Herausforderung Cloud-Sicherheitsrichtlinien

Know-how Bei der Verlagerung von Services in die Cloud mangelt es oft an einer Sicherheitsstrategie. Die immer komplexer werdenden Umgebungen mit hybriden Zugangssystemen, verschiedensten Geräten und Betriebssystemen verlangen nach einer regelmässigen Überprüfung.

Von Jonas Hofer

Cloud Computing ist in der Regel untrennbar mit mobiler Anwendung von Services und in den allermeisten Fällen auch mit vielen unterschiedlichen Endgeräten (Stichwort Bring your own Device, BYOD) verbunden. Umso erstaunlicher ist es, dass viele Firmen in Sachen Security ihren Fokus nach wie vor auf PC und Laptops und das Windows-Betriebssystem legen. Android, iOS und MacOS geraten dabei meist in Vergessenheit oder die bestehenden Möglichkeiten werden nicht sinnvoll ausgeschöpft. Dabei ist es allein schon bei reinen Microsoft-Umgebungen nicht ganz trivial, den Durchblick im Dschungel der Zugriffsberechtigungen zu behalten. Aktuell ist es indes so, dass man, wenn man von Cloud und Sicherheit spricht, damit Microsoft Azure Active Directory (AAD) und die EM+S (Enterprise Mobility and Security) Suite mit dem Gerätemanagementsystem Intune meint. Denn viele Firmen haben ihre Daten mittlerweile auf Microsoft-365-Services wie Exchange Online, Sharepoint Online und anderen abgelegt. Selbstverständlich lassen sich Geräte nach wie vor auch mit den etablierten Lösungen wie Mobileiron verwalten und es sind andere Identity-Provider wie ADFS, Ping oder Okta im Einsatz. Der Trend zu einer umfassenden Microsoft-Beschaffungsstrategie auch in Hinblick auf die Geräteverwaltung ist aber klar im Markt zu erkennen.

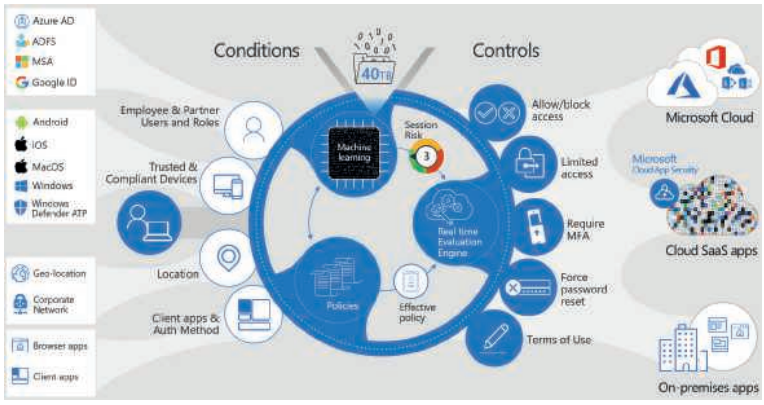
Hybrid und komplex – auch bei Microsoft-only

Das bedeutet allerdings noch lange nicht, dass damit die Komplexität aus dem Weg geräumt ist. Einerseits bleibt es bei den Cloud-Diensten, welche von den Nutzern konsumiert werden, in der Regel nicht bei Services des Software-Riesen. Die Mehrzahl der Unternehmen nutzt zusätzlich auch Produkte von Drittanbietern wie etwa Salesforce, Dropbox for Business und viele mehr. Selbst wenn also Identitäten und User Accounts sowie Geräte mit der Microsoft-Cloud verwaltet werden, müssen alle Services, also auch fremde, mit heterogenen Hard- und Software-Umgebungen klarkommen. Auch kommt als Identity-Provider selbst bei einem starken Microsoft-Fokus noch lange nicht ausschliesslich AAD zum Einsatz. Denn die Nutzer-Accounts werden nach wie vor auch On-Premises mit Active Directory, dem Verzeichnisdienst für Microsoft Windows Server, verwaltet. Bei hybridem Identity- und Access-Management (IAM) werden demzufolge die Benutzer- und Gruppeninformationen aus Active Directory in die AAD-Cloud hochsynchronisiert. Was die Geräteverwaltung angeht, ist auch hier ein Trend zu Microsoft Endpoint Manager (Intune) festzustellen. Es gibt allerdings aus technischer Sicht keinen Grund, die mobilen Endgeräte nicht weiterhin mit Mobileiron, Vmware oder anderen zu verwalten. Im Gegenteil ist dies beispielsweise für nicht Webbasierte, zum Beispiel ältere firmeneigene Anwendungen, mit Intune allein gar nicht machbar. Das ganze Microsoft-Ökosystem ist allerdings ein sehr viel weitergehendes Feld als die vergleichsweise kleine Welt des Gerätemanagements.

Kontrolle zwischen Gerät und Cloud-Dienst

Die Herausforderung in der Cloud besteht kurz gesagt darin, die Verbindung zwischen Endgeräten und Services im Griff zu haben. Dabei muss man sich immer vor Augen führen: Bei Cloud Services obliegt die Kontrolle der Plattform beim Anbieter. Es handelt sich um einen fremden Rechner, auf den man seine Nutzer mit Geräten unterschiedlichster Art

AZURE ACTIVE DIRECTORY CONDITIONAL ACCESS



Quelle: Nomasis

In Azure Active Directory Conditional Access werden Zugriffsberechtigungen und Kontrollmechanismen definiert.

zugreifen lässt. Umso erstaunlicher ist es, dass bei Cloud-Anwendungen in den allermeisten Fällen die Kontrolle für die Sicherheitsrichtlinien auf den (mobilen) Endgeräten fehlt. Es geht zum Beispiel oftmals schlicht vergessen, dass die Dienste und entsprechend die abgelegten Daten auf den Geräten «default open» eingerichtet sind. Selbst wenn man zusätzlich zu den üblichen Office- und Sharepoint-Services nur Microsoft-Anwendungen wie Teams oder One Drive verwendet, lohnt es sich, vor jedem Service-Rollout genau zu prüfen, wer von wo mit welchem Gerät darauf zugreifen darf und was mit den Daten passiert, wenn sie auf den Geräten ankommen. Man darf hier also getrost von einer komplexen und wiederkehrenden Herausforderung sprechen. Es herrscht denn auch bezüglich Cloud und Sicherheit bei den Sicherheitsverantwortlichen eine entsprechende Unsicherheit. Das muss allerdings nicht zwingend zu einem Problem werden, wenn man von Anfang an strukturiert vorgeht und vor allem die Situation regelmässig circa alle sechs Monate neu beurteilt. Die Erfahrung zeigt nämlich, dass infolge veränderter Voraussetzungen, zum Beispiel Upgrades oder durch den Rollout zusätzlicher neuer Services oder infolge konkreter Massnahmen bei der Umsetzung einer Cloud-Strategie, die Unternehmen in den letzten Jahren ihre Sicherheitsrichtlinien mehrmals neu beurteilen mussten.

Zugang nur unter gewissen Bedingungen

Hier kommt nun Conditional Access für AAD ins Spiel. Mit diesem Zugriffskontrolldienst können Richtlinien für bedingten Zugriff von Nutzeridentitäten und Geräten definiert werden. Es handelt sich also um ein Werkzeug mit einer Wenn-Dann-Regel, die aus Zuweisungen und Zugriffskontrollen besteht. Hier werden User Accounts kontrolliert, wenn sich Nutzer einloggen und gleichzeitig die Bedingungen untersucht, unter welchen der Dienst konsumiert werden darf. Es wird zum Beispiel geprüft, ob das Gerät zugelassen (compliant) ist und mittels Geolokation ermittelt, von woher der Zugriff erfolgt. So kann etwa je Nutzergruppe festgelegt werden, dass der Anwender sich mit einem zweiten Faktor authentifizieren muss (z.B. Microsoft Authenticator App oder einem Einwahlcode per SMS), wenn er sich in einem anderen Land als üblich befindet oder wenn innerhalb eines kurzes Zeitraums (z.B. Minuten statt mehrerer Stunden oder Tage) ein Zugriff verlangt wird – also wenn ein Missbrauch nicht ausgeschlossen werden kann. Aus den «Wenn-Dann»-Definitionen erfolgen «Ja-Nein»- oder «Ja-aber»-Entscheide. Die Schwierigkeit besteht nun darin, den Überblick über die Nutzerrechte zu den Services zu behalten. Dabei bietet Azure AD Conditional Access viele Features, um alle möglichen Use Cases zu managen. Trotzdem kann es auch unübersichtlich werden, wenn alle Berechtigungen jederzeit auf dem neuesten Stand sein sollen. So ist beispielsweise in der Microsoft-Cloud der Umgang mit dem Apple-Betriebssystem MacOS alles andere als trivial. Während nämlich bei Android- und iOS-Geräten die Policies sehr gut zu handhaben sind, ist beispielsweise bei (privaten oder geschäftlichen VIP-) MacBooks der Schutz vor Datenverlust (Data Loss Prevention) nur sehr schwer einzurichten. Bei den Smartphones und Tablets mit dem iOS-Betriebssystem kann etwa der Zugriff auf Exchange Online relativ einfach eingeschränkt werden, indem nur registrierte Geräte mit der offiziellen Outlook Mobile App für Apples mobiles Betriebssystem zugelassen werden. Zusätzlich empfiehlt es sich folgerichtig, die Daten, die im Service geöffnet werden, mit einer App Protection Policy zu schützen. Bei MacOS hingegen, wo die Möglichkeit einer solchen App Protection Policy nicht besteht, ist es nur schwer möglich zu verhindern, dass Daten aus Outlook auf dem Rechner abgelegt werden und von da das Gerät nicht verlassen.

Mehr Zugriffsmöglichkeiten schaffen mehr Schwachstellen

Es empfiehlt sich aus Sicherheitsgründen und um den Fortbestand der Geschäftstätigkeit (Stichwort Business Continuity) zu gewährleisten, regelmässig Security Reviews oder Security Checks durchzuführen. Verschiedene Anbieter halten in diesem Kontext entsprechende einmalige Angebote oder wiederkehrende Services im Portfolio. Wer dabei auf einen auf mobile Geräte spezialisierten Dienstleister zurückgreift, anstatt sich allein damit herumzuschlagen, kann von bei anderen Unternehmen gemachten Erfahrungen profitieren. Denn bei der nach einer Überprüfung der Identity-Management-Richtlinien zu tätigenden Anpassung kann man sich schlichtweg keine Fehler erlauben. Es gilt, nur exakt soviel Möglichkeiten freizugeben, wie auch wirklich benötigt werden. Bei jedem zusätzlichen Service, der neu in der Cloud läuft, können fehlerhafte Einstellungen fatale Folgen haben. Wer in einem produktiven System einen Fehler bei der Umstellung der Richtlinien macht, kann potenziell alle Nutzer blockieren oder aussperren. Dabei werden dann Nutzer nicht nur von den Services ausgeschlossen, sondern unter Umständen auch sofort alle offenen Sessions beendet. Eine solche Operation am offenen Herzen ist komplex, denn je hybrider die Umgebung, je mehr Zugriffswege auf Daten durch den Einsatz von Cloud Services erlaubt werden, desto mehr Schwachstellen können sich auftun.

Cloud-Sicherheit regelmässig neu beurteilen

Security Assessments können je nach Unternehmensgrösse und Komplexität in unterschiedlichen Ausprägungen durchgeführt werden – basierend auf Standardvorgehen. Je nach Ziel der Cloud-Strategie hilft basierend auf den durchgeführten Audits und der Bewertung des mobilen Reifegrads des Unternehmens die Durchführung eines strategischen Stakeholder-Workshops. Ziel ist es dabei, Schlüsselprojekte zu identifizieren und einen klaren Zeitrahmen für die Umsetzungsmassnahmen zu definieren. So kann eine strategische Cloud-Ausrichtung festgelegt und kontrolliert umgesetzt werden. Auf lange Sicht handelt es sich um einen iterativen Prozess, bei dem die Situation hinsichtlich der Anforderungen des Unternehmens und der Umstände seitens der Cloud-Anbieter immer wieder neu beurteilt werden muss. ■

DER AUTOR

Jonas Hofer ist Mobile Security Consultant bei Nomasis, einem Service-Spezialisten für mobile, sichere IT-Arbeitsplätze. Als Spezialist in der Umsetzung von mobilen IT-Infrastrukturen betreut Nomasis über 200 aktive Kunden aus der Finanz- und Versicherungsbranche, den öffentlichen Diensten, Industrie, Gesundheitswesen, Handel und Bildung.