Sonderheft I/2023

ISSN 1614-2888
€ 29,90
it-administrator.de

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Sonderheft

Cloud Security

Sicherheit in Microsoft Azure

Undurchlässig

von Klaus Bierschenk

Planen IT-Verantwortliche, Teile der lokalen Infrastruktur dauerhaft nach Azure auszulagern, sollten sie die Sicherheit nicht aus den Augen verlieren. In der Cloud warten hier ganz neue Security-Aspekte – und das gleich auf verschiedenen Ebenen. Wir liefern einen Überblick jener Features, die Azure bereitstellt, um Cloudinfrastrukturen wasserdicht zu gestalten.

Quelle: masarik512 – 123RF

Sicherheitsthemen in Azure begegnen dem Administrator gleich mehrfach. Angefangen beim Protokollieren, um zu sehen, wo Systeme verwundbar sind, bis hin zur Definition von administrativen Rollen, um Aktivitäten einzelnen Mitarbeitern zu gestatten. Dies ist in der Cloud besonders wichtig, denn im lokalen Rechenzentrum lassen sich physische Server nicht mit wenigen Mausklicks löschen, in Azure sehr wohl. Die meisten größeren IT-Landschaften setzen daher auf ein Rollenkonzept. Dies hilft dabei, die Infrastruktur zu schützen, und bietet dem Admin Sicherheit bei seiner täglichen Arbeit.

Eine gute Beschreibung eines solchen Verwaltungsmodells bietet Microsoft [1]. Es teilt die Administration in drei Ebenen ein und je nach dem, was ein Administrator beabsichtigt, bedient er sich eines Benutzerkontos der jeweiligen Ebene, das die entsprechenden Berechtigungen bietet. Ebene 0, auch T0 genannt, hat die umfangreichsten Rechte. Bezogen auf das Active Directory wäre dies die Gruppe "Organisations-Admins". Konten der Ebene T1 administrieren Server und Applikationen und Konten der Ebene T2 besitzen die Rechte, die für die Datenpflege vonnöten sind. Der Administrator meldet sich dann je nachdem, was er beabsichtigt, mit dem entsprechenden Konto an.

Im besten Fall findet sich dieses Modell auch in Ihrem Namenskonzept wieder, sodass zum Beispiel Herr Müller das Konto "adm-mueller.0" als "Organisations-Admin" (oder "Enterprise Admin" in einem englischsprachigen AD) nutzt. Für alle anderen Arbeiten bedient er sich des Kontos "adm-mueller.2". So ist bereits auszuschließen, dass der hochprivilegierte Kontext missbraucht wird. Mit mehreren Konten zu hantieren, bereitet auf den ersten Blick Mühe und nervt, bietet dafür aber Schutz. Beziehen Sie nun Elemente aus Azure in ihre IT-Landschaft mit ein, gilt es, bestehende Gruppen- und Rollendefinitionen in Richtung Azure zu erweitern.

Lokale Konten für die Cloudadministration

In etablierten IT-Landschaften existieren je nach Aufgabengebiet entsprechende Berechtigungsgruppen. So gibt es Gruppen für die Serveradministration bis hin zur Rufbereitschaft. Egal, ob Sie nun Microsoft 365 oder Azure für IaaS einsetzen: Benutzerkonten und Gruppen, die den Zugriff innerhalb der Clouddienste regeln, befinden sich immer im entsprechenden Azure AD.

Selbstverständlich können Sie die administrativen Gruppen ebenfalls im Azure AD anlegen, jedoch hätte so der Administrator zwei Orte, an denen er User- und Gruppenpflege betreibt – das lokale Active Directory und in der Cloud. Das ist aufwendig und kaum zu managen. Zum Glück geht das einfacher und lässt sich per Azure AD Connect automatisieren. Hierdurch haben Sie die Möglichkeit, Benutzerkonten (und natürlich Gruppen) aus dem lokalen AD (on-premises) mit dem Azure AD zu synchronisieren. Diese Vorgehensweise ist in erster Linie für Microsoft 365 gedacht, um bei größerer Anzahl Benutzer diese in die Cloud zu transferieren, um ihnen dort Lizenzen für Applikationen zuzuordnen.

Aber auch wenn Sie kein Microsoft 365 einsetzen, kann es hilfreich sein, auf die Synchronisation zu setzen, und sei es nur, um administrative Konten in die Cloud zu spiegeln, um sie im nächsten Schritt dort für Ressourcen zu berechtigen. Dies bietet den Vorteil, dass Benutzergruppen nur an zentraler Stelle, nämlich im lokalen Active Directory, zu pflegen sind – so wie bisher. Lediglich für die Cloud relevante, neue Aspekte wie Änderungen am Namenskonzept oder auch neue Gruppen, weil in Azure andere Objekte existieren und die Tätigkeiten verschieden sind, wären anzupassen.

Es ist daher überaus sinnvoll, sich im Vorfeld über die Gruppen und Definitionen klar zu werden. Danach haben Sie nichts weiter zu tun, als im lokalen AD die Admins in die Gruppen zu packen, den Rest erledigt Azure AD Connect im Zuge der Synchronisation. Wie ein Azure AD Connect Server eingerichtet wird, zeigt der Artikel ab Seite 86 im Detail. Eine Beschreibung von Microsoft

zu diesem Thema finden Sie zudem im Internet unter [2].

Ressourcenhierarchie und Vererbung

Gehen wir davon aus, dass Ihr Azure AD Connect eingerichtet ist, sieht das an einem Beispiel wie folgt aus: Angenommen Sie haben die Gruppe "ROL-ResGrp-Admin" im lokalen Active Directory und möchten diese für die Verwaltung aller virtueller Maschinen in Azure einsetzen. Damit Sie diese in Azure anwenden können, ist die Erfüllung von zwei Voraussetzungen erforderlich. Zum einen muss die Gruppe im Azure AD Ihres Azure-Abonnements vorhanden sein. Was sich logisch anhört, ist keinesfalls selbstverständlich – besonders, wenn Sie Microsoft 365 und Azure separat erworben haben. Mehr dazu später.

Zum anderen ist es wichtig, dass der Gruppe in Azure innerhalb des Abonnements die jeweiligen Rechte eingeräumt sind. Hierzu gibt es eine Vererbungshierarchie, ähnlich wie im Dateisystem. Weisen Sie Berechtigungen für ein Abonnement zu, was in der Vererbungshierarchie sehr weit oben ist, hat dies Auswirkungen auf alle Objekte in dem Abo. Eine Ressourcengruppe ist Teil eines Abos und es können durchaus mehrere vorhanden sein. Vergeben Sie nun Berechtigungen für Ressourcengruppen, könnten zum Beispiel zwei Administratorteams die virtuellen Computer in der jeweiligen Ressourcengruppe managen, da die Rechte nur dort gelten.

Dies ist ein sehr leistungsstarker Mechanismus und erfordert gründliche Planung. Nicht nur bei der Vergabe von Berechtigungen, auch beim Anlegen der Objekte in Azure. Getrennte Admin-Bereiche können nämlich ein Grund sein, VMs auf verschiedene Ressourcengruppen zu verteilen. Bild 1 zeigt die Berechtigungen für eine VM. Alle hier eingetragenen Benutzer stammen aus dem synchronisierten On-Premises-Active-Directory, das in unserem Beispiel den Domänennamen "kbcorp.de" hat. Eine Ausnahme in der Liste ist der Besitzer "Klaus Bierschenk". Hierbei handelt es sich um das erste Konto des Abonnements, das gleichzeitig "Globaler Admin" ist. In der Spalte "Scope" sehen Sie, ob die Berechtigung auf eine Ressource vergeben ist oder ob sie vererbt wurde. Auf diese Art lassen sich für alle zu administrierenden Objekte in Azure wie auch beispielsweise "Virtuelle Netzwerke" Berechtigungen vergeben. Selektieren Sie hierfür jeweils den Link "Zugriffssteuerung (IAM)" in der Befehlsleiste und behalten Sie die Vererbung im Auge.

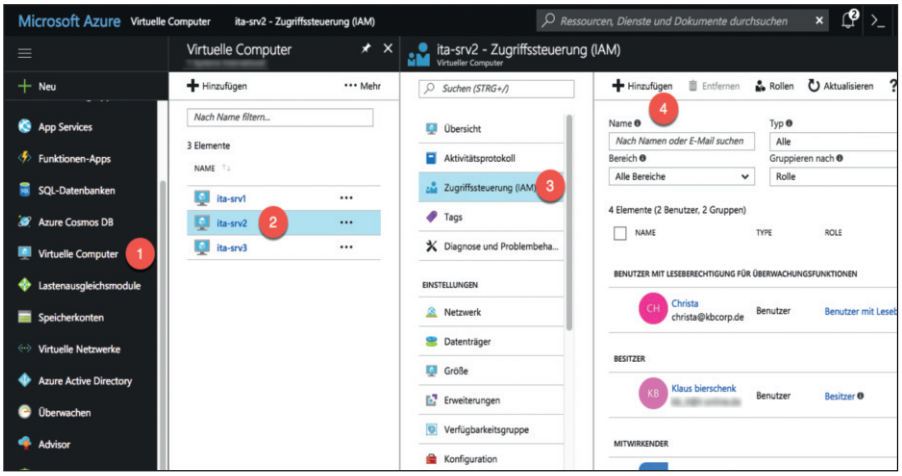

Bild 1: Über die Zugriffssteuerung gelangen Sie zu den Berechtigungen in Azure.

Feinschliff auf der Kommandozeile

Zeigen Sie die Berechtigungen für eine VM an, wie in Bild 2 zu sehen, finden Sie detaillierte Auskunft über die Rollen, Zuweisungen und letztlich die damit im Zusammenhang stehenden Berechtigungen für das jeweilige Objekt. Die Hauptaufgabe hier ist es, Zuweisungen einzurichten. Die Seite eignet sich aber genauso gut, um unter Angabe eines Benutzers dessen Möglichkeiten für dieses Objekt zu erkunden. Das ist sicherlich für Infrastrukturen von Interesse, in denen viel mittels Vererbung und Verschachtelungen gearbeitet wird.

Sollten Sie in der Vielzahl an vordefinierten Rollen nicht fündig werden, können Sie Ihre eigenen benutzerdefinierten erstellen. Dies ging lange Zeit nur von der Kommandozeile aus, mittlerweile klappt es aber auch im Azure Portal. Entscheiden Sie sich für die Kommandozeile, können Sie hierfür die Azure PowerShell, die Azure Kommandozeilenschnittstelle (CLI) oder die REST-API bemühen [3]. Trotz der Menge an vordefinierten Rollen be-

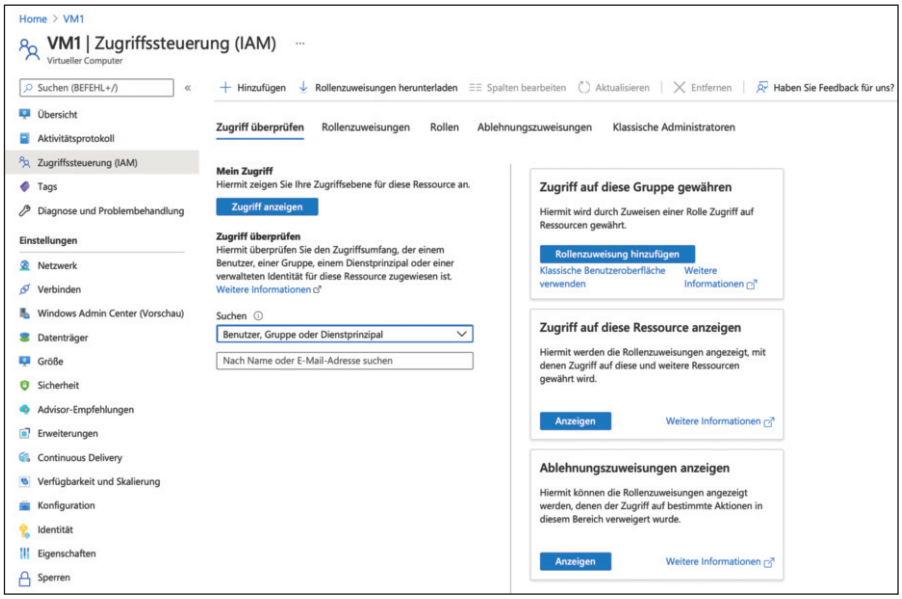

Bild 2: Über den Punkt "Zugriffssteuerung" erfahren Sie, wie die Rollen und die Rechte konfiguriert sind.

nötigt jede IT-Infrastruktur ihren individuellen Feinschliff, der eine Anpassung der Rollen nach sich zieht.

Übrigens finden Sie im persönlichen Menü (oben rechts im Portal) eine Übersicht mit allen Zugriffsmöglichkeiten in Azure. Durch Klick auf den Benutzernamen und dann auf "Weitere Optionen (…)" und "Meine Berechtigungen" aus dem Menü informiert eine neue Seite zu allen vorhandenen Abonnements über die Mitgliedschaften in den jeweiligen Gruppen. Auch hier wird nicht unterschieden, ob es sich um Gruppen handelt, die in Azure angelegt wurden, oder ob die Gruppen aus dem On-Premises-AD stammen.

Wenn Sie sichergehen möchten, dass bestimmte Elemente nicht geändert oder gar gelöscht werden, können Sie unabhängig von allen getroffenen Berechtigungen sogenannte "Sperren" einrichten. Diese lassen sich auch nicht mit den höchsten Berechtigungen umgehen, ohne die Sperre selbst zu entfernen. Sie finden die Sperren in der Leiste links bei den Eigenschaften und Optionen zu einem selektierten Element.

Azure-Login absichern

Manche administrative Konten besitzen so weitreichende Rechte, dass eine Anmeldung mit mehrstufiger Authentifizierung (Multi Factor Authentication, MFA) sinnvoll ist. Erlangt beispielsweise jemand Kenntnis über das Passwort des "Globalen Administrator", nutzt ihm das wenig, wenn er den zweiten Faktor nicht in Händen hält. Für eine Erstimplementierung ist wichtig zu unterscheiden, was es abzusichern gilt und wo die Benutzerkonten liegen, für die ein zweiter Faktor beim Anmelden Bedingung sein soll.

Dies sollte basierend auf der Kritikalität bestimmter Rollen umgesetzt werden und hierfür bietet sich Privileged Identity Management (PIM) an, das es ermöglicht, für Administrative Rollen zeitlich limitierte Mitgliedschaft anzufordern. Sei es unter der Zuhilfenahme einer Genehmigung (Approval) durch Dritte oder durch ein Self-Approval, das zum Beispiel ein MFA einfordert. Das Ganze ist kombinierbar und auf Ebene jeder Sicherheitsrolle ermöglicht es Ihnen je nach Sensibilität einzelner Rollen eine stärkere Absicherung oder auch nicht.

MFA lässt sich für einzelne Benutzer oder für größere Landschaften mittels CSV-Datei für mehrere Benutzer aktivieren. Ausgangspunkt hierfür ist in jedem Fall das "Dashboard" des Active Directories im Azure-Portal. Wechseln sie zur Ansicht "Alle Benutzer", können Sie im Bildschirm oben über die Schaltfläche "Multi-Factor Authentication" alle für die Benutzerobjekte geltenden MFA-Einstellungen vornehmen. Meldet sich der Benutzer nun das nächste Mal mit seinem Konto im Browser an, wird er gezwungen, die MFA erstmalig einzurichten. Dies gilt für einfache Benutzerkonten genauso wie für administrative Konten.

Bleiben wir beim Administrator und gehen wir davon aus, dass dieser heutzutage nicht wenige Benutzerkonten und Kennwörter verwalten muss. In diesem Fall kann er sich das Leben richtig einfach machen, wenn er die "Authenticator App", erhältlich für Android und iOS, verwendet. Das Schöne daran ist, dass in diesem Fall "einfacher" nicht automatisch "weniger sicher" heißt – im Gegenteil, die Authenticator App bietet passwortloses Anmelden oder auch anderweitige Anwendung des zweiten Faktors, wie die simple Selektion eines Codes, der im Login angezeigt wird, oder auch nur die Bestätigung, dass die Anmeldung aktuell angefragt ist.

Neben dieser doch eher statischen Verteilung von MFA an Benutzer und auch Administratoren gibt es zusätzlich noch die Möglichkeit, MFA über Conditional Access Policies einzufordern. Dies ergänzt sich mit dem zuvor Genannten und hat den Charme, MFA situationsbezogen zusätzlich und erneut zu aktivieren. Geräte oder Standorte sowie unterschiedliche Applikationen sind die Kriterien, die dabei zum Einsatz kommen.

Sehen wir uns das Beispiel der IT-Administratorin Christa aus der "kbcorp.de" an. Sie wird bei der nächsten Browseranmeldung am Portal aufgefordert, MFA zu konfigurieren. Wenn sie bei der Sicherheitsüberprüfung "Mobile App" selektiert anstatt "telefonische Benachrichtigung" oder dergleichen, kann sie über die Webseite direkt die "Authenticator App" einrichten. In der App scannt sie den auf dem Bildschirm angezeigten QR-Code, um ihr Konto einmalig hinzuzufügen. So wird sichergestellt, dass die Person, die sich anmeldet, auch im Besitz des Geräts ist.

Ist alles abgeschlossen, lässt sich das Smartphone auf verschiedene Arten verwenden: Entweder wird beim Login ein angezeigter Software-Token eingegeben oder für Konten, deren Benutzer es ganz einfach haben möchten, kann stattdessen eine Benachrichtigung in der App angezeigt werden. Sie können sich zudem festlegen, per Touch-ID oder Face-ID den zweiten Faktor zu bedienen, je nachdem wie das Smartphone ausgestattet ist und für was Sie sich beim Einrichten entschieden haben.

Das ist großes Kino, wenn der Administrator mehrere Konten besitzt, denn in der App lassen sich auch Microsoft-Konten hinterlegen – und diese sind bekanntlich nicht nur für die Anmeldung am Azure-Portal vonnöten, sondern begegnen dem Administrator laufend, zum Beispiel auch, wenn er sich bei MSDN anmeldet. Microsoft ist stetig bestrebt, den Umgang mit verschiedenen Passwörtern zu vereinfachen, und verbessert die Integration der Authenticator-App als

Grundlegende Verzeichnisrollen

An dieser Stelle sei noch auf drei grundlegende Verzeichnisrollen hingewiesen. Unabhängig von weiteren Gruppenmitgliedschaften kann ein Benutzerobjekt im Azure AD eine von drei vordefinierten grundlegenden Rollen innehaben. Standardmäßig ist einem Benutzerkonto die Verzeichnisrolle "Benutzer" zugeordnet. Daneben existiert noch "Gobaler Administrator", den Sie gut hüten sollten, denn er hat die umfassendsten Berechtigungen, ähnlich einem Organisations-Admin in den Active Directory Domain Services. Zu guter Letzt wären da noch die eingeschränkten Administratoren. Die Möglichkeiten und welche Rollen sich dahinter verbergen, sehen Sie anhand der selbsterklärenden Namen der Verzeichnisrollen.

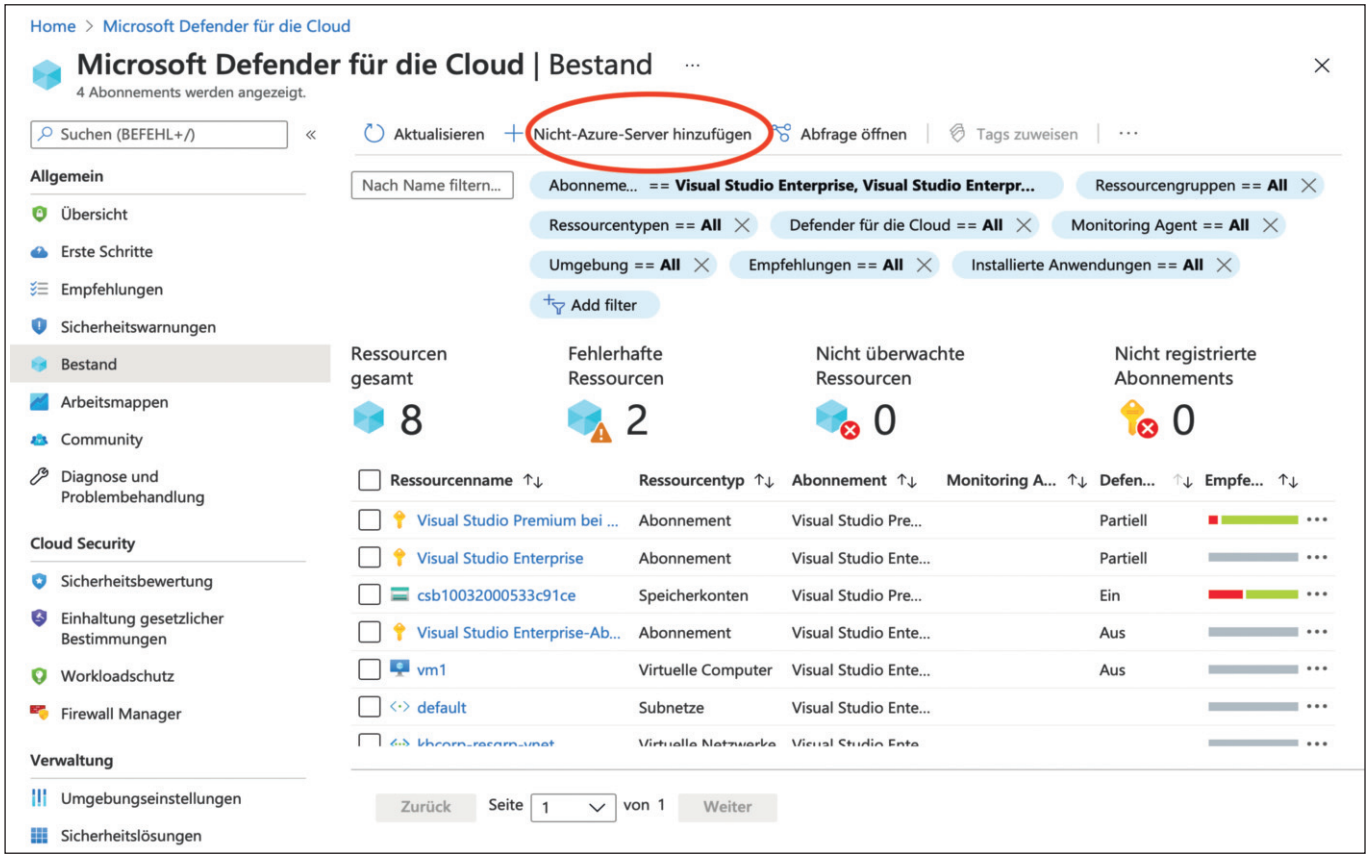

Bild 3: Unter dem Punkt "Bestand" im Defender-Dashboard fügen Sie bei Bedarf auch Nicht-Azure-Server hinzu.

Bestandteil der Anmeldung seit Jahren kontinuierlich.

Sicherheit im Blick behalten

Microsoft Defender for Cloud, ehemals Security Center, versteht sich als Werkzeug, das dabei hilft, der Sicherheit in der Azure-Umgebung auf den Zahn zu fühlen. Defender ist in der Zwischenzeit eine umfassende Suite und der Begriff "Defender" taucht in der Microsoft-Cloudwelt verschiedentlich auf, sowohl bezogen auf die Infrastruktur in Azure als auch in Microsoft 365. Im Portal selbst ist hier und dort noch vom Security Center die Rede, Microsoft nimmt es mit den Begrifflichkeiten hier nicht so genau.

Bezogen auf unseren Schwerpunkt in diesem Beitrag, in dem es uns um die Absicherung von Ressourcen im hybriden Umfeld geht, ist zum Beispiel von Bedeutung, wie Server in Azure oder auch on-premises in die Bewertungen und Analysen einfließen können. Hierfür ist auf den Servern der Log-Analytics-Agent notwendig. Er lässt sich automatisch installieren oder auch aus dem Portal herunterladen, um ihn dann auf Server im Rechenzentrum zu verteilen. Für den manuellen Weg navigieren Sie im Defender-Dashboard zum Bereich "Bestand" und können hier über den entsprechenden Befehl "Nicht-Azure-Server" sowohl Windows- als auch Linux-Server hinzufügen.

Die dazu notwendigen Agenten stehen zum Download bereit, Sie müssen hier lediglich die Bereichs-ID und den primären Schlüssel über die Zwischenablage auf dem lokalen Server beim Setup hinzufügen und schon ist der Server aus dem Rechenzentrum Teil des Bestands im Security Center. Übrigens: Wenn Sie im Rechenzentrum Server ohne Internetzugriff besitzen, besteht die Möglichkeit, über ein Log Analytics Gateway, eine Art Proxy, die Konnektivität zu Azure herzustellen, um diejenigen lokalen Server bei den Sicherheitswarnungen zu berücksichtigen.

Zugriff auf virtuelle Server einschränken

Über den Defender-Plan besteht die Möglichkeit, den Zugriff auf virtuelle Server abzusichern. Die Funktion hierfür heißt "JIT-VM-Zugriff" (Just-In-Time). Hier wird sich der Netzwerksicherheitsgruppen (NSG) bedient und für den Zugriff notwendige Ports werden nur auf Anforderung geöffnet, indem eine temporäre NSG zugewiesen wird. Diese gestattet den Zugriff für einen bestimmten Zeitraum und wird dann wieder entfernt, wodurch der Zugriff auf die VM wieder erlischt.

Administratoren können nun den Zugriff anfordern, indem sie zum Bereich "JIT" navigieren und dort für die entsprechende VM "Zugriff anfordern" wählen. Genauso können Sie aber in den Eigenschaften der VM unter "Einstellungen" den Befehl "Verbinden" selektieren. Hier erscheint nun der Hinweis, dass der Zugriff erst angefordert werden muss, was Sie an Ort und Stelle auslösen können.

Das Ergebnis ist jeweils das Gleiche: Ist der Zugriff angefragt, wird eine zusätzliche Netzwerksicherheitsgruppe erstellt, mit den Portregeln, die den Zugriff gestatten, und zwar mit genau der Quell-IP-Adresse der Admin-Workstation, von der die Anfrage kam. Die NSG bleibt für

den angegebenen Zeitraum zugeordnet und hat die höchste Priorität, setzt somit die zuvor erstellte NSG erst einmal außer Kraft. Ist der Zugriff wieder beendet, wird sie gelöscht und übrig bleiben dann wieder die ursprünglichen NSGs, die den Zugriff einschränken.

Auf einen Aspekt sei hier noch hingewiesen, und zwar befindet sich in der Liste mit den für JIT konfigurierten VMs rechts das Dreipunkte-Menü. Hier haben Sie die Möglichkeit, nachträglich Änderungen an den Ports vorzunehmen. Genauso findet sich hier, leider aber etwas versteckt, ein Aktivitätsprotokoll mit Hinweisen darüber, wer wann den Zugriff für eine VM angefordert hat.

Kostenlose oder kostenpflichtige Pläne

Standardmäßig ist in "Defender für die Cloud" eine fortlaufende Security-Bewertung verbunden mit Empfehlungen für alle Ressourcen aktiv. Möchten Sie aber weiteren Schutz, zum Beispiel Bedrohungsschutz für VMs oder den JIT-VM-Zugriff nutzen, müssen Sie den sogenannten Defender-Plan aktivieren. Das kling erst einmal verwirrend, wird aber klarer, wenn Sie im Microsoft-Defender-Portal in den Bereich "Umgebungseinstellungen" navigieren und dort eine Subscription selektieren. Hier lässt sich bezogen auf einzelne Elemente in Ihrer Azure-Infrastruktur der Defender-Plan ein- oder ausschalten, sogar auf Ebene der einzelnen Funktionen. In früheren Versionen des Security Centers war hier auch von einem "Standard Plan" die Rede. Dieser Begriff taucht heute noch in der einen oder anderen Dokumentation auf.

Mittlerweile heißt es einfach nur Defender und Sie sehen hier, welche Funktionen geboten sind. Dabei ist auch schnell ersichtlich, dass nur der Defender-Plan wirklich Sinn ergibt. Werkzeuge wie "JIT-VM-Zugriff" oder auch die "Berichte zur Einhaltung gesetzlicher Bestimmungen" sind wichtige Funktionalitäten, die eigentlich kaum ein Administrator vermissen möchte. Für ein Feintuning und zur Kostenkontrolle lassen sich aber auch Ressourcen im Wirkungskreis von Defender ein- und ausschließen, was das Ganze preislich entzerrt. So kann zum Beispiel Defender in Bezug auf virtuelle Maschinen eingesetzt werden, bei SQL-Datenbanken ließe sich, wenn gewünscht, darauf verzichten.

Entwicklungs- und Trainingsumgebung

Unkenntnis ist oftmals ein Risiko. Aber wie Kenntnis über etwas erlangen, ohne Dinge auszuprobieren? Nicht jeder Administrator hat verschiedene Abonnements zur Hand, um in getrennten Umgebungen Szenarien durchzuspielen. Da kommen die DevTest Labs gerade richtig. Sie können beliebig Umgebungen einrichten, hier Lab genannt, und darin quasi eine Parallelinfrastruktur mit Benutzern, Netzwerken, virtuellen Maschinen und was sonst noch alles dazu gehört aufbauen. Dieses Feature ist besonders für Unternehmen interessant, die eine größere Anzahl Administratoren haben, die sich mit den neuen Technologien beschäftigen möchten, oder auch für Entwickler und deren Applikationstests. Sie haben die Kontrolle über die Kosten, indem Sie entweder pro Lab oder pro Benutzer definieren, wie viele VMs bereitgestellt werden.

Sie können von zentraler Stelle aus VM-Images bereitstellen, die von den Lab-Benutzern abgerufen werden und deren Größe limitiert ist, um Wildwuchs zu vermeiden. Ein gesamtes Lab lässt sich zu einem definierten Zeitpunkt herunterfahren, um unnötige Kosten zu vermeiden. All das charakterisiert eine Test- und Spielumgebung, ohne eine Produktionsumgebung in irgendeiner Weise zu gefährden. Azure DevTest Labs [4] ist kostenlos. Berechnet werden Ihnen lediglich die Ressourcen und die Nutzungszeit, die Sie darin verwenden.

Weitere Schutzmechanismen

Ein weiteres Sicherheitsfeature ist die Verschlüsselung von virtuellen Festplatten in Azure. Zugegeben, die Handhabung von Schlüsseln und Verschlüsselungsschlüsseln in Azure Key Vaults ist nichts, was ein Administrator nebenbei aus dem Hut zaubert, insbesondere wenn er neu im Thema ist. Aber die Komplexität ist auch ein Garant für Leistungsfähigkeit und die gute Nachricht ist, dass Microsoft Docs sehr gute Artikel bereithält, die die Sachverhalte einfach erklären, besonders Themen wie Verschlüsselung. Auffällig dabei ist, dass eine Vielzahl der Artikel nicht mehr durch Roboter übersetzt wurde, sondern direkt in deutscher Sprache verfasst ist, was das Lesen sehr viel angenehmer gestaltet.

Es ergibt Sinn, für Azure-Server mit sensiblen Daten über eine Serverhärtung nachzudenken. Hierfür stellt Microsoft das Security Compliance Toolkit (SCT) bereit, das quasi eine Weiterführung des Security Compliance Managers darstellt, den einige Administratoren eventuell noch kennen und den Microsoft im Sommer 2017 bereits in Rente geschickt hat. Seine Aufgabe damals war, im Bereich der Härtung vordefinierte Richtlinien für Windows Server 2016 auszuliefern, sogenannte Baseline Policies. Diese Lücke schließt das Compliance Toolkit.

Fazit

Security ist ein weites Themenfeld für IT-Verantwortliche. Das war zu Zeiten so, als Server noch ausschließlich viereckige Kisten waren und im Rechenzentrum für Wärme sorgten. Und in Zeiten virtueller Infrastrukturen, in denen Ihr wichtigstes Gut, nämlich Ihre Daten, irgendwo auf dem Globus in Microsoft-Rechenzentren liegen, ist das wichtiger denn je. Da heißt es: am Ball bleiben und permanent Dinge auf den Prüfstand stellen. Es ist nicht notwendig, jedem Trend zu folgen und auf jedes Pferd zu setzen, das Microsoft in Microsoft 365 oder in Azure aufzäumt. Aber die Funktionen, die uns Redmond mitgibt, um Infrastrukturen zu schützen, wachsen bei alldem mit. *(dr)*

Link-Codes

[1] Sicherer privilegierter Zugriff mithilfe eines Rollenkonzepts
i2z51

[2] Azure AD Connect einrichten
i2z52

[3] Benutzerdefinierte Rollen erstellen
i2z53

[4] Azure DevTest
i2z59