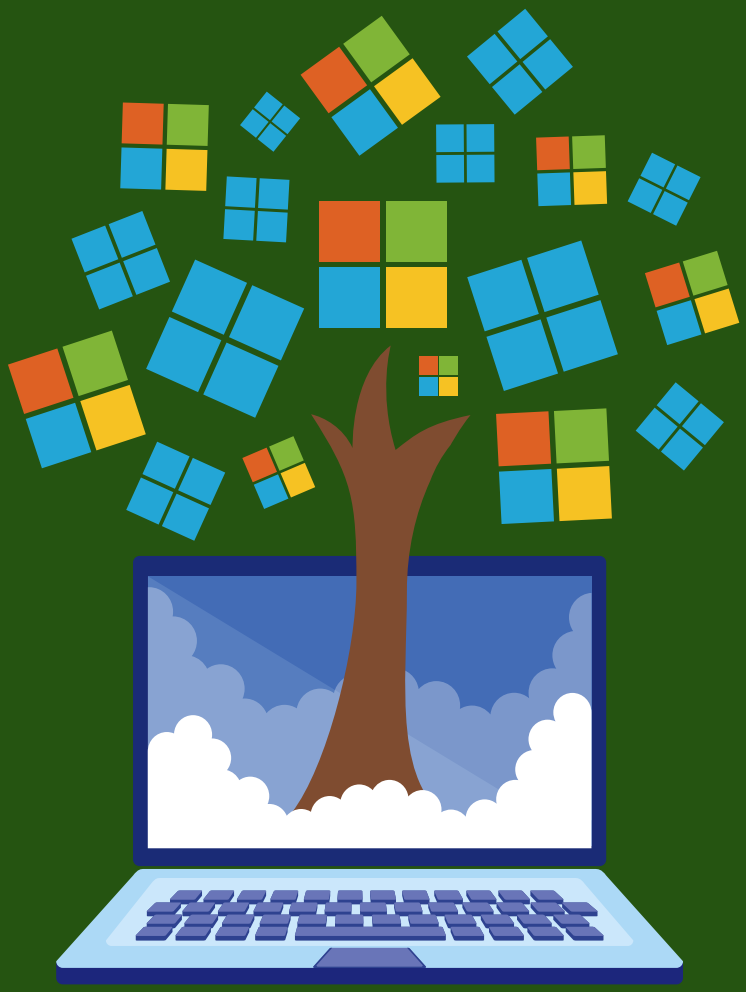
Grundlagen von Azure Active Directory und Azure-Diensten

# Ins Netz gezogen

**Frank Ully**

Der Identitätsdienst Azure Active Directory kontrolliert den Zugriff auf Microsofts Cloud-Dienste von Azure bis Microsoft 365. Er ist ein beliebtes Angriffsziel – und standardmäßig nicht gut gesichert.



Eine wachsende IT-Öffentlichkeit diskutierte in den vergangenen Jahren über die Sicherheit von On-Premises-Installationen des Verzeichnisdienstes Active Directory (AD) von Microsoft. Verglichen damit noch wenig Beachtung findet Azure Active Directory (Azure AD oder AAD), der zentrale Identitäts- und Zugangsverwaltungsdienst von Microsofts Cloud-Lösung Azure.

Einige Sicherheitsverantwortliche und ITler wissen womöglich nicht, wie zentral AAD für Microsofts Cloud ist: Selbst wenn man keine Azure-Dienste für Infrastructure as a Service (IaaS) wie virtuelle Maschinen oder Platform as a Service (PaaS) wie Speicherkonten (Storage) einsetzt, verfügt die eigene Organisation über ein Azure Active Directory, wenn sie ein Software-as-a-Service-Produkt (SaaS) aus dem Microsoft-365-Portfolio wie Teams oder Exchange Online nutzt oder ein anderes Microsoft-Angebot wie Dynamics 365 [1, 2].

Selbst unbemerkt kann ein Azure AD für die Organisation angelegt worden sein, wenn nur einer ihrer Mitarbeiter vor Mai 2018 eine Einladung zu einem von anderen genutzten Microsoft-Cloud-Dienst angenommen hat.

### X-TRACT

- Azure Active Directory (AAD) ist der Identitäts- und Zugriffsverwaltungsdienst der Microsoft-Cloud Azure.
- Jede Organisation, die Microsoft 365 oder andere Azure-Dienste für SaaS, PaaS oder IaaS einsetzt, verwendet diesen zentralen Dienst, oft ohne sich dessen bewusst zu sein.
- Trotz fast gleichlautender Namen sind Aufgaben, Konzepte und Funktionsweisen des klassischen Active Directory und des Azure Active Directory stark voneinander verschieden.
- Wie im On-Premises Active Directory sind im AAD die Standardeinstellungen auf Funktionalität ausgelegt und nicht auf Sicherheit. Das führt dazu, dass reguläre Benutzer im Azure Active Directory unerwartet viele Berechtigungen haben.

Ein AAD einer Organisation wird auch als Mandant bezeichnet, ebenfalls gebräuchlich ist die englische Bezeichnung Tenant, und ist das Äquivalent zur Gesamtstruktur (Forest) im klassischen AD. Mit einem Konto im AAD kann ein Mitarbeiter nicht nur seine Firmen-E-Mails abrufen, sondern sich bei Hybrid-Installationen am eigenen Laptop oder bei internen Anwendungen anmelden und im SharePoint Online eines Partnerunternehmens Dokumente einsehen. Dabei werden auf Wunsch Passwörter zwischen dem lokalen AD und Azure AD synchronisiert. AAD kann als Identitätsplattform für Anwendungen von Dritten dienen. Somit ist Single Sign-on (SSO) nicht nur für Microsoft-Dienste möglich.

Das macht das AAD für Angreifer attraktiv. Wenn ein Unternehmen hybrid arbeitet und eine Verbindung zwischen On-Premises AD und Azure AD hergestellt hat, ist für sie der Sprung aus einer kompromittierten Cloud-Instanz zur lokalen Installation möglich – und umgekehrt. Das zeigt die Supply-Chain-Attacke auf die Netzwerkmanagementplattform von SolarWinds im Jahr 2020. Damals wurden Eindringlinge beobachtet, die von einem kompromittierten Tenant eines Microsoft-Cloud-Partners über die delegierte Administration („Administrator im Auftrag von“ oder „Admin on Behalf Of“, AOBO) auf die Tenants von dessen Kunden überge-

sprungen sind (siehe ix.de/z646). Das kann man sich als Entsprechung zum Ausnutzen von Vertrauensstellungen zwischen Active Directory Forests vorstellen [3].

## Gleicher Name, andere Funktionen

Active Directory erschien zusammen mit Windows Server 2000 im Jahr 1999. Die Entwicklung von Azure startete 2008 als „Project Red Dog"; veröffentlicht wurde es 2010 als Windows Azure. 2014 änderte Microsoft den Namen in Microsoft Azure, um zu verdeutlichen, dass es mehr als nur Windows-Produkte abdeckt. Im selben Jahr wurden das Azure Active Directory (Azure AD) und der Azure Resource Manager (ARM) freigegeben; zu ihm später mehr. Azure AD ist als Identitätsdienst nur ein sehr kleiner – aber zentraler – Teil der Microsoft-Cloud.

Azure AD ist nicht einfach ein Active Directory, das in der Cloud gehostet wird. Es gibt keine Organisationseinheiten oder Gruppenrichtlinien, das Abfrageprotokoll LDAP und die Authentisierungsprotokolle Kerberos und Net-NTLM [4] werden nicht unterstützt. Damit ist AAD nicht direkt für herkömmliche On-Premises-Anwendungen geeignet. Es ist die Authentifizierungskomponente sowohl für die Dienstplattform Azure als auch für SaaS-Angebote wie Microsoft 365. Statt über Gruppenmitgliedschaften – man denke an die Gruppe der Domänenadmins – werden Rechte über Rollen vergeben. Die Vergleichstabelle stellt On-Premises und Azure Active Directory gegenüber. Microsoft pflegt eine umfangreiche Dokumentation, die die beiden Dienste vergleicht (siehe ix.de/z646).

Als ob Microsoft wegen der Unterschiede zum klassischen AD mit der Bezeichnung Azure Active Directory nicht schon genug Verwirrung gestiftet hätte – für die Cloud-Variante wäre „Azure Identity Services" eine treffendere Benennung gewesen –, gibt es weitere Azure-Dienste mit „Active Directory" im Namen.

Azure AD B2C (Business to Consumer) ist ein Dienst, der in einem Azure-Abonnement aktiviert werden kann, um Identitäten für Kunden bereitzustellen, die sich damit in Webanwendungen des Unternehmens anmelden können. B2C-Konten sind völlig separat vom AAD-Mandanten der Organisation.

Darüber hinaus stellen Azure Active Directory Domain Services (Azure AD DS) eine klassische AD-Domäne mit Controllern in Azure bereit, die Microsoft verwaltet und in AAD integriert. Mit ihr kann man virtuelle Maschinen und Anwendungen in die Cloud einbinden, die noch angewiesen sind auf klassische Techniken, die in der Cloud nativ nicht mehr vorkommen, zum Beispiel Gruppenrichtlinien oder Kerberos-Authentisierung. Schließlich können Admins über virtuelle Maschinen mit Windows-Servern, die sie als Domänencontroller einrichten, selbst mit Azure-IaaS-Diensten ein klassisches On-Prem AD nachbauen – ob das ein kluger Weg ist, sei dahingestellt.

## Architektur: AAD, ARM, Microsoft 365

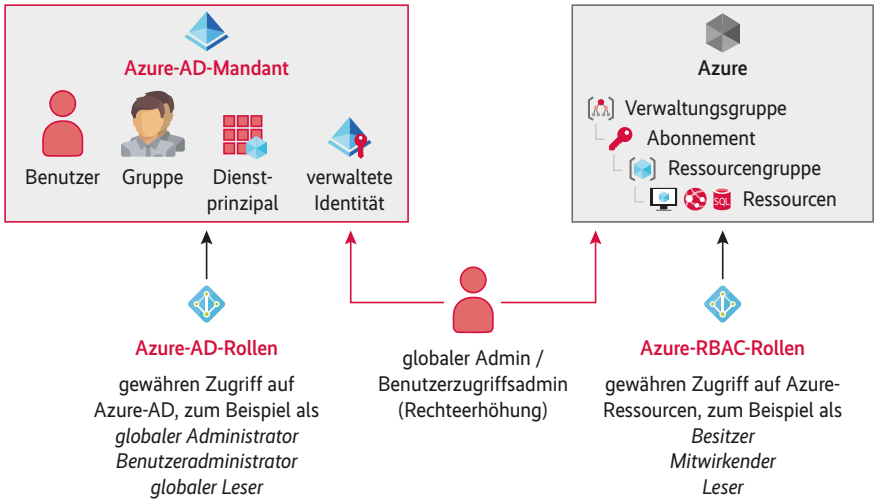
Ein AAD-Tenant enthält alle Benutzer, Gruppen, Geräte und Anwendungen der Organisation. Automatisch erstellt wird er, wenn ein Unternehmen ein Abo für einen Cloud-Dienst wie Microsoft 365 oder Azure abschließt. Er repräsentiert die Organisation, ist die Basis, um ihre Identitäten und Ressourcen für die Microsoft-Cloud zu verwalten und dient als Sicherheitsgrenze.

Auf AAD-Ebene gibt es ungefähr 30 eingebaute Rollen wie globaler Leser, Sicherheitsoperator, globaler Administrator und weitere Adminrollen, die sich auf die Verwaltung des Identitätsdienstes beziehen. Der initiale Mandantenname ist <tenant>.onmicrosoft.com. Ein Eigentümer kann individuelle Domänen damit verbinden, deren Besitz er nachweisen kann. Eine Organisation kann mehrere Mandanten verwalten; das ist manchmal bei Tochtergesellschaften der Fall. Diese Mandanten sind voneinander getrennt: Der Zugriff auf einen Mandanten gewährt zunächst keinerlei Rechte in einem anderen, analog zu unterschiedlichen Gesamtstrukturen ohne Vertrauensstellungen im On-Prem AD.

Auf der anderen Seite steht ein Azure-Abonnement, in dem PaaS- oder IaaS-Ressourcen wie virtuelle Maschinen oder Datenbanken laufen. Ein Azure-Abo hat eine Vertrauensbeziehung zu Azure AD: Jedes Abo ist genau einem AAD-Tenant zugeordnet; demselben Tenant können mehrere Abonnements vertrauen. Das Konto, das ein Azure-Abonnement abschließt, wird als dessen Besitzer eingetragen. Abonnements werden oft nach Verwendungszweck unterteilt, zum Beispiel ein Abo für produktive Webanwendungen,

**Vergleich zwischen lokalem Active Directory und Azure Active Directory**

| | On-Premises Active Directory | Azure Active Directory |
|---|---|---|
| Funktion | Domänendienste auf Domänencontrollern | Identitätsdienst in der Azure-Cloud |
| Sicherheitsgrenze | Gesamtstruktur (Forest) | Mandant (Tenant) |
| Abruf von Informationen | LDAP | REST-Schnittstellen, Microsoft Graph |
| Authentisierungsprotokolle | Net-NTLM, Kerberos | OAuth2 und OpenID Connect, SAML und WS-Federation |
| Verwaltungsprotokolle | meist Remote Desktop Protocol (RDP) oder PowerShell Remoting | Management-APIs |
| Berechtigungskonzept | granulare Delegierung über Zugriffskontrolllisten (Access Control Lists, ACL) | meist vordefinierte Rollen; separate Rollen für AAD und Azure |
| Rechtevergabe | Sicherheitsgruppen mit delegierten Berechtigungen | Azure-AD-Rollen in Bezug auf AAD; Azure RBAC (Role-based Access Control) in Bezug auf Azure |
| Clienteinbindung | Windows-Client der Domäne hinzufügen | Azure-AD- oder Hybrid-Azure-AD-eingebundene Windows-Geräte; außerdem Mobile Device Management (MDM) für Android, iOS und macOS |
| Geräteverwaltung | Gruppenrichtlinien (GPOs) | Richtlinien im Microsoft Endpoint Manager, Microsoft Intune |
| Servereinbindung | Server der Domäne hinzufügen | nicht direkt in AAD; beispielsweise über den PaaS-Dienst Azure Active Directory Domain Services (Azure AD DS) |
| Dienstbereitstellung | Server | Anwendungen |
| Dienstauthentisierung | Dienstkonto | Dienstprinzipal (Unternehmensanwendung), verwaltete Identität |
| Einbindung von Externen | Vertrauensstellungen (Trusts) | Gäste, B2B-Benutzer |
| Unterstützung für SaaS-Anwendungen | nicht im klassischen AD, nur mit Active Directory Federation Services (AD FS) | SaaS-Anwendungen mit OAuth2/OpenID Connect, SAML und WS-Federation; Kundenkonten in Azure AD B2C |
| Echtzeit-Zugriffsentscheidungen | – | Richtlinien für bedingten Zugriff wie Mehr-Faktor-Authentisierung (MFA), auch risikobasierter bedingter Zugriff |




**Der Zusammenhang zwischen Azure-AD- und Azure-RBAC-Rollen ist äußerst komplex. Eine Rolle im Azure AD bedeutet nicht, dass man diese Rolle auch in Azure hat. In beiden Umgebungen existieren unterschiedliche Rollen, gemeinsame Definitionen gibt es nicht (Abb. 1).**

ein anderes für die Entwicklung von Web-Apps.

## Rollenbasierte Verwaltung der Ressourcen

Ressourcen in Azure erstellt, verändert und löscht der Azure Resource Manager (ARM). Hier gibt es ein eigenständiges Berechtigungsmodell mit mehr als 120 integrierten Rollen, die rollenbasierte Zugriffssteuerung (Azure Role-based Access Control, Azure RBAC). Basisrollen sind dabei:

- Besitzer (Owner) mit vollen Rechten auf alle Ressourcen und der Möglichkeit, den Zugriff weiter zu delegieren;
- Mitwirkender (Contributor), der ebenso wie der Besitzer selbst alle Rechte hat, aber keine Berechtigungen ändern darf;
- Leser (Reader), der nur Attribute von Ressourcen anzeigen kann.

Andere Mitwirkenden- oder Leserrollen beziehen sich auf spezifische Azure-Ressourcen wie virtuelle Maschinen oder Speicherkonten. Schließlich verwaltet der Benutzerzugriffsadministrator den Zugriff auf Azure-Ressourcen. Selbst wenn er nicht Besitzer einer Ressource ist, kann er Berechtigungen an andere Konten delegieren. RBAC in Azure ermöglicht benutzerdefinierte Rollen, aber viele Unternehmen verlassen sich auf die integrierten Rollen.

Azure-RBAC-Rollen können auf vier Ebenen vergebenen werden, je nach Anwendungsbereich (Scope): Verwaltungsgruppe, Abonnement, Ressourcengruppen und einzelne Ressourcen. Verwaltungsgruppen dienen dazu, mehrere Abonnements zu gruppieren, und können verschachtelt sein. An ihrer Spitze steht die optionale Stammgruppe. Einstellungen, die auf diese Verwaltungsgruppe angewendet werden, wirken sich auf jede darunterliegende Ebene und letztlich auf alle untergeordneten Ressourcen aus.

## Geerbte Berechtigungen

Oft bündelt ein Unternehmen in einer Verwaltungsgruppe alle produktiven oder Entwicklungsressourcen, etwa mehrere produktive Abos für unterschiedliche Geschäftszweige. Ressourcengruppen fassen zusammengehörige Ressourcen zusammen, typischerweise alle Dienste, die für den Betrieb einer einzelnen Anwendung notwendig sind. Auf einer oberen Ebene zugeordnete Rollen werden vererbt und gelten für alle darunterliegenden Elemente: Ein Mitwirkender für die Ressourcengruppe hat Mitwirkenden-Zugriff auf jede Ressource innerhalb der Gruppe.

Auf derselben Ebene wie das AAD stehen SaaS-Angebote unter dem Microsoft-365-Schirm wie Exchange, SharePoint Online oder Teams. Deren Anwendungen werden von Microsoft quasi in seinem eigenen Azure-Abo gehostet; die einzelne Kundenorganisation nutzt ihren AAD-Tenant, um ihren Zugriff darauf zu verwalten. Ein Microsoft-365-Abo wird mit einem AAD-Mandanten verknüpft, anwendungsbezogene administrative Rollen wie der SharePoint-Administrator werden in AAD zugewiesen.

Die rollenbasierten Zugriffskontrollsysteme von AAD und ARM sind getrennt (siehe Abbildung 1): Eine Rolle in Azure AD bedeutet nicht, dass man diese Rolle in Azure hat. In beiden Umgebungen sind die Rollen unterschiedlich und haben keine gemeinsamen Rollendefinitionen. Eine Rollendefinition beschreibt, welche Aktion ausgeführt werden darf oder verboten ist und auf welchem Scope sie gelten kann. Ein Sicherheitsprinzipal verfügt also über die Rechte gemäß Rollendefinition auf der zugewiesenen Ebene, bei Azure-RBAC-Rollen beispielsweise auf einem Abonnement.

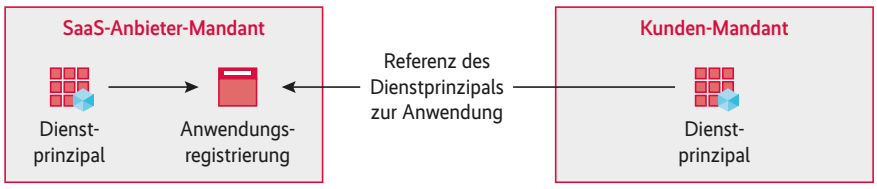
## Benutzer, Gruppen und Dienstprinzipale

Ein Sicherheitsprinzipal ist eine Identität, der Berechtigungen zugewiesen werden. Davon gibt es im AAD grob drei: Benutzer, Gruppen und Dienstprinzipale.

Benutzer können in Azure verwaltet oder mit einem lokalen AD synchronisiert werden. Sie werden über ihren Benutzerprinzipalnamen (User Principal Name, UPN) eindeutig identifiziert, zum Beispiel peter.pan@2consult.onmicrosoft.com. Außerdem kann ein Mandant Gäste beherbergen, die in anderen Mandanten verwalten werden, erkennbar an der Zeichenkette #EXT#.

In Gruppen können Benutzer direkt ein Mitglied sein oder über Regeln Teil einer dynamischen Gruppe werden. Jede Gruppe hat mindestens einen Besitzer, der bearbeiten kann, wer darin Mitglied ist. Neben diesen Sicherheitsgruppen gibt es noch Microsoft-365-Gruppen, die ähnlich zu E-Mail-Verteilergruppen im klassischen AD sind.

Eine Azure-Anwendung ist eine Registrierung für eine Software, die dazu dient, Benutzern Funktionen bereitzustellen. Single-Tenant-Anwendungen werden für ein bestimmtes AAD registriert und sind nur in dem Mandanten verfügbar, in dem




**Mandantenfähige Anwendungen werden über Dienstprinzipale in den AADs der Kunden verwaltet (Abb. 2).**

sie registriert wurden. Mandantenfähige Anwendungen sind für die Nutzung in mehreren Tenants verfügbar. Ein gängiger Anwendungsfall ist eine Software-as-a-Service-Anwendung: Der SaaS-Anbieter registriert die App in seinem Mandanten.

## Ein Dienstprinzipal für jede Anwendung

Ein Dienstprinzipal (Service Principal) ist die Identität, die in den einzelnen Azure ADs für eine mandantenfähige Anwendung erstellt wird, damit sie auf dieses AAD oder auf Azure-Ressourcen zugreifen darf. Im Portal wird er als Unternehmensanwendung bezeichnet. Mehr-Mandanten-Anwendungen wie Microsoft-365-Apps erstellen in jedem Mandanten einen oder mehrere Dienstprinzipale, die dort die Anwendung repräsentieren (siehe Abbildung 2). Microsoft 365 besteht aus mehr als 200 Anwendungen im Microsoft-Tenant, das heißt, im Mandanten jedes Kunden gibt es ebenso viele Dienstprinzipale.

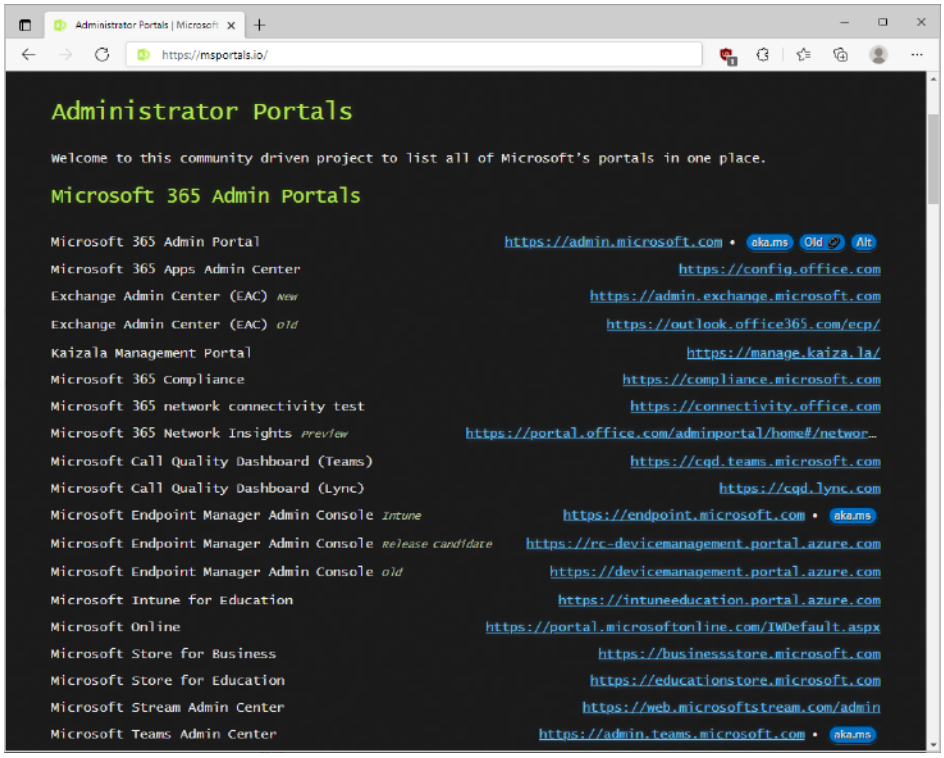
Dienstprinzipale können über ein Geheimnis – das entspricht einem Passwort – oder ein Zertifikat authentisiert werden. Eine verwaltete Identität (Managed Identity) für Azure-Ressourcen ist ein bestimmter Typ von verwaltetem Prinzipal, der an definierte Azure-Ressourcen angehängt werden kann, um zum Beispiel einer virtuellen Maschine Berechtigungen in AAD oder ARM zu erteilen. Anmeldeinformationen werden dabei automatisch gehandhabt.

Es gibt zwei Arten von Berechtigungen für Anwendungen und Dienstprinzipale: Anwendungsberechtigungen und delegierte Berechtigungen. Eine Anwendungsberechtigung kann eine App unmittelbar und jederzeit nutzen; ein Admin muss sie initial freigegeben. Dienstprinzipale, denen delegierte Berechtigungen zugewiesen sind, verkörpern die Berechtigungen des angemeldeten Benutzers. Einige delegierte Berechtigungen, beispielsweise die Freigabe der eigenen E-Mails, kann ein Benutzer selbst genehmigen – privilegierte Berechtigungen erfordern die Zustimmung eines Admins.

Damit eine Anwendung in AAD ein bestimmtes Recht hat, werden ihr beziehungsweise ihrem Dienstprinzipal diese Berechtigungen verliehen.

## Kritische Berechtigungen

Berechtigungen auf den Microsoft Graph und damit auf Azure AD haben die Struktur `{Objekt}.{Zugriff}.{Einschränkung}`. Beispiele sind `Directory.ReadWrite.All`, das volle Kontrolle über das AAD gewährt, oder das sprechend benannte `Mail.Send`. Die Einschränkung `All` bedeutet, dass die Anwendung diese Rechte selbst auf allen Ressourcen im jeweiligen AAD hat.




**Das Gemeinschaftsprojekt msportals.io bietet eine Übersicht über Microsoft-Portale (Abb. 3).**

Fehlt die Einschränkung wie im zweiten Beispiel, gilt die Berechtigung nur für die Ressourcen, die dem aktuellen Benutzer gehören. Kritische Microsoft-Graph-Berechtigungen sind etwa `AppRoleAssignment.ReadWrite.All`, `RoleManagement.ReadWrite.Directory` oder `DelegatedPermissionGrant.ReadWrite.All`, in Bezug auf Exchange Online `Exchange.ManageAsApp` oder `Mail.ReadWrite.All` (siehe ix.de/z646).

Ein Angreifer kann die Berechtigungen enumerieren. Hat er den Eigentümer einer Anwendung beziehungsweise eines Dienstprinzipals kompromittiert, kann er den Prinzipal übernehmen und mit dessen Rechten agieren – wie, schildert der folgende Artikel „Ins Netz gegangen“ ab Seite 50. Die Rolle Anwendungsadministrator kann gar die Anmeldeinformationen für alle Dienstprinzipale ändern.

Auch für Azure-Dienste gibt es Rollendefinitionen. Unterschieden wird zwischen Berechtigungen auf Management- und Datenebene; außerdem können Aktionen ausdrücklich verboten werden. Sie haben die Struktur

```
{Anbieter}.{Provider}/↵
        {Ressourcentyp}/{Aktion}
```

Zum Beispiel hat die RBAC-Rolle „Mitwirkender von virtuellen Computern“ die Berechtigung `Microsoft.Compute/virtualMachines/runCommand/action` und darf deswegen auf virtuellen Computern Skripte mit Systemrechten ausführen.

## Unzählige Portale und Kommandozeilenwerkzeuge

Häufiger Einstieg und für manche vielleicht die einzige Berührungsfläche mit den Cloud-Portalen von Microsoft ist das Microsoft-365-Admin-Portal unter admin.microsoft.com für SaaS-Admins sowie das Azure-Portal unter portal.azure.com. Daneben stellt Microsoft Dutzende weitere Weboberflächen bereit, die oft eine spezielle Teilmenge der großen Adminportale bieten und sich untereinander verlinken. Das AAD hat eine eigene Pforte unter aad.portal.azure.com. Benutzer können auf myapps.microsoft.com eine Liste der verwendeten Dienste einsehen, beispielsweise Outlook Online oder das Videoarchiv Stream.

Die genannten Adressen beziehen sich auf die bekannte kommerzielle Azure-Cloud. Die nationalen Clouds für US-Regierungsbehörden und China, die von der globalen Cloud getrennt sind, haben eigene Endpunkte. Die separate Microsoft-

Cloud für Deutschland wurde Ende 2021 geschlossen (siehe ix.de/z646). Eine hilfreiche Übersicht über Microsoft-Portale bietet die Website des Gemeinschaftsprojekts msportals.io (siehe ix.de/z646).

Daneben können Admins über mehrere Kommandozeilenwerkzeuge auf AAD und ARM zugreifen. Die Azure-Befehlszeilenschnittstelle, kurz Azure CLI, basiert auf Python und bringt einen eigenen Interpreter mit; sie lässt sich unter Windows, macOS und Linux installieren (Installations- und Aktualisierungshinweise siehe ix.de/z646).

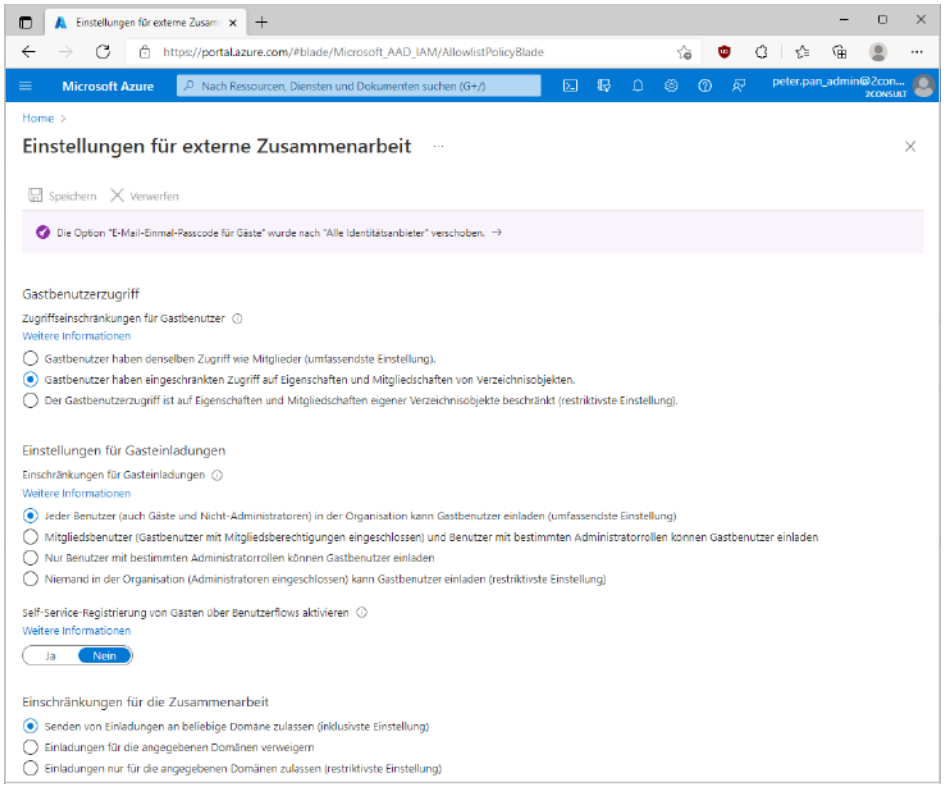
Microsoft setzt stark auf sein Automatisierungs- und Konfigurationsmanagement-Framework PowerShell und dessen Skriptsprache, die integrale Bestandteile aktueller Windows-Installationen sind. Für das Management von AAD dient dort das PowerShell-Modul AzureAD, für die Verwaltung von Azure-Diensten die Az-Modulsammlung. Beide können mit dem Befehl `Install-Module` eingerichtet werden.

Statt diese Werkzeuge lokal zu installieren, finden Admins alternativ in ihrem Browser im Azure-Portal mit der Cloud Shell eine vorkonfigurierte Bash- und PowerShell-Umgebung vor. Aber nicht nur den Admins, auch den Angreifern nützen diese textbasierten Werkzeuge.

## Unter der Haube stecken APIs

Die Weboberflächen und die Kommandozeilentools greifen unter der Haube über HTTP-Anfragen auf REST-Schnittstellen auf Microsoft-Servern zu. Die wichtigsten öffentlichen Endpunkte für AAD und Microsoft-365-Dienste liegen im Microsoft Graph unter graph.microsoft.com und für den Azure Resource Manager unter management.azure.com.

Für beide Schnittstellen stehen mit dem Graph Explorer beziehungsweise der Azure-REST-API-Referenz umfangreiche Dokumentationen bereit (siehe ix.de/z646). Die Authentisierung findet über Protokolle wie OAuth2 und dessen Erweiterung OpenID Connect statt. Als Schlüssel zu den APIs dienen in der Regel JSON Web Token (JWT). Dabei gibt es Sitzungstoken, die bis zu einem Tag lang gültig sind, und Aktualisierungstoken, mit denen bis zu 90 Tage nach Ausstellung neue Sitzungs- und Aktualisierungstoken abgerufen werden können. Die Doku zur Microsoft Identity Platform (siehe ix.de/z646) beschreibt für Interessierte dazu mehr Hintergründe. Wenn ein Angreifer in den Besitz eines solchen Tokens gelangt, kann er direkt auf die REST-APIs zugreifen, wie im folgenden Artikel gezeigt wird.




**Unsichere Standardeinstellungen für die externe Zusammenarbeit, mit denen jeder Benutzer Gäste einladen kann (Abb. 4).**

Weil sie die Grundlage der offiziellen Portale und Werkzeuge bilden, kann man über die öffentlichen APIs alle möglichen Aktionen ausführen, beispielsweise die Auflistung von AAD-Benutzern und Azure-Ressourcen und jede Änderung für jeden Azure-Ressourcentyp, sofern sie im jeweiligen Benutzerkontext erlaubt sind. Aus internen undokumentierten APIs lassen sich unter Umständen Informationen abrufen, die öffentliche Schnittstellen nicht bereitstellen. Dafür stehen Angriffswerkzeuge zur Verfügung, die im nächsten Artikel vorgestellt werden.

## Bugs gibt es auch in der Cloud, aber …

Die Diskussion über die grundsätzliche Sicherheit von Cloud-Diensten wie Azure im Vergleich zu selbst verwalteten Umgebungen und der sich verschiebenden Verantwortung kann man sicherlich mit erhitztem Gemüt führen – während die Provider ihre Umsätze steigern und anfangen, bewährte Produkte wie das klassische Exchange zu vernachlässigen [5]. Genauso wie bei Microsofts On-Premises-Verzeichnisdienst AD mit patchbaren Schwachstellen wie „PetitPotam“ [6] fanden sich im vergangenen Jahr Bugs bei einzelnen Azure-Diensten wie App Services (mit dem Namen „NotLegit“ versehen), Cosmos DB („ChaosDB“) und im Software-Agent OMI bei Linux-VMs („OMIGOD“). Eine lesenswerte Übersicht über Sicherheitsfehler von Cloud-Service-Providern sammelt ein GitHub-Projekt (siehe ix.de/z646).

Schlimmer, zumindest zahlreicher als gelegentliche Bugs in der Plattform sind jedoch Fehlkonfigurationen, die eine betroffene Organisation in ihrem AAD oder einem Azure-Dienst verursacht hat. Dabei kommt Microsoft als Nachzügler im Vergleich zu den früher gestarteten Konkurrenten Amazon Web Services (AWS, veröffentlicht 2006) oder Google Cloud Platform (GCP, 2008) zugute, dass bestimmte Arten von Fehlkonfigurationen in Azure schwieriger zu bewerkstelligen sind – etwa in Bezug auf Metadatenzugriff und Speicherkonten [7] –, dass sich Schlüssel und Geheimnisse in Schlüsseltresoren verwalten lassen und dass das Azure-Portal für alle Dienste aus einem Guss wirkt.

Schwer wiegt für ein betroffenes Unternehmen, wenn ein hoch privilegiertes AAD-Konto kompromittiert wird, das über umfangreiche Berechtigungen im Identitätsdienst selbst oder auf Azure-Diensten verfügt. Denn im Gegensatz zu klassischen Umgebungen, die nach dem Zwiebelprinzip mit Firewalls und anderen Sicherheitsprodukten abgeschottet werden, kann ein Angreifer mit den gestohlenen Benutzerdaten über das Internet direkt auf die Cloud-Umgebung zugreifen. Daher stammt die

Rede von der Identität als neuem Perimeter [1]. Als Reaktion auf diese veränderten Netzwerkstrukturen hat sich das Zero-Trust-Sicherheitskonzept durchgesetzt, bei dem Azure AD als zentraler Dienst fungiert [8].

Die Wahl sicherer Passwörter ist mitentscheidend, siehe dazu [9], vor allem in Branchen, in denen das Sicherheitsbewusstsein geringer ist. Dennoch werden laut Daten von Microsoft jeden Monat 0,5 Prozent aller AAD-Konten von Angreifern kompromittiert – die Mehrzahl davon durch Passwort-Spraying-Angriffe, bei denen ein wahrscheinliches Passwort wie „Sommer2022!“ für alle Konten durchprobiert wird, und durch wiederverwendete Passwörter, die in Leakdatenbanken auftauchen. Bei 99 Prozent dieser kompromittierten Konten ist Mehr-Faktor-Authentisierung (MFA) nicht aktiv. Dabei wäre das ein wichtiger Schutz gegen aktuelle Angriffstechniken.

Wie zahlreich Angriffe auf Identitäten in Azure sind, zeigen Zahlen von Microsoft aus dem Februar 2022, nach denen das Unternehmen im Vorjahr 25 Milliarden Brute-Force-Angriffe auf AAD erkannt und blockiert hat (siehe ix.de/z646). Nur 22 Prozent der Kunden hätten ausreichend starken Authentifizierungsschutz wie MFA implementiert.

## Verbreitet: unsichere Standardeinstellungen

Reguläre Benutzer können sich im Azure-Portal anmelden und auf Mandanten-Informationen zugreifen, diese Option ist normalerweise nicht gesperrt.

Andere Standardeinstellungen im Azure AD bieten ebenfalls nicht die höchstmögliche Sicherheit. Kennwortlose Authentifizierungsmethoden sind deaktiviert. Ein normaler AAD-Benutzer kann

- Sicherheitsgruppen erstellen;
- Gäste einladen (siehe Abbildung 4) und zu Mitgliedern von Gruppen machen, die ihm gehören;
- eine Benutzereinwilligung für Anwendungen geben und sogar eigene Anwendungen registrieren;
- bis zu 50 Geräte am Mandanten anmelden, ohne dass für die Geräteregistrierung ein zweiter Faktor abgefragt wird.

Wenn ein Benutzer ein Windows-Gerät in Azure AD einbindet, wird er zu dessen Eigentümer und damit Mitglied der lokalen Admingruppe. Benutzer sollten aber nie lokaler Admin sein [10].

Auf diesem Weg kann ein Angreifer Richtlinien für bedingten Zugriff umgehen, selbst wenn diese entweder Mehr-Faktor-Authentisierung oder ein konformes Gerät fordern: Ohne den zweiten Faktor für das kompromittierte Konto zu kennen, kann er sein eigenes Gerät registrieren, konform machen und mit dem konformen Angriffsrechner auf weitere Azure-Dienste zugreifen.

## Nicht automatisch sicher

Nicht bei jedem Azure-Dienst sind die Standardeinstellungen ausreichend sicher. Beispielsweise sind Azure App Services und CosmosDB-Datenbanken aus dem gesamten Internet zugänglich, wenn der Systemverwalter beim Erstellen nur die unbedingt notwendigen Daten wie das Abonnement und die Region ausfüllt und nicht alle Schritte im Assistenten durchläuft.

Darüber hinaus können unachtsame Admins durch unbedacht vorgenommene, harmlos klingende Einstellungen Lücken in ihre Cloud-Umgebung reißen: Wenn sie bei Datenbanken die Option „Anderen Azure-Diensten und -Ressourcen den Zugriff auf diesen Server gestatten“ aktivieren, gehen sie wahrscheinlich davon aus, dass nur Zugriff möglich ist von anderen Diensten, die im eigenen Tenant oder demselben Abonnement verwaltet werden. Allerdings wird die Datenbank damit für jede Quelladresse aus der Microsoft-Cloud freigegeben. Ein Angreifer kann einfach einen virtuellen Rechner in seinem eigenen Azure-Abo aufsetzen und von da auf sie zugreifen.

Für Admins ist es somit wichtig, sich nicht nur auf die Benennung im Azure-Portal zu verlassen, sondern dem Link zu weiteren Informationen aus dem Informations-Pop-up zu folgen oder auf anderem Weg zur passenden Microsoft-Dokumentation zu finden – und die Auswirkungen der einzelnen Konfigurationen zu verstehen, bevor sie sie ändern.

## Fazit

Microsoft macht den schrittweisen Umstieg auf Azure-basierte Dienste vor allem solchen Unternehmen leicht, die intern schon viel mit Windows-Servern und -Clients sowie mit Standardanwendungen wie SharePoint arbeiten. Auch Microsofts Kommunikation der jüngeren Schwachstellen im On-Premises-Mailserver Exchange, beginnend bei ProxyShell, haben gezeigt, dass die Redmonder ihre Kunden unter dem Vorwand der höheren Sicherheit zu ihren Cloud-Diensten locken wollen.

Das führt zum zunehmenden Einsatz von Microsoft-365-SaaS-Lösungen wie Exchange Online, von Azure-Diensten für IaaS wie virtuelle Maschinen oder PaaS wie Functions – und dem Wechsel zu hybriden Umgebungen, bei denen Mitarbeiterrechner ganz oder teilweise aus der Cloud verwaltet werden.

Dadurch ist Azure AD als zentraler Identitätsdienst der Microsoft-Cloud in den Fokus von Angreifern gerückt. Wie sie vorgehen, beschreibt der folgende Artikel „Ins Netz gegangen“. (ur@ix.de)

### Quellen


[1] Inés Atug; Anforderungspuzzle; Microsoft 365 in Unternehmen sicher nutzen; *iX* 7/2021, S. 46

[2] Bastian Dingfeld, Maximilian Marius Klose; Cloud-Schnitt; Microsoft 365 sicher konfigurieren; *iX* 7/2021, S. 54

[3] Frank Ully; Vertrauensfragen; Active Directory: Wie Angreifer Tickets, Delegierung und Trusts missbrauchen; *iX* 2/2021, S. 116

[4] Frank Ully; Allgegenwärtig; Der Verzeichnisdienst Active Directory: einer für alle(s); *iX* 10/2020, S. 48

[5] Susanne Nolte; Trotz früher Patches: Exploits gefährden Exchange Server; *iX* 10/2021, S. 22

[6] Hans-Joachim Knobloch; Und ewig grüßt das Nilpferd; PetitPotam und weitere Wege, die Kontrolle über das AD zu übernehmen; *iX* 9/2021, S. 91

[7] Andreas Dann, Johannes Späth, Manuel Benz; Blinder Alarm; Kontext als Schlüssel zur sicheren Cloud; *iX* Developer „Sichere Softwareentwicklung“ 2021, S. 44

[8] Jens Lüttgens, Dominik Oepen; Misstrauen mit System; Azure AD und Zero Trust; *iX* 2/2022, S. 102

[9] Sandro Affentranger; Schwierige Wahl; Passwortsicherheit (nicht nur) im Active Directory; *iX* 1/2022, S. 116

[10] Marco Wohler; Mit aller Härte; Wie Administratoren ihr Active Directory absichern; *iX* 5/2021, S. 106

[11] Frank Ully; Ins Netz gegangen; Angriffe auf das Azure Active Directory und Azure-Dienste; *iX* 4/2022, S. 50

[12] Alle im Artikel erwähnten Werkzeuge, Blogartikel und Microsoft-Dokumente sind über ix.de/z646 zu finden.



**Frank Ully**

ist Head of Research der Oneconsult Deutschland AG in München. Er beschäftigt sich mit aktuellen Themen der offensiven IT-Sicherheit.