ja
Windows XP SP3	nein	–	–	–	–	–	–	ja	nein	ja	nein	ja
Mac OS X	ja	–	–	–	–	–	–	–	–	ja	ja	ja

Tabelle 9.7 Unterstützte Betriebssystem-/Browserkombinationen

Anwendung

Wollen Sie mit einem der beiden Clients an einer Konferenz teilnehmen, klicken Sie beispielsweise im Outlook-Kalendereintrag auf den Link An Lync-Besprechung teilnehmen (siehe Abbildung 9.31).

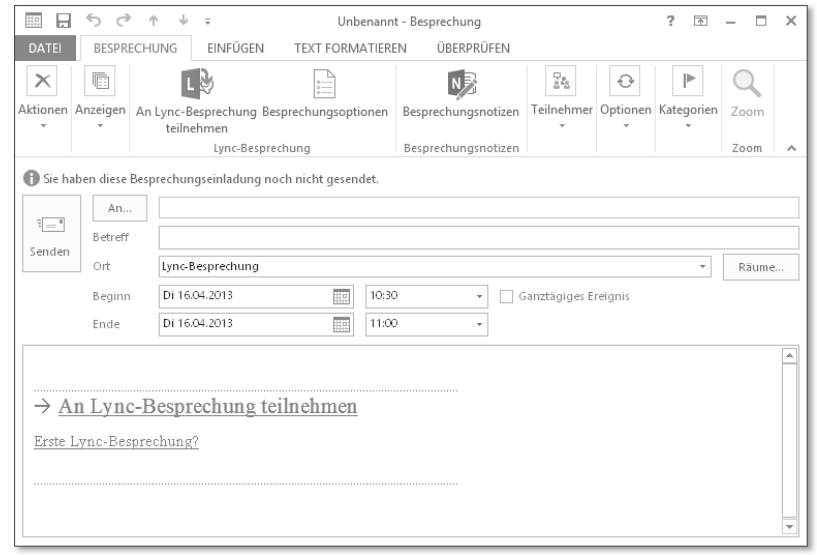

Abbildung 9.31 Kalendereintrag für eine Online-Besprechung

Wenn kein Lync-Client installiert ist, gelangen Sie zu einer Website, die automatisch die Lync Web App startet.

[»] Wollen Sie die Lync Web App nutzen, obwohl ein Lync-Client installiert ist, hängen Sie einfach an die Besprechungs-URL den Parameter `?SL=1` an. Damit wird die Arbeit mit der Lync Web App erzwungen.

9.4.4 Mobile Lync-Clients

Microsoft stellt aktuelle Lync-Clients für Windows Phone 8, iOS 6 und Android ab 4.0 kostenfrei bereit.

Tabelle 9.8 vergleicht wichtige Features der mobilen Clients mit dem Lync 2013-Client.

Zur Verwendung der mobilen Lync-Clients mit einer eigenen Domäne (also nicht **.onmicrosoft.com*) ist es erforderlich, dass Sie die beiden CNAME-Einträge aus Tabelle 9.9 in Ihrer DNS-Konfiguration eingetragen haben.

Überprüfen Sie das, um Probleme beim Anmelden zu vermeiden.

Feature	Lync 2013	Windows Phone	iPhone	iPad	Android
Pushbenachrichtigungen	nein	ja	nein	nein	nicht erforderlich (Anwendung läuft im Hintergrund)
Anwesenheitsstatus	ja	ja	ja	ja	ja
Kontaktliste	ja	ja	ja	ja	ja
Anpassung Kontaktliste	ja	nein	nein	nein	nein
Kontaktgruppen	ja	ja	ja	ja	ja
Gruppenverwaltung	ja	nein	nein	nein	nein

Tabelle 9.8 Vergleich mobile Lync-Clients

Feature	Lync 2013	Windows Phone	iPhone	iPad	Android
Suche im Unternehmensadressbuch und in der Kontaktliste	ja	ja	ja	ja	ja
Chat (Instant Messaging)	ja	ja	ja	ja	ja
Vibrationsbenachrichtigung bei eingehender Sofortnachricht	nein	ja	ja	ja	ja
Videokonferenz	ja	ja	ja	ja	ja
Audiokonferenz	ja	ja	ja	ja	ja
Freigabe von Desktop und Anwendungen, PowerPoint-Präsentationen	ja	nein	nein	nur Anzeige	nein

Tabelle 9.8 Vergleich mobile Lync-Clients (Forts.)

Hostname	Verweist auf	Gültigkeitsdauer
sip.DOMÄNE	*sipdir.online.lync.com*	1 Stunde
lyncdiscover.DOMÄNE	*webdir.online.lync.com*	1 Stunde

Tabelle 9.9 CNAME-Einträge für Lync

Windows Phone-Client

Auch für Windows Phone 8 gibt es einen eigenen Lync-Client. Diesen können Sie kostenfrei im *Marketplace* herunterladen: *www.windowsphone.com/en-us/store/app/lync-2013/d85d8a57-0f61-4ff3-a0f4-444e131d8491*

Beim ersten Start der App können Sie auswählen, ob Sie über Pushbenachrichtigungen über eintreffende Nachrichten informiert werden wollen.

Nach der Anmeldung haben Sie Zugriff auf die folgenden Bereiche:

- KONTAKTE
  Der Bereich enthält die Gruppen mit Ihren Lync-Kontakten samt deren Anwesenheitsstatus. Von dieser Liste aus starten Sie auch eine Sofortnachrichtenkonferenz, rufen den Kontakt an (nicht mit Lync Online) oder senden ihm eine E-Mail (siehe Abbildung 9.32).

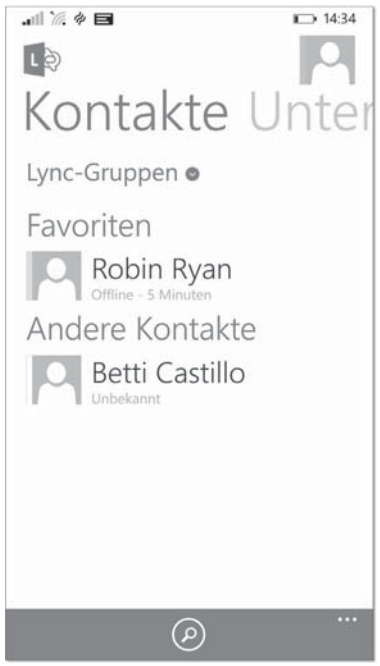

Abbildung 9.32 Kontaktverwaltung im Lync-Client von Windows Phone

- UNTERHALTUNGEN
  eine Aufzeichnung der zuletzt geführten Sofortnachrichtenkonferenzen
- BESPRECHUNGEN
  eine Liste der aktuellen Besprechungen
- EIGENE INFOS (Klick auf das Anwendersymbol)
  zur Änderung Ihres Status und zum Hinterlegen einer allgemeinen Mitteilung (siehe Abbildung 9.33)

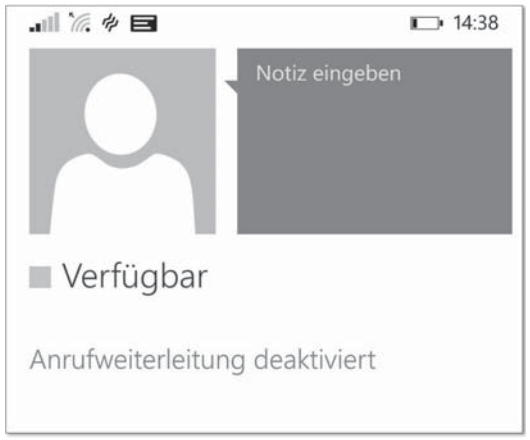

Abbildung 9.33 Statusänderung im Windows Phone-Client

iOS-Client

Für iOS-Geräte gibt es sogar zwei unterschiedliche Clients, und zwar für das iPhone bzw. den iPod sowie für das iPad. Beide sind im *iTunes Store* kostenfrei erhältlich und setzen mindestens Version 7 von iOS voraus:

- iPhone/iPod: *https://itunes.apple.com/DE/app/id605841731*
- iPad: *https://itunes.apple.com/DE/app/id605608899*

Die iPad-Variante nutzt dabei den größeren Bildschirm aus (siehe Abbildung 9.34).

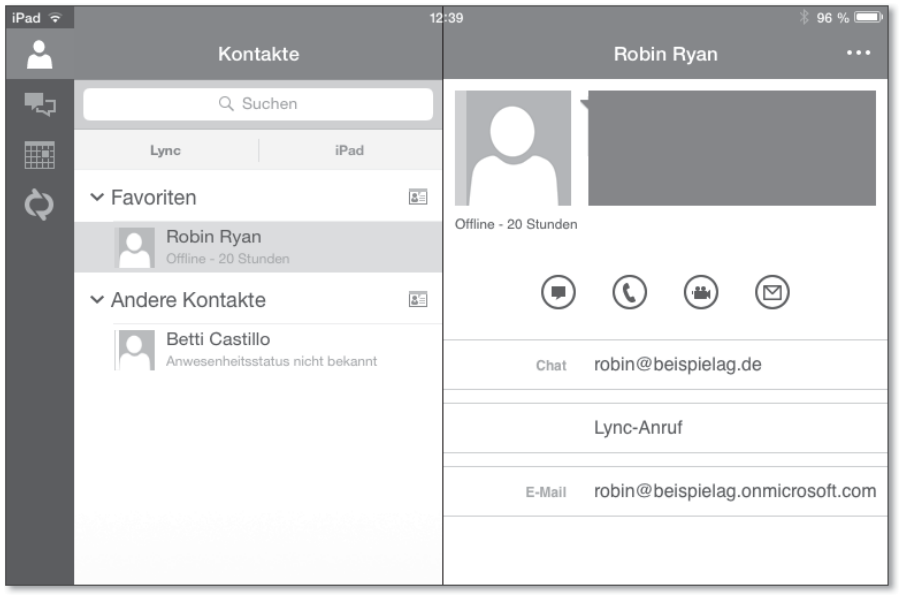

Abbildung 9.34 Lync auf dem iPad

Android-Client

Auch für Android-basierte Geräte (ab Version 4.0) gibt es einen eigenen Lync-Client, den Sie im *Play Store* unter *https://play.google.com/store/apps/details?id=com.microsoft.office.lync15* herunterladen können.

Abbildung 9.35 zeigt den Client in Aktion.

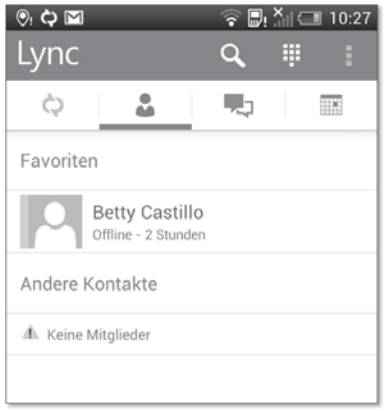

Abbildung 9.35 Lync auf einem Android-Smartphone

9.4.5 Lync-Client für Mac OS X

Auch für Mac OS X ab Version 10.5.8 ist ein Lync-Client verfügbar. Er trägt den Namen Lync for Mac 2011 (siehe Abbildung 9.36). Besuchen Sie den Downloadbereich von Office 365, können Sie ihn herunterladen – vorausgesetzt, Sie besuchen die Seite von einem Mac aus: *https://portal.office.com/OLS/MySoftware.aspx*

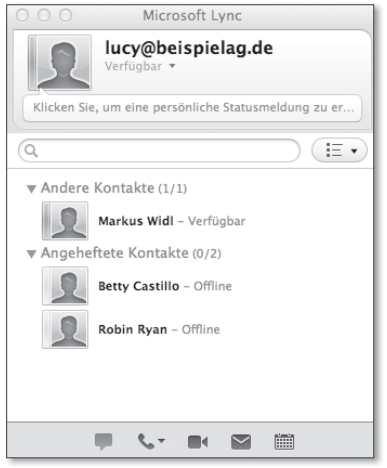

Abbildung 9.36 Lync-Client für Mac OS X

Konfiguration

Damit die Anmeldung vom Lync-Client aus durchgeführt werden kann, ist folgende Konfiguration erforderlich:

1. Starten Sie den Lync-Client.
2. Klicken Sie auf ERWEITERT.
3. Die Option KERBEROS VERWENDEN darf nicht ausgewählt sein.
4. Die VERBINDUNGSEINSTELLUNGEN müssen manuell konfiguriert werden (siehe Abbildung 9.37):
   - INTERNER SERVERNAME: `sipdir.online.lync.com:443`
   - EXTERNER SERVERNAME: `sipdir.online.lync.com:443`

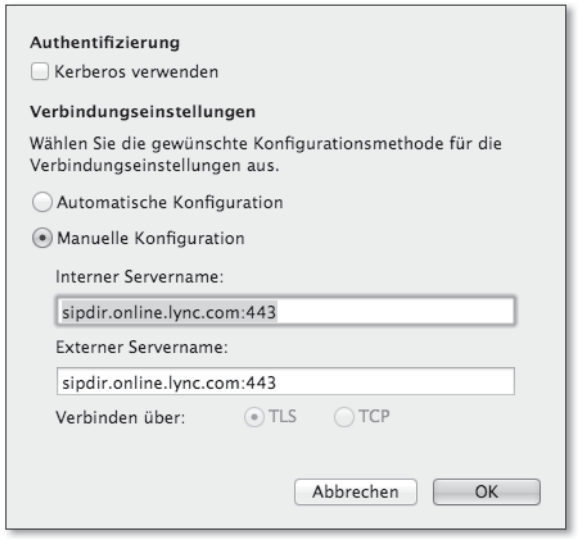

Abbildung 9.37 Konfiguration

Anmeldung

Im Anmeldefenster des Lync-Clients geben Sie unter E-MAIL-ADRESSE ebendiese ein. Als BENUTZER-ID verwenden Sie Ihren Office 365-Benutzernamen mit dem zugehörigen Kennwort.

Anwendung

Der Lync-Client unterstützt folgende Funktionalitäten:

- Lync-Kontaktverwaltung
- Anzeige des Anwesenheitsstatus
- Chat

- Audio- und Videokonferenzen
- Anzeige von PowerPoint-Präsentationen anderer Konferenzteilnehmer
- Freigabe des Desktops an andere Konferenzteilnehmer
- Dateiübertragung an alle Konferenzteilnehmer
- Einladungen per E-Mail versenden
- Konferenzen in Outlook planen

Das Konferenzfenster sieht dabei aus wie in Abbildung 9.38 dargestellt.

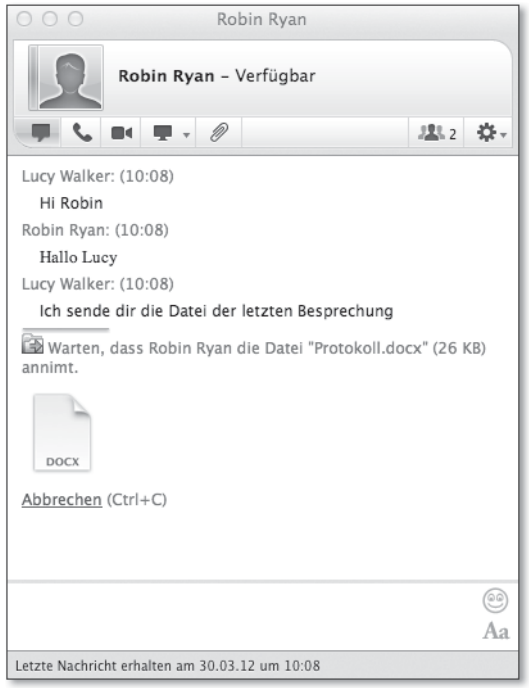

Abbildung 9.38 Lync-Konferenz auf Mac OS X

9.4.6 Problembehebung

Sollte es Probleme bei der Anmeldung mit einem Lync-Client geben, kann das viele Ursachen haben, beispielsweise eine blockierende Firewall, falsche Einträge im lokalen DNS etc. Um der Problemursache auf die Spur zu kommen, hilft möglicherweise das *Remote Connectivity Analyzer*-Tool, das auf einem lokalen Client ausgeführt wird (siehe Abbildung 9.39). Sie finden es unter folgender URL auf der Registerkarte Client:

http://testconnectivity.microsoft.com

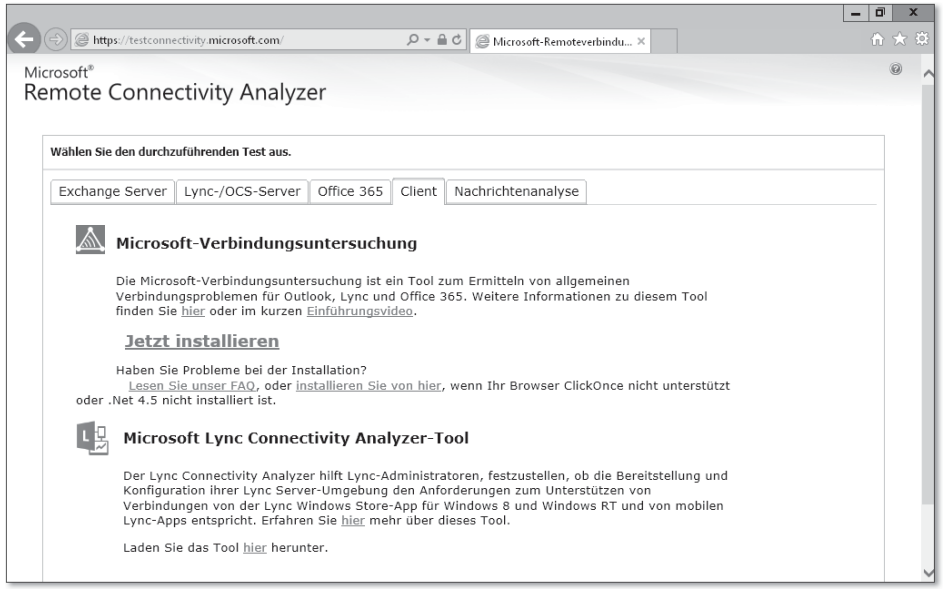

Abbildung 9.39 Remote Connectivity Analyzer-Tool

9.5 Telefonie

Vergleichen Sie die beiden Produkte Lync Online und Lync Server miteinander, finden Sie bei den Funktionsbereichen Chat, Anwesenheitsinformationen und Konferenzen eine hohe Übereinstimmung. Bei den Bereichen Sprache, Telefonanlagenfunktionen (*PBX = Private Branch Exchange*) und Administration sieht die Sache schon ganz anders aus: Hier hinkt Lync Online dem Lync Server stark hinterher. Beispielsweise sind die folgenden Funktionen nur beim Lync Server vorhanden:

- Telefonie in das »normale« Telefonnetz
- Anbindung an oder der Ersatz von Telefonanlagen
- Bandbreitenmanagement
- Integration mit Videosystemen

Vergleich mit Lync Server 2013

Einen detaillierten Vergleich zwischen Lync Server 2013 und Lync Online finden Sie in der Dienstbeschreibung unter folgender URL:

http://technet.microsoft.com/library/jj822172.aspx

Sind die fehlenden Funktionen für Sie unverzichtbar, bleibt nur die Einrichtung eines eigenen Lync Servers.

E4-Lizenz und Lync Server

Nachdem wir nun geklärt haben, dass Lync Online nur sehr eingeschränkte Telefoniefunktionen bietet, stellt sich die Frage: Wozu dient denn dann die *Lync Plus CAL*, die auf Marketingfolien gerne auch als »Sprachfunktionen« aufgeführt ist und die in der E4-Lizenz gegenüber der E3-Lizenz zusätzlich enthalten ist? Es handelt sich dabei um eine *CAL (Client Access License)* für den Lync Server, mit der Sie gegebenenfalls Kosten sparen, die Sie sonst bei der Lizenzierung der Benutzer des lokal vorhandenen Lync Servers hätten. Den Server selbst müssen Sie aber separat betreiben und lizenzieren.

9.6 So geht es weiter

In diesem Kapitel habe ich die Funktionalität von Lync Online beschrieben. Sie haben erfahren, wie die Administration vonstattengeht und welche Einschränkungen dabei bestehen. Außerdem haben Sie gesehen, wie die Konfiguration der verschiedenen Lync-Clients vorgenommen wird.

Weiter geht es im zehnten Kapitel mit der Verwaltung von Informationsrechten.