Azure Active Directory und Azure-Dienste absichern

Das Netz verstärkt

Frank Ully

Eine Grundabsicherung von Azure Active Directory und Microsofts Cloud-Diensten ist kein Hexenwerk. Doch um an den richtigen Stellschrauben zu drehen, gilt es, sie zunächst zu finden. Dabei helfen die Bordmittel des Admin-Portals, kostenlose Tools, Tipps aus dem Netz und vor allem das Verständnis von Microsofts Sicherheitskonzepten.

So besorgniserregend die in den beiden vorangegangenen Artikeln beschriebenen Angriffsmöglichkeiten auf Azure Active Directory sind, so einfach sind zumindest grundlegende Schutzmaßnahmen einzurichten. Oft reichen die Bordmittel des Azure-Portals bereits aus. Kleine, frei verfügbare Tools, meist als PowerShell-Skripte implementiert, und zusätzliche Portale und Werkzeuge helfen beim Aufspüren von Schwachstellen. Dieser Artikel stellt Maßnahmen in den Vordergrund, die Nutzer möglichst wenig einschränken, dennoch die Sicherheit erhöhen und zudem selten Premiumlizenzen von Azure erfordern. In der zweiten Hälfte geht es vor allem um die Absicherung hybrider Umgebungen aus AAD und dem On-Premises-Verzeichnisdienst. Eine ausführliche Liste mit weiterführenden Informationen findet sich in den *iX*-Links (siehe ix.de/z4qh).

Unsichere Standardkonfigurationen beheben

Die im Artikel „Ins Netz gezogen“ ab Seite 44 beschriebenen unsicheren Standardkonfigurationen kann ein Admin einfach beheben. Im Azure-Portal sollte unter Benutzereinstellungen für das AAD die Option „Zugriff auf Azure AD-Verwaltungsportal einschränken“ auf Ja gestellt werden. Das Abrufen von Daten der Benutzer und Gruppen ist damit für Nicht-Admins unterbunden.

Zusätzlich könnten Standardbenutzer auch über die API-Schnittstellen mittels PowerShell-Modulen Daten abfragen. Deshalb werden diese ebenfalls eingeschränkt. Damit sind dann auch Enumerationswerkzeuge wie ROADrecon lahmgelegt. Ein globaler Admin nimmt dazu folgende Einstellung in einer PowerShell-Sitzung vor:

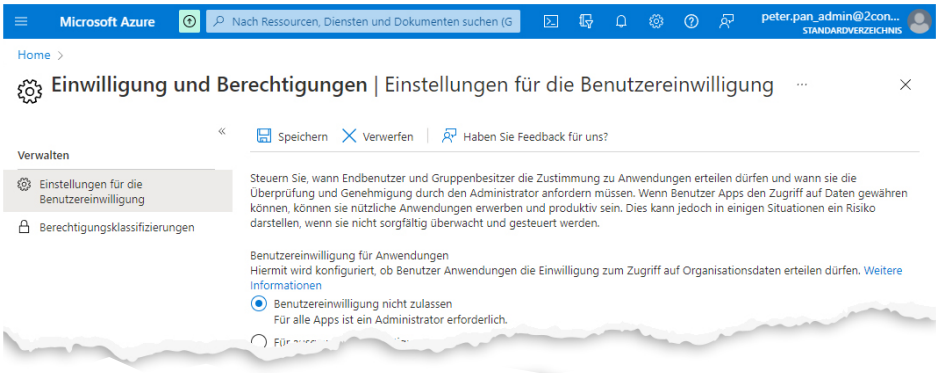
```
Install-Module MSOnline
Connect-MsolService
Set-MsolCompanySettings -Users↵
      PermissionToReadOtherUsers↵
                  Enabled $false
```

Unter Umständen führt Letzteres dazu, dass Mitarbeiter in Teams keine Gäste mehr hinzufügen können, das sollten Admins kurz testen. Ebenfalls in den Benutzereinstellungen sollte der Punkt „Benutzer können Anwendungen registrieren“ ausgeschaltet werden. Dadurch wird unter anderem OAuth-Phishing aus dem eigenen Mandanten heraus verhindert.

Von den Benutzereinstellungen führt ein Link zu den „Einstellungen für externe Zusammenarbeit“. Für Gäste sollte gewählt werden: „Der Gastbenutzerzugriff ist auf Eigenschaften und Mitgliedschaften eigener Verzeichnisobjekte beschränkt“. Gasteinladungen sollten nur für Benutzer mit

iX-TRACT

- Ein Azure Active Directory (Azure AD) in der Standardkonfiguration ist nicht ausreichend sicher; harmlos erscheinende Einstellungen können gravierende Angriffe ermöglichen. Eine sichere Konfiguration ist jedoch leicht vorgenommen und bringt oft keine wesentlichen Funktionseinbußen.
- Mit kostenlosen quelloffenen Tools und in Azure eingebauten Werkzeugen wie Microsoft Defender für die Cloud (früher Azure Security Center) können Cloud-Admins und Sicherheitsverantwortliche Verbesserungspotenzial aufspüren.
- Außerdem gibt es für die Microsoft-Cloud und ihren Identitätsdienst Azure AD zahlreiche Funktionen, die die Sicherheit von AAD-Identitäten und von Azure-Diensten erhöhen – manchmal erfordert das jedoch Premium-Lizenzen, zumindest für einige wenige Benutzer.



Die Einstellungen zur Benutzereinwilligung legen fest, ob Nutzer den von ihnen installierten Anwendungen Zugriff auf Unternehmensdaten gewähren können (Abb. 1).

bestimmten Administratorrollen oder für niemanden erlaubt werden. Zusätzlich kann man Einladungen nur für angegebene Domänen zulassen, die man für seine Partnerunternehmen zusammensucht.

Um OAuth-Phishing generell zu unterbinden, kann bei den Unternehmensanwendungen im Blatt „Einwilligung und Berechtigungen“ eine Benutzereinwilligung überhaupt nicht zugelassen oder zumindest auf Apps von verifizierten Herausgebern eingeschränkt werden (siehe Abbildung 1). Analog lässt sich einstellen, ob Gruppenbesitzer Anwendungen für ihre Gruppen die Einwilligung zum Zugriff auf Organisationsdaten erteilen dürfen.

Außerdem sollte bei den Unternehmensanwendungen unter Gruppen im Blatt Allgemein deaktiviert werden, dass Benutzer Sicherheitsgruppen in Azure-Portalen, API oder PowerShell erstellen können, Gleiches gilt für Microsoft-365-Gruppen. Dadurch wird verhindert, dass ein bereits kompromittierter Benutzer oder ein bösartiger Insider eine Sicherheitsgruppe erstellt, alle AAD-Benutzer hinzufügt und einer bösartigen Anwendung für diese Gruppe Berechtigungen erteilt.

Direkt im Azure-AD-Portal unter Unternehmensbranding kann eine mit Firmenlogo und Hintergrundbild angepasste Anmeldeseite als kleine Maßnahme dabei helfen, auf Phishingversuche mit generischen Azure-Anmeldeseiten aufmerksam zu machen. Unter „Zurücksetzen des Kennworts“ und dort im Banner Benachrichtigungen sollte eingestellt werden, dass alle Administratoren benachrichtigt werden, wenn andere Admins ihr Kennwort zurücksetzen. Damit erkennt man einfach einen möglichen schon fortgeschrittenen Angriff.

Im Blatt Geräte (der Geräte-Direktlink aus dem Suchfeld führt hingegen zum Endpoint Manager) und dort unter Geräteeinstellungen können Admins den Benutzern verbieten, Geräte in Azure AD einzubinden oder zu registrieren. Zudem sollten diese Aktionen eine Mehr-Faktor-Authentifizierung verlangen. Übrigens: Falls ein in Azure AD eingebundenes Endgerät verloren geht oder kompromittiert wurde, sollte ein Admin es in AAD deaktivieren, anschließend das Passwort des betroffenen Benutzers ändern und seine Aktualisierungstoken mit dem AzureAD-Befehl `Revoke-AzureADUserAllRefreshToken` widerrufen.

Vorsicht ist beim Nutzen dynamischer Gruppen geboten. Vor allem darf die Mitgliedschaft nicht auf Attributen beruhen, die Benutzer in AAD bearbeiten können. Wenn das AAD mit einem On-Premises AD mit Azure AD Connect synchronisiert wird, ist darauf zu achten, dass Nutzer die verwendeten Attribute für dynamische Mitgliedschaften nicht in der On-Premises-Umgebung ändern dürfen. Die Attribute sind oft tief in den ACLs des klassischen AD vergraben und erfordern sorgfältige Suche. Über Azure AD Connect legt man fest, welche Attribute synchronisiert werden, oder schließt komplette OUs aus.

Ob ein Microsoft-Cloud-Partner über delegierte Administration Zugriff auf den eigenen Mandanten hat, kann unter admin.microsoft.com geprüft werden. Bisher nur als Vorschaufunktion verfügbar ist die Möglichkeit, dass Organisationen in ihrem AAD-Tenant unter den mandantenübergreifenden Zugriffseinstellungen für die B2B-Zusammenarbeit Einstellungen für eingehenden und ausgehenden Datenverkehr weiter härten können.

Zurück zu den Wurzeln: Least-Privilege-Prinzip

Wie mächtig globale Administratoren und andere Adminrollen sind, wurde im vorigen Artikel beschrieben. Deshalb sollten höchstens fünf Benutzer globale Admi-

nistratoren sein. Für alle anderen sollten Cloud-Architekten AAD- und Azure-Rollen mit den niedrigsten ausreichenden Rechten wählen. Falls lesender Zugriff auf das AAD ausreicht, beispielsweise für Auditoren und Sicherheitsverantwortliche, gibt es die Rollen Sicherheitsleser und globaler Leser.

Hilfreich ist eine strikte Trennung zwischen regulären und Adminkonten: peter.pan@2consult.onmicrosoft.com für das Tagesgeschäft und peter.pan_admin@2consult.onmicrosoft.com für administrative Aufgaben. Diese klare Trennung erleichtert die Wartung, beugt Fehlkonfigurationen vor und macht beim Wechsel zum Adminkonto klar, dass man jetzt besonderer Vorsicht walten lassen muss.

Zwei weitere, weniger bekannte Möglichkeiten, den Zugriff einzuschränken: Eine AAD-Verwaltungseinheit kann ähnlich wie eine AD-Organisationseinheit Benutzer und Gruppen enthalten; Zuweisungen privilegierter Rollen wie der des Benutzeradmin lassen sich auf die Verwaltungseinheit beschränken. Sicherheitsgruppen, denen wichtige Rollen zugewiesen werden, die aber nur begrenzte Zeit benötigt werden, können Admins in den Einstellungen mit einem Ablaufdatum versehen.

Das Least-Privilege-Prinzip gilt nicht nur für echte Nutzer, sondern erst recht für verwaltete Identitäten, die Anwendungen zugeordnet sind. Anders als eine Identität für einen echten Benutzer muss eine solche nur eine genau definierbare Menge an Aufgaben erfüllen. Es beugt Privilegieneskalation vor, wenn Anwendungen und ihre Dienstprinzipale nur die Mindestberechtigungen erhalten, die zum Ausführen ihrer Verwaltungsaufgaben erforderlich sind.

Im Berechtigungssystem von Azure selbst, also bei Azure-RBAC, sollte die Anzahl von Abonnementbesitzern und -mitwirkenden begrenzt werden – auch das sind administrative Konten. Für die restlichen Konten sollte nur der erforderliche Zugriff gewährt werden, möglichst auf dem geringsten zutreffenden Scope: auf der Ressourcengruppe statt auf dem Abonnement oder gar einer Verwaltungsgruppe mit mehreren Abos.

Angreifer versuchen, auf dem Weg des geringsten Widerstands einen Fuß in die Tür zu bekommen. Problematisch sind Staging-Umgebungen mit laxen Sicherheitsanforderungen, die einfach kompromittiert werden und direkt sensible Daten enthalten oder die den Weg in die Produktionsumgebung ebnen, da Cloud-Dienste eng miteinander verknüpft sind. Um solche Angriffspunkte zu erkennen, ist es wichtig, auch in der Cloud ein Asset-Management einzurichten.

Auditwerkzeuge

Beim Auffinden hoch privilegierter Benutzer, auch als Schattenadministratoren bezeichnet, hilft das PowerShell-Skript AzureStealth, das Teil der SkyArk-Werkzeugsammlung von CyberArk ist. Zum Ausführen werden die Standard-PowerShell-Module für Azure und AAD benötigt und ein Benutzer mit Lesezugriff auf das Verzeichnis und alle Abonnements. Über Abfragen der Microsoft-APIs findet AzureStealth überprüfenswerte hoch privilegierte Benutzer:

```
git clone https://github.com/↵
                    cyberark/SkyArk
cd .\SkyArk\
Import-Module .\SkyArk.ps1 -force
Start-AzureStealth
```

Das ebenfalls quelloffene Audit-Tool Scout Suite der NCC Group untersucht AWS, Azure, GCP und noch exotischere Clouds auf typische Fehlkonfigurationen (siehe Abbildung 2). Neben Leserechten wie oben benötigt es noch die Sicherheitsleser-Rolle auf allen Abos und deckt zahlreiche gefährliche Einstellungen auf; für AAD etwa Gastbenutzer und für Azure-Dienste zum Beispiel öffentlich zugängliche Speicherkonten.

```
az login
pip install scout
scout azure --cli --report-↵
        dir C:\Reportverzeichnis
```

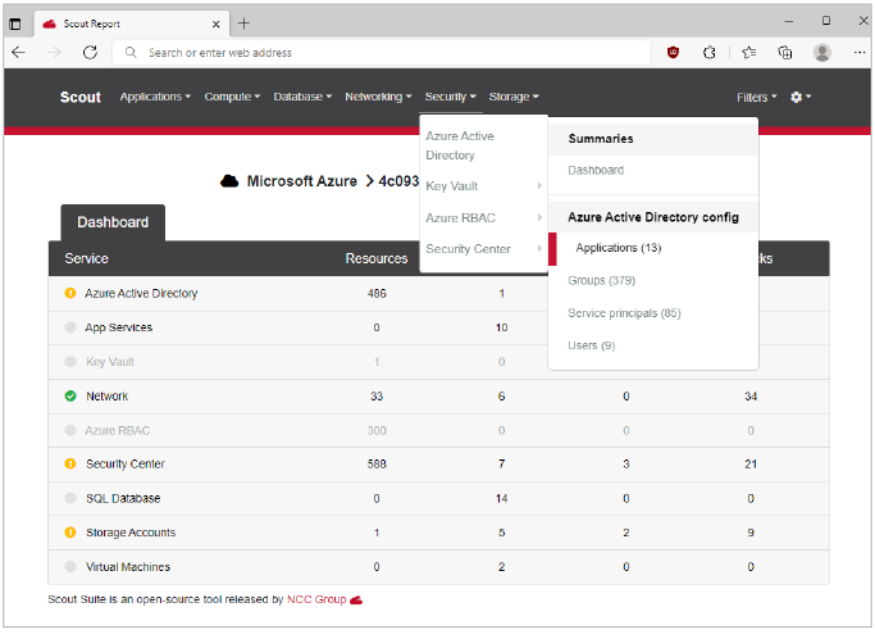
Eigentümer von Anwendungen, die deren Rechte übernehmen können, spürt das PowerShell-Skript `report-AzAppOwnerPermissions.ps1` von Jan Geisbauer auf, das als globaler Admin oder Leser ausgeführt wird. Es exportiert die Ergebnisse direkt in eine übersichtliche CSV-Datei.

```
Connect-AzureAD
git clone https://github.com/↵
  jangeisbauer/report-AZAppOwner↵
                    Permissions.git
.\report-AZAppOwnerPermissions\↵
 report-AzAppOwnerPermissions.ps1
```

Konkreten Anwendungen mit zu vielen Berechtigungen kommt man ebenfalls mit PowerShell auf die Spur. Philippe Signoret stellt auf GitHub das Skript `Get-AzureADPSPermissions.ps1` bereit:

```
.\Get-AzureADPSPermissions.ps1 ↵
      | Export-CSV permissions.↵
          csv -NoTypeInformation
```

Es gibt delegierte (OAuth2Permission Grants) und Anwendungsberechtigungen (AppRoleAssignments) zurück, die man nach Zustimmungen für AllPrincipals durchforstet oder nach Benutzern, die Genehmigungen erteilt haben. Ein Export von Berechtigungen ist ebenso im CrowdStrike Reporting Tool (CRT) enthalten. Es deckt zudem für Exchange Online sonst schwierig zu findende Berechtigungen und Einstellungen auf. Mit den Ausgaben jedes der beiden Skripte muss man sich allerdings etwas auseinandersetzen. Zielgerichtet nach wenigen hochkritischen API-Berechtigungen für Microsoft Graph und damit AAD, die eine Privilegieneskalation zum globalen Administrator ermöglichen,



Das Multi-Cloud-Auditwerkzeug Scout Suite sucht Fehlkonfigurationen in Azure und weiteren Cloud-Plattformen und stellt die Reports im HTML-Format dar (Abb. 2).

sucht das Skript `AuditAppRoles.ps1` von Andy Robbins.

Im heruntergeladenen Quelltext muss man die ersten Zeilen zur Anmeldung entfernen, kann sich dann mit `Connect-AzAccount` mit einem Konto an Azure anmelden und das restliche Skript ausführen. Jeder Dienstprinzipal, den das Skript findet, ist kritisch und sollte idealerweise entfernt werden – wenn man das nicht kann, sollte man eingehend untersuchen, wer dessen Eigentümer sind oder wer sonst darüber Kontrolle erlangen könnte. Alle erwähnten Werkzeuge sind unter ix.de/z4qh verlinkt.

Portale, Portale, Portale

Das wichtigste Portal von Microsoft in Bezug auf Azure-Sicherheit ist der Microsoft Defender für die Cloud, früher Azure Security Center (siehe Abbildung 3). Auch wenn Microsoft bei dessen erstem Aufruf hartnäckig ein Defender-Abonnement verkaufen will, mit dem viele weitere Funktionen freigeschaltet werden, lassen sich dort auch ohne Abo zentral Empfehlungen, Warnungen und Bewertungen zur Sicherheit abholen. Auch wenn der Defender für die Cloud eine einheitliche Oberfläche bietet, muss eine Organisation doch ein wenig Aufwand in die Einrichtung stecken – und auf dort erscheinende Warnungen angemessen reagieren. Weiteres zum Defender siehe [1].

Das gemeinnützige Center for Internet Security (CIS) stellt mit seinen Foundation-Benchmarks Konfigurationsempfehlungen für Azure und Microsoft 365 zum kostenlosen Download als PDF bereit. Der Defender für die Cloud kann die eigene Konfiguration gegen diese Benchmarks prüfen. Dort ist Azure Policy das Werkzeug, das die Compliance zu den CIS-Benchmarks und den Microsoft-eigenen Sicherheits-Baselines für Azure untersucht. Mit solchen Richtlinien kann man nicht nur gegen Empfehlungen prüfen, sondern unmittelbar verhindern, dass zum Beispiel Ressourcen in einer Azure-Region außerhalb der EU angelegt werden, oder erzwingen, dass Ressourcen keine öffentlichen IP-Adressen erhalten.

Für Nutzer von Microsoft 365 gibt es neben dessen Admincenter noch ein weiteres, aus Sicherheitsperspektive bemerkenswertes Portal: die Inhaltssuche unter protection.office.com, deren Nutzung allerdings erweiterte Lizenzen erfordert. Identitäten mit der Rolle eDiscovery-Manager können dort bei allen Microsoft-365-Diensten wie Exchange, Teams, OneDrive und SharePoint nach Inhalten in Nachrichten und Dokumenten der Nutzer suchen und Berichte erstellen. Das bedeutet andererseits auch, dass ein Benutzer mit der entsprechenden Rolle ein lohnendes Opfer für einen Angreifer ist, mit dessen Zugangsdaten er in vielen Nachrichten des Unternehmens nach interessanten Inhalten stöbern könnte.

Sichere Cloud auch in hybriden Umgebungen

Microsoft beschreibt in seiner Doku „Schützen von Microsoft 365 vor lokalen Angriffen“ (siehe ix.de/z4qh) mehrere Maßnahmen, wie Azure AD so gesichert wird, dass ein Angreifer, der sich im Netzwerk eines Unternehmens breitgemacht hat, nicht gleich noch dessen Azure-Umgebung unter Kontrolle bringt (siehe Abbildung 4). Diese Empfehlungen sind unabhängig davon wichtig, wie tief die Integration zwischen on Premises und Cloud ist.

Wesentlich ist vor allem, dass die Konten von Administratoren und anderen Hochprivilegierten nicht aus einer lokalen Umgebung synchronisiert, sondern direkt in AAD erstellt werden (erkennbar an einem UPN wie peter.pan_admin@2consult.onmicrosoft.com). Damit bleiben administrative Benutzer beider Umgebungen getrennt. Das gilt in die eine Richtung wie in die andere. Ein lokales Domänen- oder Serveradminkonto hat in einer Cloud-Umgebung nichts verloren; ein Konto aus der Domäne sollte in Azure keine administrativen Rechte haben.

Darüber hinaus sollten nur solche Benutzer übertragen werden, die wirklich auf Onlinedienste zugreifen müssen. Je mehr On-Premises-Objekte repliziert werden, desto größer die Angriffsfläche auf Cloud-Identitäten. Bei einer Synchronisierung mit Azure AD Connect lässt sich festlegen, welche Organisationseinheiten oder, bei größeren Gesamtstrukturen, Domänen lokal und in Azure synchron gehalten werden sollen; idealerweise geschieht das vor der ersten Synchronisierung.

Falls entgegen der Empfehlung Admin- oder Dienstkonten synchronisiert werden, lässt sich über den Synchronisierungsregel-Editor immerhin verhindern, dass die Passwort-Hash-Synchronisierung (PHS) deren Passwörter überträgt. Zum weiteren Sichern von Azure AD Connect siehe [2].

Cloud-Admins sollten natürlich besonders geschützt sein – durch MFA, die über Richtlinien für bedingten Zugriff erzwungen wird (dazu unten mehr). Als weiteren wesentlichen Härtungsschritt sollte ein Admin seine Cloud-Umgebung nicht über den regulären Computer verwalten, mit dem er E-Mails liest und im Web surft, sondern nur über speziell gesicherte Arbeitsplätze. Dieses Konzept ist schon aus der lokalen AD-Welt als Privileged Access Workstations (PAW) bekannt. Dabei fungiert in der sichersten, aber unkomfortabelsten Variante ein eigener physischer Computer als PAW. Ein einzelnes Gerät genügt, wenn die tägliche Arbeit in einer virtuellen Maschine erledigt wird und das Hostbetriebssystem ausschließlich administrativen Zwecken dient.

Auf keinen Fall darf der Rechner zur Cloud-Administration an einer Domäne angemeldet sein – wenn ein Angreifer das lokale AD kompromittiert hat, gewinnt er mit On-Premises-Gruppenrichtlinien die Kontrolle über ein System, mit dem Azure administriert wird. Stattdessen bietet Microsoft auf GitHub eine Intune-Konfiguration an, die Windows-10-Arbeitsplätze für die Azure- und AAD-Administration härtet (siehe ix.de/z4qh).

Der abgesicherte Arbeitsplatz wird ausschließlich zum Managen der Tier-0-Umgebung in Azure eingesetzt und nicht mit anderen Netzwerken verbunden. Denn eng mit PAWs hängt das Tier- oder Ebenenmodell zusammen [3]. Kerngedanke dabei ist, privilegierte Benutzer und Systeme vom Rest zu trennen und speziell zu schützen. Tier 0 ist die am besten gesicherte Zone, in der sich on Premises etwa der Domänencontroller befindet. Weil Azure AD Connect hoch privilegierte Konten in AD und Azure AD verwendet, gehören Connect-Server und ihre SQL-Datenbanken ebenfalls zu Tier 0 und müssen wie ein Domänencontroller behandelt werden. Dasselbe gilt für Verbundserver, falls die Organisation Federation Services einsetzt. Eine Microsoft-Doku beschreibt weitere Methoden zum Schützen von ADFS.

Auf der anderen Seite zählen Plattformen zum Mobile Device Management (MDM) wie der Microsoft Endpoint Manager und Rollen wie der Intune-Admin zum Tier 0, wegen des großen Schadenspotenzials im Falle einer Kompromittierung, weil sie Code auf den verwalteten Rechnern ausführen können.

Lokale Adminpasswörter für Computer in der Cloud

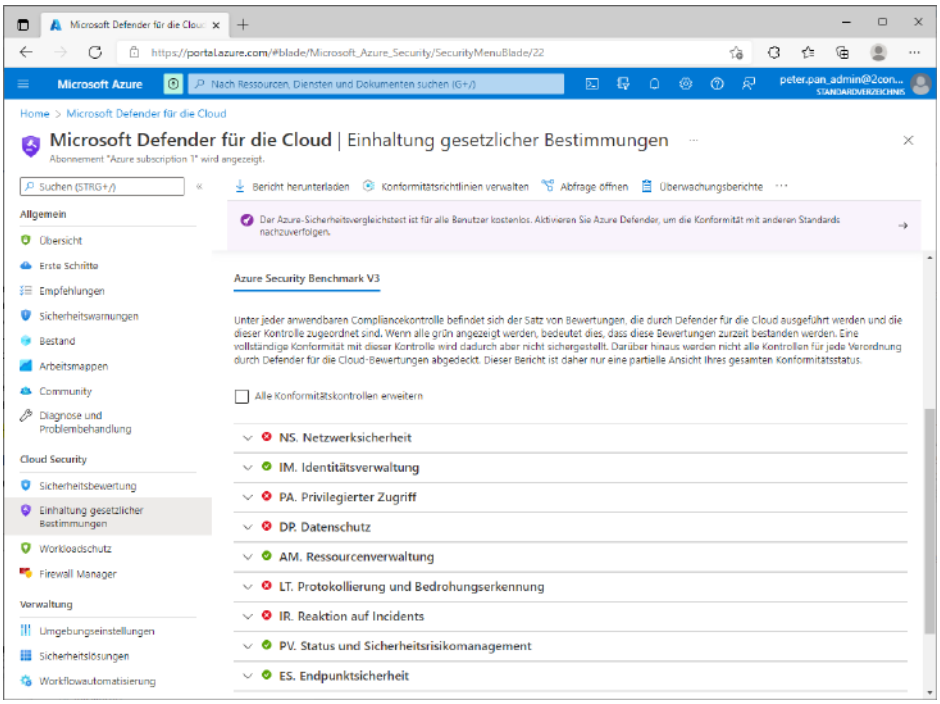
Lokale Administratorkonten einzelner Rechner sollten für jeden Computer in einer Windows-Umgebung unterschiedlich sein, um klassische Angriffe wie Pass-the-Hash zu erschweren [4]. Beim On-Premises Active Directory empfiehlt sich dafür Microsofts kostenloses Werkzeug LAPS, kurz für Local Administrator Password Solution (Passwortlösung für lokale Admins). Es erzeugt und verwaltet starke und unterschiedliche Passwörter für diese hoch privilegierten lokalen Konten [5]. Bei Geräten, die nur in Azure AD eingebunden sind und die mit dem Endpoint Manager verwaltet werden, bietet die CloudLAPS Community Edition analoge Funktionen.

Bedingter Zugriff und alternative Sicherheitsstandards

Richtlinien für den bedingten Zugriff sind grundlegender Bestandteil der Sicherheit in Azure, da sie Regeln und Einschränkungen innerhalb des Mandanten festlegen, etwa für Authentifizierung und Zugriff auf bestimmte Ressourcen nach IP-Adresse. Selbst Mandanten ohne Premiumlizenz kommen über die Funktion der Sicherheitsstandards (Security Defaults) in den Genuss mancher Funktionen des bedingten Zugriffs, allerdings ohne sie einzeln konfigurieren zu können.

Sind die Sicherheitsstandards aktiviert, müssen sich alle Benutzer innerhalb von 14 Tagen für MFA registrieren, Admins werden beim Anmelden nach dem zweiten Faktor gefragt und ältere Authentifizierungsprotokolle sind gesperrt. Bei Mandanten, die nach Oktober 2019 erstellt wurden, sind die Sicherheitsstandards in der Regel aktiv – sonst kann man sie aktivieren. Wollen Admins allerdings den bedingten Zugriff selbst verwalten, müssen sie die Standards ausschalten und dafür Sorge tragen, dass sie keine der darin enthaltenen Maßnahmen in ihrer individuellen Konfiguration vergessen.

Die manuelle Konfiguration kann dabei aber auch unerwartete Lücken reißen, etwa wenn in der MFA-Richtlinie Ausnahmen definiert sind für Anmeldungen von einem vertrauenswürdigen Standort wie dem Netzwerkbereich des Hauptsitzes oder von VPN-Bereichen. Ein Angreifer, der einen Arbeitsplatzrechner unter seiner Kontrolle hat, wird von einer dieser vermeintlich sicheren Adressen aus auf Azure zugreifen. Eher sollte umgekehrt jeglicher Zugriff aus einem Land oder einer Region blockiert werden, in der Mitglieder der eigenen Organisation nie zugange sein werden. Richtlinien sollten also möglichst wenig Ausnahmen haben und für alle Clients und Anwendungen gelten, weil sich sonst das Risiko von Lücken erhöht.



Als wichtige Sicherheitszentrale ist der Microsoft Defender für die Cloud, das frühere Azure Security Center, auch schon in seiner kostenlosen Version empfehlenswert (Abb. 3).

Admins sollten Ausnahmebedingungen regelmäßig prüfen.

Eine Richtlinie, die für alle Cloud-Apps und für alle Geräte gilt, aber als Ausnahmen Android, iOS, Windows Phone, Windows und macOS definiert, erfasst auch nicht unterstützte Geräte wie Linux oder Anfragen mit fehlendem User-Agent-String und kann jeglichen Zugriff blockieren oder dafür MFA erzwingen. Über die neue Funktion des bedingten Zugriffs für Workload-Identitäten können seit Kurzem Dienstprinzipale abgesichert und Anmeldungen außerhalb vertrauenswürdiger IP-Adressbereiche blockiert werden, derzeit allerdings nur für Anwendungen mit einem Mandanten (siehe ix.de/z4qh).

In hybriden Umgebungen kann eine Regel das Azure-AD-Connector-Konto Sync_ auf On-Premises-IP-Adressen einschränken. Und die relativ neue Filterregel für Geräte kann man dazu nutzen, den Zugriff mit Adminrollen nur von ausgewählten PAWs aus zu erlauben. Eine Sitzungsregel zur Anmeldehäufigkeit stellt sicher, dass Benutzer regelmäßig nach ihren Zugangsdaten gefragt werden, im Standard sieht AAD ein rollierendes Zeitfenster von 90 Tagen vor. Zumindest administrative Sitzungen sollten aber nicht so lange ohne erneute Authentisierung gültig bleiben.

Legacy-Authentisierung, die MFA nicht beherrscht, sollte man vollständig blockieren. Um festzustellen, ob solche Anwendungen auf den eigenen Mandanten zugreifen, können Admins in Azure AD unter den Anmeldeprotokollen nach der Client-App filtern und dort Legacy-Authentifizierungsclients auswählen. Falls das Abschalten nicht gleich möglich ist, hilft zumindest das Begrenzen auf vertrauenswürdige Netzwerke, mit den eben beschriebenen Einschränkungen. Als langfristiges Ziel für den bedingten Zugriff kann man sich überdies setzen, Anmeldungen nur von verwalteten und als konform gekennzeichneten Geräten zu erlauben. Im Oktober 2022 will Microsoft die Legacy-Anmeldung für alle Mandanten blockieren, mit Ausnahme von SMTP-Authentifizierung. Mandantenübergreifende Richtlinien, die Gäste besser verwalten, befinden sich derzeit in einem Betatest.

Eine empfehlenswerte Informationsquelle zu vielen Themen rund um Azure, besonders aber zum bedingten Zugriff, ist das Blog von Daniel Chronlund (siehe ix.de/z4qh). Er beschreibt weniger bekannte Einstellungen, beispielsweise wie PAWs für administrativen Zugriff verpflichtend gemacht werden können, wie eine Liste der Zugriffseinstellungen nach Excel exportiert oder ihre Bearbeitung mit PowerShell automatisiert werden kann. Er stellt mit der „Conditional Access Baseline“ eine Vorlage zur Verfügung.

Einige Funktionen nur mit teuren Zusatzabos

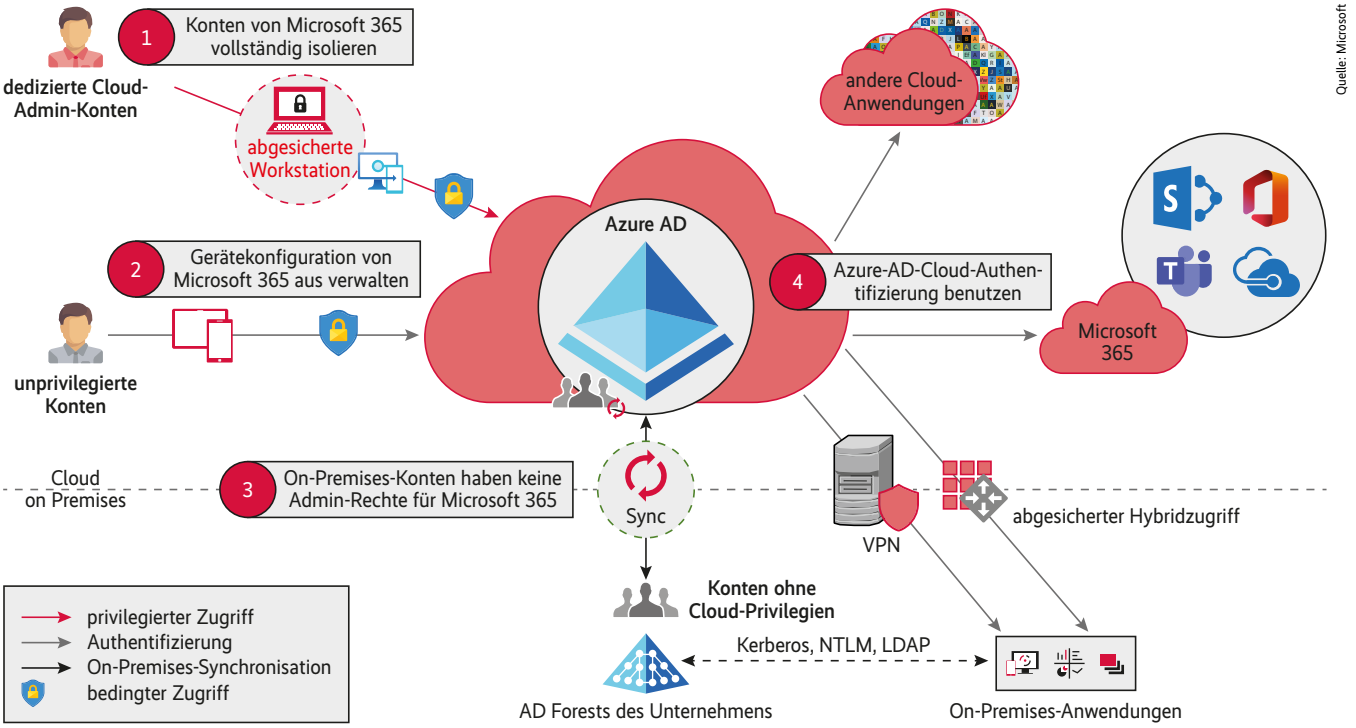
Einige sicherheitsrelevante Funktionen von Azure AD sind leider den teureren Premiumlizenzen P1 und P2 vorbehalten. Regeln für bedingten Zugriff erfordern mindestens eine P1-Lizenz; das ist auch die Voraussetzung dafür, dass Aktivitätsberichte 30 statt nur 7 Tage lang gespeichert werden. Für längerfristige Speicherung müssen Logs ohnehin mit Azure Monitor an ein Speicherkonto weitergeleitet werden; Details finden sich in einer Microsoft-Dokumentation (siehe ix.de/z4). Unabhängig von einer Premiumlizenz können Diagnoseprotokolle für Azure-Dienste aktiviert werden.

Erst mit P2 kann man Just-in-Time-Zugriff (JIT) über das Privileged Identity Management (PIM) einrichten. Dadurch werden Rechte in AAD oder auf Azure-Ressourcen erst dann angefordert und nur kurzzeitig zugewiesen, wenn sie benötigt werden – und bei besonders privilegierten Rollen erst nach einer abermaligen Mehr-Faktor-Authentisierung oder einer Freigabe nach dem Vier-Augen-Prinzip. Außerdem schaltet erst diese Lizenz alle Funktionen von Microsofts Identity Protection frei, darunter Anmelde- und Benutzerrisikorichtlinien. Es ist sehr zu empfehlen, AAD-Rollen wie den globalen oder den Benutzeradministrator ebenso wie dienstbezogene Rollen wie Exchange- oder Teams-Admin mit PIM abzusichern.

Falls ein Unternehmen sparen will, kann es P2-Lizenzen nur für Administratoren beschaffen. In der Praxis reicht bereits eine einzige P2-Lizenzzuweisung aus, damit Identity Protection für alle Benutzer aktiviert werden kann. Einen guten Überblick über Microsoft-365-Lizenzen, den darin jeweils enthaltenen Funktionsumfang und die integrierten AAD-Lizenzen bieten die Feature-Matrix und die zugehörigen Diagramme des Microsoft-Mitarbeiters Aaron Dinnage (siehe ix.de/z4qh).

Mehr-Faktor-Authentisierung für alle Nutzer

Mehr-Faktor-Authentisierung sollte selbstredend in jedem Fall für privilegierte Kon-



Die Prinzipien zum Schutz von Microsoft 365 vor On-Premise-Angriffen gelten generell für Azure AD (Abb. 4).

ten und für reguläre Benutzer aktiviert werden. Obwohl es Phishingtechniken gibt, die Sitzungscookies oder Zugriffstoken abfangen und den zweiten Faktor umgehen, ist MFA ein wichtiger Schutz gegen aktuelle passwortbasierte Angriffe. Es kann direkt am jeweiligen Benutzer oder granular über Regeln für bedingten Zugriff konfiguriert werden, beispielsweise nur bei erkannten riskanten Anmeldungen.

Starke Faktoren wie das Nutzen der Microsoft-Authenticator-App sind veralteten Techniken wie SMS vorzuziehen. Konten für den Notfallzugriff sollte man von Regeln für bedingten Zugriff und MFA ausnehmen, dafür aber besonders überwachen. Mehr Informationen zu MFA in Azure AD finden sich in [6] und zu Notfallkonten in einer Microsoft-Doku (siehe ix.de/z4qh).

Einfache Kennwörter sperren

Als weitere Maßnahme sollten Admins in ihrem AAD unter Kennwortschutz eine benutzerdefinierte Liste gesperrter Kennwörter anlegen, in denen der Name der eigenen Organisation und von Angeboten und Dienstleistungen enthalten ist – und die Sperre erzwingen. Dadurch können Benutzer nicht das schwache Passwort „Unternehmen2022!“ auswählen. Diese Funktion erfordert mindestens eine Premium-P1-Lizenz.

Bei der Bereitstellung von Anwendungen auf Azure sollten Unternehmen darauf achten, welche Risiken die Standardkonfigurationen mit sich bringen. Bei IaaS-Ressourcen wie virtuellen Maschinen sollten so wenig Ports wie möglich offen und Verwaltungsprotokolle wie RDP oder SSH nicht aus dem gesamten Internet zugänglich sein.

Bei jeder öffentlichen IP-Adresse muss ein Systemverwalter sich fragen, ob sie wirklich gebraucht wird, und sie gegebenenfalls absichern. Mindestens sollten Ports, bei denen der öffentliche Zugriff nicht notwendig ist, auf bekannte IP-Adressen beschränkt werden. Netzwerksicherheitsgruppen oder Firewalls können verwendet werden, um den Zugriff zu beschränken. Weitere Lösungen sind Just-in-Time-Zugriff oder Azure Bastion. Auch für PaaS-Dienste wie Speicherkonten kann man den Zugriff auf Netzwerkebene über private Endpunkte einschränken.

Angriff ist die beste Verteidigung

Wer selbst Angriffe auf Azure AD und Azure-Dienste üben, die verursachten Spuren wie Logeinträge untersuchen oder die Auswirkung von Sicherheitsmaßnahmen auf die Machbarkeit einer Attacke prüfen will, kann das kostenfrei tun. In einem eigens angelegten AAD-Mandanten mit einem Azure-Test-Abo und dem GitHub-Projekt XMGoat kann eine kleine verwundbare Konfiguration geschaffen und mithilfe von Musterlösungen kompromittiert werden; in der zugehörigen Befehlsdokumentation wird aber wenig erklärt.

Mehr Hintergründe zu Azure und AAD sowie Anleitungen für Angriffe darauf finden Sicherheitstester und engagierte Cloud-Admins im lesenswerten Buch „Penetration Testing Azure for Ethical Hackers“ von David Okedoye und Karl Fosaaen, erschienen Ende 2021. Die Autoren beschreiben die Installation und Kompromittierung mehrerer größerer Umgebungen mithilfe von Skripten, die sie auf GitHub bereitstellen. Dort findet sich mit „Azure Red Team“ auch eine umfangreiche Befehlssammlung für Sicherheitstester; „Awesome Azure Pentest“ ist eine gute Ergänzung mit vielen Links.

Wer Angriffe mit mehr Anleitung in einer bereitgestellten Azure-Umgebung üben und Schritt für Schritt durch die Angriffsphasen geführt werden will, wird beim Sicherheitsforscher Nikhil Mittal fündig, der schon zum lokalen AD viele Inhalte veröffentlicht hat. Auf der englischsprachigen Onlinelernplattform „Pentester Academy: Bootcamps“ veranstaltet er regelmäßig preiswerte Onlineseminare. Eher interessant für Sicherheitsdienstleister oder größere Organisationen ist die BlackSky-Laborumgebung der Online-Hacking-Plattform Hack The Box; deren

Preise richten sich an Unternehmen. Für die Clouds von Amazon, Google und Microsoft gibt es dort jeweils Übungsszenarien.

Mehr Stoff für Verteidiger

Einen weiteren Überblick über Sicherheitsmaßnahmen mit Fokus auf Microsoft 365, die viel mit AAD zu tun haben, bieten zwei Beiträge in *iX* 7/2021 [7, 8] und für hybride Umgebungen ein Artikel in *iX* 3/2022 [2].

Wer nur ein einziges Dokument von Microsoft zu AAD lesen möchte, findet viele Grundlageninformationen im Whitepaper „Securing Azure environments with Azure Active Directory“ und dessen Anhang, das allerdings nicht ins Deutsche übersetzt wurde. Vor einem Wechsel zu Azure-Diensten empfiehlt sich für Entscheider wie für Architekten ein Blick in Microsofts Framework für die Cloud-Einführung (Cloud Adoption Framework), das unter anderem Referenzen und Implementierungsleitfäden sammelt und über einen großen Bereich zu Sicherheit verfügt. Ebenfalls einen Blick lohnt der entsprechende Abschnitt in der Azure-Dokumentation mit grundlegenden Informationen zu Azure Active Directory, der bereits mehr in die Tiefe geht.

Für Cloud-Admins, die sich in den Details für das Absichern von Azure fit machen wollen, bietet Microsoft die Zertifizierungsprüfung „AZ-500: Microsoft Azure-Sicherheitstechnologien“. Dazu stellt das Unternehmen auf Deutsch kostenfreies Lernmaterial zur Verfügung sowie englischsprachige Übungen für eine Azure-Testumgebung. Das lesenswerte Buch „Microsoft Azure Security Technologies Certification and Beyond“ von David Okedoye bereitet als einzelne Lernunterlage ähnliche Inhalte auf und streut zahlreiche Praxisszenarios mit herunterladbaren Einrichtungsvorlagen ein. Analog zu Azure stellt Microsoft Lernmaterial zur Zertifizierungsprüfung MS-500 bereit, die sich mit Microsoft-365-Sicherheitsadministration befasst. Dazu gibt es auf Englisch das im Eigenverlag erschienene Buch „Securing Microsoft 365“ von Joe Stocker.

Wie Angreifer in hybriden Umgebungen vorgehen und wie man sie dort aufspürt, beschreibt der Konferenzbeitrag „Who owns your hybrid Active Directory? Hunting for adversary techniques“. In Bezug auf eine konkrete Angreifergruppe beschreibt das Whitepaper „Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452“, wie Hacker von lokalen Umgebungen auf die Cloud überspringen. Zur Absicherung von Azure AD Connect hilft ein Beitrag von Trimarc Security, auf deren Blog man weitere hilfreiche Beiträge findet.

Fazit

Microsoft entwickelt seine Azure-Dienste für IaaS und PaaS, das SaaS-Angebot Microsoft 365 und den zugrunde liegenden Identitätsdienst Azure AD ständig weiter und ergänzt regelmäßig neue Sicherheitsfunktionen. Viele alte und neue Funktionen müssen jedoch vor dem Einsatz konfiguriert werden. Zudem kann eine unbedachte Einstellung Lücken in die Verteidigung reißen. Die Konfiguration von Azure AD sollte dementsprechend nicht als einmaliger Vorgang betrachtet werden, sondern als kontinuierlicher Prozess. Dann können Admins ihre Cloud-Umgebung gut sichern. (ulw@ix.de)

Quellen

[1] Christoph Puppe; Krähennest in der Wolke; Cloud Security Operations Center im Vergleich; *iX* 7/2021, S. 88

[2] Inés Atug, Matthias Reintges; Zu Diensten; Active Directory grundschutzkonform absichern; *iX* 3/2022, S. 90

[3] Marco Wohler; Mehr ist mehr; AD-Härtungsmaßnahmen jenseits von Group Policies; *iX* 6/2021, S. 92

[4] Frank Ully; Fette Beute; Passwörter und Hashes – wie Angreifer die Domäne kompromittieren; *iX* 11/2020, S. 94

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

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

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

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

[9] Alle im Artikel erwähnten Werkzeuge, Blogartikel und Microsoft-Dokumente sind über ix.de/z4qh zu finden.

Frank Ully

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