Cloud-Sicherheit auf dem Prüfstand

Wolken ohne Regen

Joshua Tiago

Die drei größten Cloud-Plattformen von Amazon, Microsoft und Google realisieren unterschiedliche Sicherheitskonzepte – und genau das ist für Unternehmen von großer Relevanz.

Ob im Unternehmensumfeld oder im Privatleben: Kaum eine App, ein IoT-Gerät oder auch Fahrzeug kommt ohne Cloud aus. Die drei größten Anbieter, die den Großteil des Cloud-Marktes für sich beanspruchen, sind Amazon (AWS), Microsoft (Azure) und Google (GCP). Sie gelten als Allrounder und decken alle gängigen Szenarien für Cloud-Umgebungen ab.

Während der Pandemie hat sich die Cloud für viele Arbeitnehmer als wesentliches Arbeitsmittel entpuppt. Zudem konnten Unternehmen, die vom Homeoffice-Trend erfasst wurden, dank Cloud-Angeboten oftmals zügig in den betrieblichen Alltag zurückkehren. Kein Wunder also, dass für das Jahr 2020 der weltweite Umsatz der großen Cloud-Anbieter auf etwa 300 Mrd. US-Dollar geschätzt wurde.

Bevor die Cloud-Ära eingeläutet wurde, standen jedoch für viele Sicherheitsverantwortliche in Unternehmen einige Fragen im Raum: Wie sicher sind meine Daten in der Cloud? Wer hat Zugriff auf diese Daten? Wo lauern Gefahren und Risiken? Die Fragen sind zwar noch heute aktuell, der große Unterschied ist, dass sich die Unternehmen zum großen Teil für Cloud-Dienste entschieden haben. Inzwischen liegen aber nicht mehr nur eine Handvoll Daten bei den Cloud-Anbietern, sondern teilweise die komplette Infrastruktur samt allen Daten eines Unternehmens. Die spannenden Fragen lauten heute daher eher: Wie kann ich den sicheren Betrieb meiner Cloud-Umgebung gewährleisten und welcher Cloud-Anbieter bietet den besten Schutz für meine Daten?

Der Beginn einer neuen Ära

Cloud-Dienste entstanden, als sich heutige Internetgiganten wie Amazon und Google zu Beginn der 2000er-Jahre auf rasantem Wachstumskurs befanden. Klassische Rechenzentren und IT Infrastrukturen reichten ihnen für die Verarbeitung großer Datenmengen nicht mehr aus. So bauten sie sich nach und nach ein Portfolio an Cloud-Produkten auf, das sie später auch anderen Unternehmen zur Verfügung stellten.

Als Pioniere gelten die Cloud-Dienste von AWS: EC2 und S3. EC2 bietet die Möglichkeit, virtuelle Computer zu mieten und je nach Bedarf beliebig viel Rechenleistung der verwendeten virtuellen Systeme nach oben oder unten zu skalieren. Damit lassen sich zum Beispiel Szenarien abbilden, die kurzzeitig mehr Rechenleistung oder Speicherplatz erfordern. S3 hingegen dient als universeller Cloud-Speicherdienst für unterschiedliche Szenarien. Heute umfasst das Portfolio von AWS fast 200 Dienste.

Gerade in der Anfangszeit von Cloud-Computing waren die Sicherheitsmechanismen rudimentär, sofern überhaupt vorhanden. Sie zu verbessern, erforderte bei älteren Diensten große Anpassungen, was sich noch heute in der Benutzung älterer AWS-Dienste widerspiegelt. Ein AWS-Einsteiger dürfte immer wieder über kleinere Inkonsistenzen innerhalb einzelner

iX-TRACT

- AWS, Azure und GCP sind die drei größten Cloud-Plattformen, die alle gängigen Szenarien für Cloud-Umgebungen abdecken.
- Die Vergabe von Benutzerrechten kann in AWS verwirrend sein, Unternehmen sollten dafür zuerst ein Konzept entwerfen.
- Um Benutzer und Gruppen lokal zu verwalten, kann ein Administrator in der Azure-Umgebung das interne Active Directory mit dem Azure Active Directory koppeln.
- Im Security Command Center von GCP kann man alle sicherheitsrelevanten Informationen auf einen Blick einsehen.

Dienste stolpern, die mit deren langer Geschichte einhergehen. Später auf den Markt gekommene Anbieter wie Azure oder GCP lernten aus den Fehlern der ersten Stunde und bauten ihre Dienste von Anfang an um ein bestehendes Sicherheitsmodell herum auf.

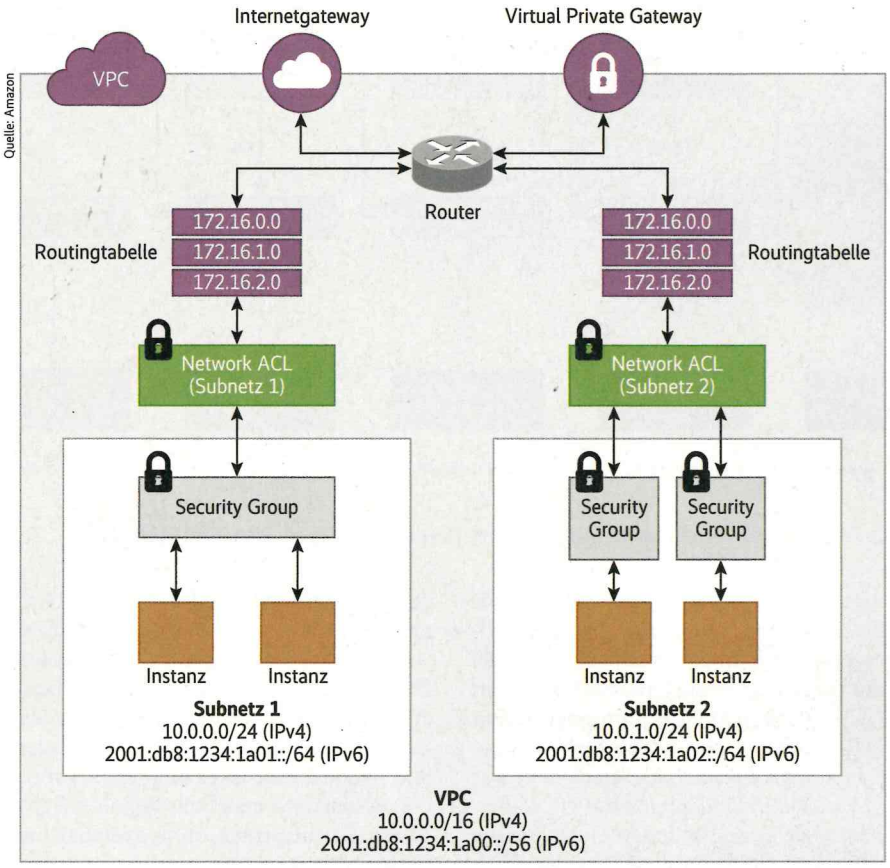
Netzwerksicherheit und Firewalls innerhalb der Cloud

Ein wesentlicher Baustein für die Absicherung einer Cloud-Umgebung ist die Abschottung einzelner Bereiche oder Dienste innerhalb der Cloud-Umgebung vom Internet und von den internen Bereichen eines Unternehmens. Das sind typischerweise Aufgaben, die Firewalls in Unternehmensnetzwerken übernehmen. AWS, Azure und GCP bieten auf unterschiedlichen Ebenen die Möglichkeit an, den Zugriff auf Systeme und Dienste innerhalb der eigenen Cloud-Umgebung einzuschränken. Kunden können sich in der Cloud-Umgebung mit Virtual Private Clouds die eigenen Netzwerkbereiche einfach und schnell einrichten sowie nach eigenen Vorgaben absichern.

AWS bietet mehrere Sicherheitsebenen zur Abschottung und Segmentierung der eigenen Virtual Private Cloud (VPC) an (siehe Abbildung 1). Besonders wichtig sind die Sicherheitsfunktionen Network ACL und Security Groups. Mit Network ACL legt man zum Beispiel fest, ob der Webserver innerhalb einer VPC aus dem Internet erreichbar ist. Mit Security Groups schränkt man die ein- und ausgehende Kommunikation ein, indem man Regeln erstellt, die dem Regelwerk gängiger Firewalls ähnlich sind.

Die Tabelle zeigt exemplarisch definierte Regeln für Security Groups. Man erkennt, dass die ausgehende Kommunikation ohne Einschränkungen erlaubt ist. Nicht eingeschränkt ist auch die eingehende Kommunikation aus dem Internet für einen Webserver im VPC (Port 443). Der SSH-Dienst innerhalb der VPC ist jedoch nur aus dem definierten IP-Adressbereich erreichbar. Auf diese Art kann man zum Beispiel Umgebungen entwerfen, in denen sich die Anforderungen an die Kommunikation zwischen den einzelnen Segmenten oder dem Internet schnell umsetzen lassen.

Azure verfolgt ein ähnliches Konzept wie AWS. Analog zu Virtual Private Clouds stellt Azure Virtual Networks (VNets) zur Segmentierung der eigenen Cloud-Umgebung und zur Einschränkung des Netzwerkzugriffs zur Verfügung.



Die eigene Cloud-Umgebung kann mittels Network ACL und Security Groups auf verschiedenen Ebenen abgesichert werden (Abb. 1).

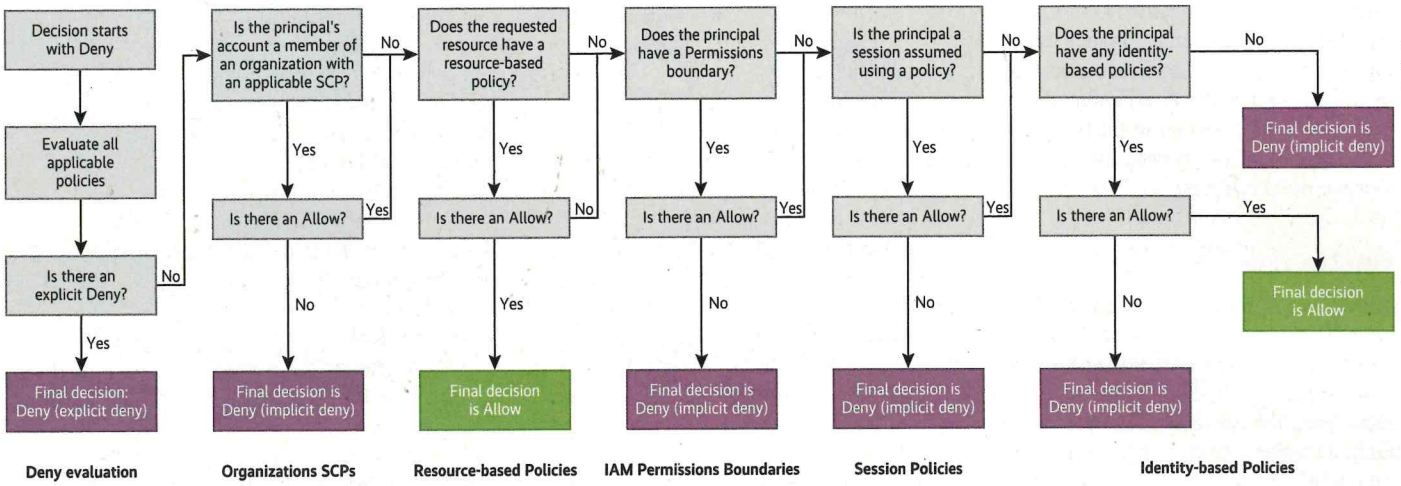
Innerhalb des VNets lässt sich die Umgebung in Subnetze unterteilen. Dadurch kann man zum Beispiel Subnetze mit Webservern von Subnetzen mit Datenbanksystemen trennen oder auch bestimmte Verbindungen untereinander erlauben. Mittels Network Security Groups ist es wie bei AWS möglich, per Regelwerkkonfiguration Regeln für die erlaubte Kommunikation festzulegen.

Im Gegensatz zu AWS bietet Azure mit dem Firewall Manager einen Sicherheitsverwaltungsdienst an, um die Funktion einer Firewall in der eignen Cloud-Umgebung zu realisieren. Damit können Kunden ein Firewallregelwerk konfigurieren und einige Einstellungen vornehmen. Für die Nutzung dieser Firewall fallen weitere Kosten an, die von der Nutzungsdauer und dem übertragenen Volumen abhängig sind. Enthalten sind Funktionen wie Microsoft Threat Intelligence, womit man bekannte IP-Adressen und Hostnamen blockiert, und Funktionen wie Source und Destination NAT sowie URL-Filter. Es lassen sich außerdem Regeln auf Basis von Domainnamen definieren. Nutzer der Azure-Firewall müssen allerdings einige Einschränkungen hinnehmen. Microsoft hat bewusst Regeln implementiert, die man nicht deaktivieren kann. Zum Beispiel ist die ausgehende Kommunikation auf TCP-Port 25 nicht erlaubt. Microsoft blockiert sie standardmäßig mit der Begründung, dass SMTP auf Port 25 als unsicher gilt, da die übertragenen Daten auf dem Transportweg nicht verschlüsselt werden. Dies mag zwar in einigen Fällen so sein, aber in Zeiten von STARTTLS werden auch Verbindungen geblockt, die eigentlich verschlüsselt sind, da mittels STARTTLS auch über Port 25 verschlüsselte Kommunikation möglich ist. Weitere Einschränkungen betreffen Protokolle wie FTP. Der Vorteil der Azure-Firewall ist aber, dass der Dienst zentral Einschränkungen bezüglich der Kommunikation für mehrere VNets erzwingen kann.

Google ist mit seinem Cloud-Angebot GCP ähnlich aufgestellt wie die Konkurrenz. Das Unternehmen bietet dedizierte Umgebungen als Virtual Private Clouds (VPC) an. Man kann sie in kleine Segmente

Regelwerk für Security Groups

Direction	Protocol	Port Rang	Source
Inbound	TCP	22	195.243.60.224/28
Inbound	TCP	443	0.0.0.0/0
Inbound	TCP	All	0.0.0.0/0



Quelle: Amazon

In AWS gibt es verschiedene Möglichkeiten, Benutzerrechte zu verteilen (Abb. 2).

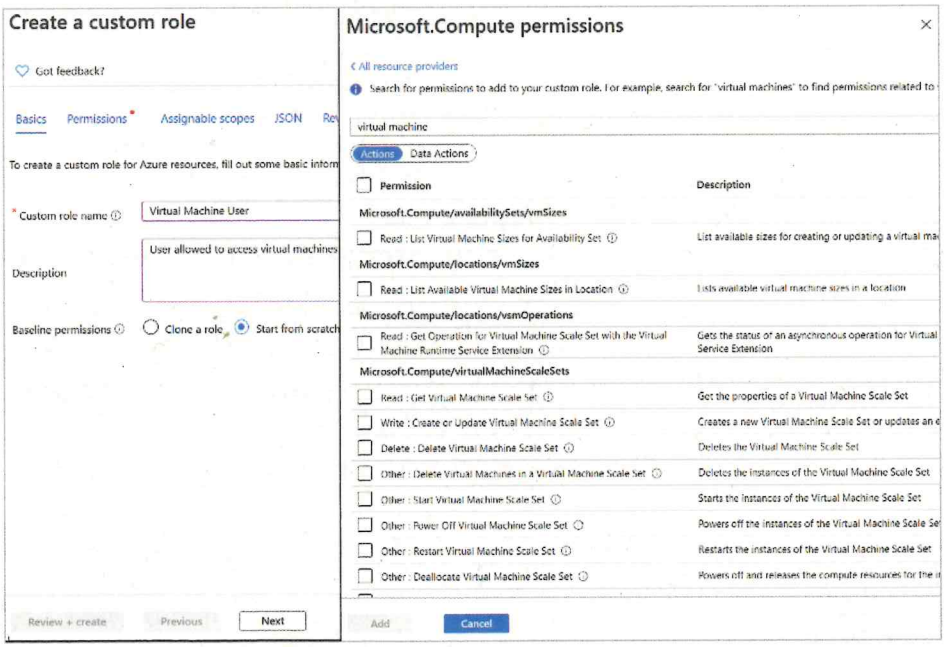
mittels Subnetzen einteilen – genauso wie bei AWS und Azure. Bei den Firewallregeln ist allerdings Vorsicht geboten: Bei der Erstellung eines Subnetzes generiert GCP automatisch Firewallregeln. Sie erlauben standardmäßig die Kommunikation zu und aus anderen Subnetzen, was in vielen Fällen nicht gewollt ist. Außerdem sind in den Standardeinstellungen auch Verbindungen zu RDP- und SSH-Diensten im Subnetz des jeweiligen VPC für jeden Benutzer im Netzwerk und damit auch im Internet erlaubt. Entsprechend sollte man die Regeln nach der Erstellung des Subnetzes anpassen oder löschen. Analog zur Azure Firewall sind auch in GCP keine ausgehenden Verbindungen zu Systemen auf TCP-Port 25 erlaubt. Zudem fügt GCP automatisch Regeln hinzu, wenn man bestimmte Dienste verwendet. Nimmt man beispielsweise Googles Kubernetes Engine in Anspruch, erstellt es automatisch Regeln für die Kommunikation der Kubernetes-Cluster und -Nodes. Hier ist es empfehlenswert, die automatisch erstellten Regeln dahingehend zu überprüfen, ob sie eventuell ein Risiko bergen.

Zugriff auf Daten kontrollieren

Ein weiterer Baustein für eine sichere Cloud-Umgebung ist die Benutzer- und Rechteverwaltung. Ziel ist es, den Benutzern der Cloud-Umgebung an zentraler Stelle nur die von ihnen benötigten Berechtigungen einzuräumen und diese Berechtigungen zu verwalten. Während die meisten Unternehmen Systeme wie den Verzeichnisdienst Active Directory von Microsoft oder andere Produkte zum Identity and Access Management (IAM) verwenden, um Zugriffsrechte zentral zu verwalten, divergieren die Konzepte der Cloud-Anbieter enorm. In der Cloud-Welt geht es oftmals nicht nur um Benutzerrechte, sondern vielmehr um die Rechte jeder einzelnen Ressource in der Cloud-Umgebung.

AWS bietet die Benutzer- und Rechteverwaltung unter dem Namen IAM an. Mittels IAM können Administratoren AWS-Benutzer und -Gruppen anlegen und verwalten sowie mittels Berechtigungen deren Zugriff auf AWS-Ressourcen zulassen oder verweigern. Die Arten, mit denen sie die Rechte von Benutzern und Ressourcen definieren, sind im Vergleich zu Azure und GCP an manchen Stellen sehr komplex. Dies ist der Tatsache geschuldet, dass man die Rechte nicht zentral, sondern an sehr vielen Stellen definieren kann. Daran erkennt man, dass AWS die Funktionen für das Identity Management nach und nach in seine Produkte integriert hat.

Administratoren können mittels IAM Einzelberechtigungen erteilen und Rechte auf Gruppenebene mittels Permissions Boundary, Service Control Policies, Session Policy und Ressource-based Policies definieren. Für AWS-Einsteiger kann diese Rechtevergabe eine enorme Hürde aufbauen. Zudem sieht man in der AWS-Auswertungslogik, dass das Benutzerrecht an diversen Stellen gewährt oder verweigert wird (siehe Abbildung 2). Kunden, die ihre Cloud-Umgebung in AWS aufbauen



In Azure kann man bereitgestellte Rollen verwenden und eigene definieren, hier die Rolle Virtual Machine (Abb. 3).

möchten, sollten sich zu Beginn ein Konzept für das Benutzer- und Rechtemanagement erstellen. In diesem sollte man festlegen, welche der oben genannten Mechanismen von IAM in Kraft treten, um zu verhindern, dass am Ende die Übersicht über die Benutzer- und Rechteverwaltung in IAM verloren geht.

Wer sich intensiv mit dem IAM-Konzept von AWS auseinandersetzt, kann jede Berechtigung in der Cloud-Umgebung konfigurieren – etwa die der Benutzer und der Ressourcen, wie einer virtuellen Maschine, eines Speicherdienstes oder einer Tabelle innerhalb der Datenbank. Darüber kann man sehr granular definieren, wann, wie und wo welche Dienste in welcher Art genutzt werden.

Für die Rechte- und Benutzerverwaltung nutzt Azure seinen Ressource Manager. Er ähnelt stark dem Konzept in Windows-Umgebungen und ist verständlicher als IAM. Ein Administrator setzt die Rechte in Azure mit einem Role-based-Access-Control-Modell um. Dabei wird ein Whitelist-Modell genutzt, bei dem alles standardmäßig verboten ist, was nicht durch eine Rolle explizit erlaubt ist. Ist ein Benutzer zum Beispiel Entwickler und gleichzeitig Administrator einer Testumgebung, so leiten sich seine Rechte von seiner Gruppenzugehörigkeit ab – in diesem Fall zum Beispiel von den Gruppen Entwickler und Administratoren. Der Benutzer erhält die Summe aller Rechte seiner jeweiligen Rollen. Um dann noch die individuellen Anforderungen eines Kunden abzubilden, können Administratoren neben den bereits von Azure bereitgestellten Rollen auch eigene Rollen definieren. Einer Rolle kann man verschiedene Rechte zuweisen – etwa virtuelle Maschine starten, beenden oder löschen (siehe Abbildung 3).

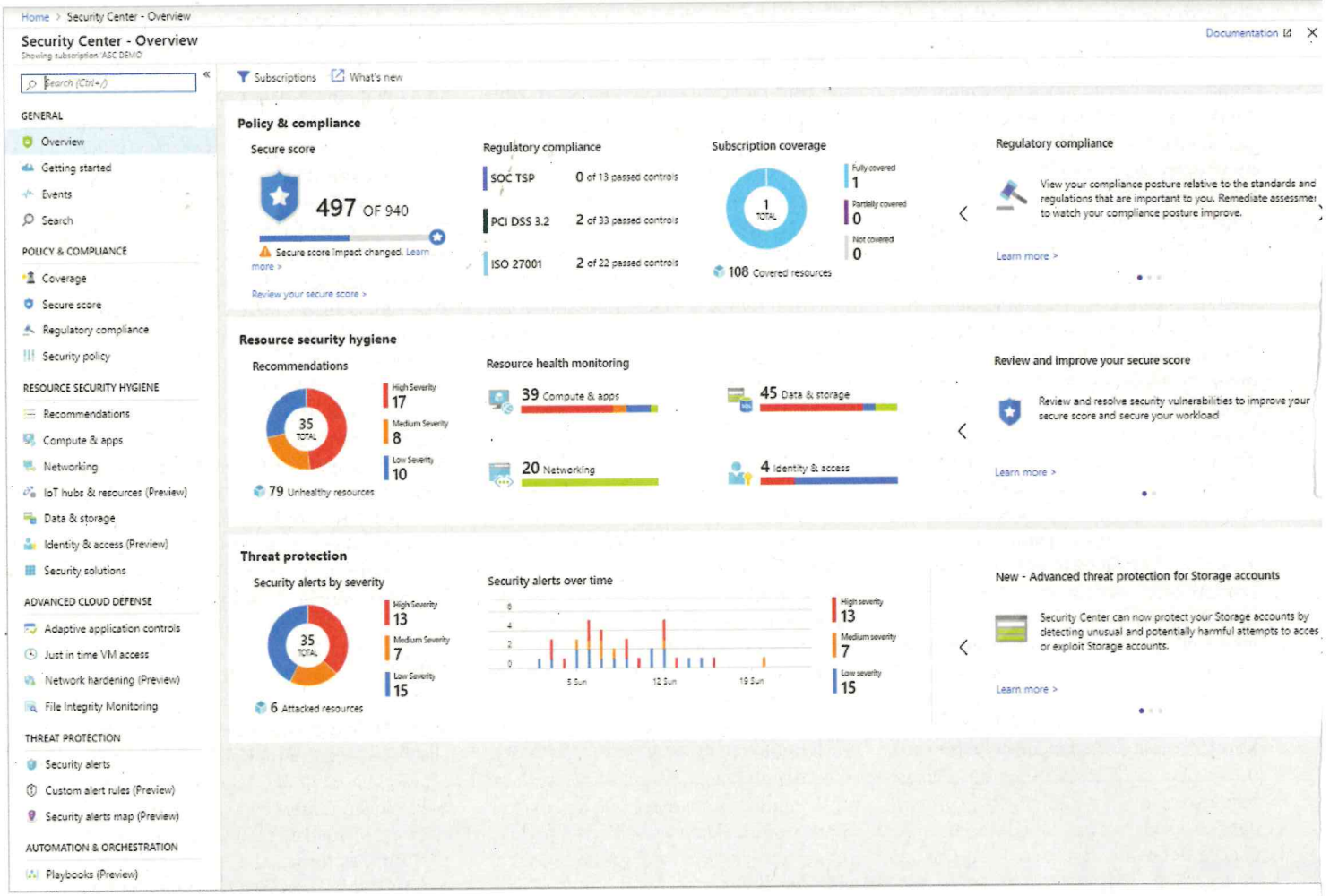
Ein Argument, warum sich viele Kunden für Azure entscheiden, ist die Kopplung des internen AD (Active Directory) mit dem Azure Active Directory. Auf diese Weise lassen sich Benutzer und Gruppen nach wie vor lokal verwalten, die dann reibungslos in die Cloud-Umgebung synchronisiert werden. Somit nutzt der Kunde zur Verwaltung der Identitäten weiterhin nur eine zentrale Plattform. Für die Synchronisierung des internen AD mit dem Azure AD beherrscht Azure unterschiedliche Verfahren.

GCP definiert die Rechte für Benutzer und Ressourcen im zentralen Cloud-IAM-Dienst. Die Konfiguration der Rechte erfolgt wie auch bei AWS und Azure entweder über die Webkonsole oder über eine REST-API, die alle drei Anbieter zur Verfügung stellen. GCP weist für manche Ressourcen und Dienste automatisch Rollen zu. Aus Sicherheitsgründen sollten Kunden vordefinierte und sogenannte einfache Rollen vermeiden, da diese meist zu viele Berechtigungen besitzen. Sie dienen oftmals als Vorlage zum Erstellen benutzerdefinierter Rollen, die man anpassen und einschränken kann.

Mit dem Policy Analyzer bietet GCP zudem ein weiteres Tool, das zeigt, auf welche Ressourcen und Dienste ein beliebiger Benutzer Zugriff hat. Es gibt unter anderem Antworten auf die Fragen: „Für welche BigQuery-Datasets hat der Nutzer XYZ Leseberechtigungen?“, „Wer sind die Abrechnungsadministratoren in meiner Organisation?“ und „Welche VMs kann Benutzer XYZ in Projekt A löschen?“

Encryption at Rest

Ein weiterer Vorteil der hier vorgestellten Cloud-Anbieter ist Encryption at Rest.



Im Azure Security Center wird der Sicherheitsstatus aller Cloud-Ressourcen bewertet (Abb. 4).

Hierbei geht es nicht um die Verschlüsselung der Daten auf dem Transportweg, sondern auf dem Datenträger. Insbesondere in Cloud-Umgebungen ist die Frage berechtigt, was mit den Daten geschieht, wenn ein Datenträger beim Hardwaretausch oder durch Diebstahl abhandenkommt. Genau für diese Szenarien ist Encryption at Rest ein wichtiger Aspekt.

Alle drei Cloud-Provider bieten für einen Großteil der Dienste Encryption at Rest an. AWS verschlüsselt die Datenträger der EBS- und EFS-Speicherdienste. Da die meisten Dienste in AWS auf diesen Speicher zurückgreifen, profitieren andere Dienste wie EC2 und AI automatisch davon. Aber auch die Verschlüsselung von Daten in Datenbanken wird teilweise angeboten – etwa mittels symmetrischer Verschlüsselung (AES-256).

Azure bedient ebenfalls das Thema Encryption at Rest – für mehr als 50 Dienste, wie virtuelle Maschinen, Speicherdienste, das Azure Active Directory, aber auch Datenbanksysteme. Gerade in diesem Bereich sticht Azure hervor, da nicht nur die eigene SQL-Datenbank berücksichtigt wird, sondern auch Datenbanken auf virtuellen Maschinen. Dabei kommt ein Verfahren zur transparenten Ver- und Entschlüsselung der Daten zum Einsatz. GCP verschlüsselt die Daten sowohl auf Block- als auch auf Datenträgerebene. Bei allen drei Anbietern findet die Verschlüsselung auch auf Datenträgerebene statt.

Beim Thema Verschlüsselung ist es wichtig zu wissen, wer im Besitz des Schlüsselmaterials ist und Zugriff darauf hat. Sowohl AWS als auch Azure und GCP bieten dafür diverse Modelle an. Im einfachsten Fall stellt der Cloud-Anbieter das Schlüsselmaterial selbst zur Verfügung, sodass sich der Kunde nicht um die Schlüsselverwaltung kümmern muss. Alternativ bieten die drei Anbieter eine Möglichkeit, für bestimmte Dienste eigene Schlüssel zu verwenden. Teilweise ist sogar der Einsatz kundeneigener Verschlüsselungshardware (HSM-Komponenten) möglich. Je nachdem, bei welchem Cloud-Dienst beziehungsweise auf welcher Ebene Verschlüsselung zum Einsatz kommt, liegt die Schlüsselverwaltung und damit das Schlüsselmaterial entweder in der Hoheit des Kunden oder des Cloud-Anbieters. Liegt es in den Händen des Cloud-Anbieters, wie es in der Regel bei den gemanagten Diensten der Fall ist, besteht im Vergleich zur kundenseitigen Verwaltung des Schlüsselmaterials das zusätzliche potenzielle Risiko, dass Mitarbeiter des Cloud-Providers oder Geheimdienste auf den Schlüssel zugreifen und die Daten somit entschlüsseln können. Dieses Risiko muss der Cloud-Kunde für alle Cloud-Dienste tragen, für die es keine kundenseitigen Möglichkeiten zur eigenen Schlüsselverwaltung gibt.

Cloud-Umgebung überwachen und protokollieren

Die Komplexität und die enorme Anzahl beteiligter Dienste und Systeme in der Cloud-Umgebung erfordern aus Sicherheitssicht eine Übersicht über die Vorgänge innerhalb der Umgebung – etwa durch Logging und Monitoring. AWS, Azure und GCP sind in diesem Bereich gut aufgestellt.

Beim Logging lässt sich bei allen drei Anbietern detailliert festlegen, welche Aktionen geloggt werden sollen, da jede Aktion in der Cloud-Umgebung einen Aufruf der REST-API darstellt. Die Protokollierung wird so konfiguriert, dass das System sicherheitsrelevante Ereignisse erfasst, was wiederum für die lückenlose Aufklärung und Nachvollziehbarkeit von Sicherheitsvorfällen hilfreich ist.

Mit CloudTrail von AWS kann man lückenlos alle Vorgänge innerhalb einer Cloud-Umgebung protokollieren: zum Beispiel jede Anmeldung, das Starten einer virtuellen Maschine, die Änderung einer Rechte-Policy, das Löschen einer Ressource et cetera. Die Kosten für CloudTrail korrelieren mit der Anzahl der erfassten und gespeicherten Meldungen. Es ist daher ratsam, nur sicherheitsrelevante Ereignisse zu protokollieren. Der Zugriff auf die Protokolldaten ist einzuschränken. Das dazugehörige Protokoll ist standardmäßig in einem S3-Bucket gespeichert, dessen Berechtigung man restriktiv konfigurieren muss.

Azure zeichnet die Activity Logs standardmäßig im Dienst Azure Monitor auf. Man kann das Aufzeichnen weiterer Logs in den Diagnostic Settings aktivieren. Außerdem ist es möglich, Zugriffe auf das Schlüsselmaterial des Key Vaults oder andere sicherheitsrelevante Ereignisse zu protokollieren.

GCP bietet im Rahmen von Audit-Logs ebenfalls die Möglichkeit, sicherheitsrelevante Ereignisse zu protokollieren. Standardmäßig protokolliert GCP von Administratoren ausgelöste Schreibvorgänge in den Audit-Logs. Zusätzlich sollten lesende API-Aufrufe protokolliert werden. Die Konfiguration kann man im GCP-IAM-Dienst anpassen.

Definierte Richtlinien für Unternehmen

Wenn unterschiedliche Fachbereiche die Cloud-Umgebung unternehmensweit nutzen, ist der Wunsch groß, die Richtlinien des Unternehmens in der Cloud-Umgebung durchzusetzen und Abweichungen festzustellen. Dies ist typischerweise die Aufgabe von Compliance und Governance. In AWS stehen hierfür die Dienste Service Control Policy und Control Tower zur Verfügung.

Als Teil des Control Towers kann Guardrails die Verwendung von Diensten und Funktionen einschränken. Es gibt eine große Auswahl an vorkonfigurierten Guardrails, sie gelten global für alle Fachbereiche, die die AWS-Dienste nutzen. Der AWS Control Tower bietet eine Übersicht über die verwendeten Guardrails.

Azure bietet mit Azure Policy einen ähnlichen Dienst. Damit lassen sich Vorgaben unternehmensweit durchsetzen und darüber hinaus sehr effektiv Abweichungen feststellen und verhindern – je nach Konfiguration. Auch GCP unterstützt ihre Kunden bei der Durchsetzung von Vorgaben. Mittels Organization Policy Constraints können sie Einschränkungen für die gesamte Organisation oder einzelne Projekte vornehmen. GCP liefert wie auch AWS von Haus aus eine große Menge an vorkonfigurierten Richtlinien.

Sichtbarkeit der Sicherheit

Die Sichtbarkeit der sicherheitsrelevanten Vorgänge und Ereignisse spielt in der Cloud-Umgebung eine wichtige Rolle. Typische Cloud-Kunden nutzen bewusst oder unbewusst eine Fülle unterschiedlicher Dienste: Programme zur Benutzerverwaltung, gemanagte Datenbanksysteme, Cloud-Speicher, virtuelle Maschinen, API-Gateways und vieles mehr. Da kommt Sicherheitsverantwortlichen die Frage nach dem Ist-Stand der Cloud-Umgebung in Bezug auf Sicherheitsprobleme in den Sinn. Sind alle Dienste nach den Vorgaben des Unternehmens konfiguriert? Haben einzelne Benutzer zu viele Rechte? Gibt es Versuche, mit bekannten oder unbekannten Zugangsdaten unerlaubten Zugriff zu erlangen? Wie ist der Patchstand meiner Systeme? Hat man Malware innerhalb einer virtuellen Maschine ausgeführt? Je komplexer und umfangreicher die Cloud-Umgebung, desto eher wünschen sich Sicherheitsverantwortliche Antworten auf diese Fragen. Und genau das ist der Bereich, in dem sich die drei betrachteten Cloud-Anbieter stark unterscheiden.

AWS bietet den Security Hub an. Wie der Name suggeriert, stellt der Dienst an zentraler Stelle Sicherheitsrelevantes dar. In vielen Bereichen gelingt das gut. So lassen sich Meldungen anzeigen zu unsicher konfigurierten Diensten oder Systemen, die nicht dem Regelwerk des Unternehmens entsprechen. Der Security Hub erhält dazu Informationen von anderen Diensten. Allerdings lässt sich sein Umfang nicht mit dem des Azure Security Centers vergleichen. In diesem sind in einer Art Dashboard anschaulich Informationen zu Ereignissen aus vielen Quellen dargestellt – etwa Abweichungen der Azure Policies, Ereignisse im Bereich Benutzerverwaltung, Patchstand sowie Meldungen zu Malware innerhalb virtueller Maschinen oder Auffälligkeiten im Netzwerkverkehr (siehe Abbildung 4). Der Vorteil an Azure ist, dass die Informationen von Windows-Systemen in der Cloud und lokal eingebunden sind.

Googles GCP Security Command Center zeigt an zentraler Stelle sicherheitsrelevante Informationen an. Darüber lässt sich eine Übersicht über das gesamte Inventar in der Cloud-Umgebung erstellen, gleichzeitig meldet es aber auch Verstöße gegen die geltenden Compliancerichtlinien. Im Security Command Center kann man Trigger für Alarmierung und andere Aktionen definieren. Die erhobenen Daten lassen sich wie auch bei AWS und Azure über die REST-API an SIEM-Werkzeuge übergeben. Dies ist sinnvoll, um im Security Operations Center Informationen gebündelt zu analysieren. In manchen Fällen übernimmt das Azure Security Center sogar diese Aufgabe, weil nach und nach mehr Informationen aus der On-Premises-Welt in Azure exportiert werden.

Fazit

Viele Parameter entscheiden darüber, welche Cloud-Plattform im Einzelfall die richtige ist. Es ist üblich, dass Unternehmen mehrgleisig fahren und gleichzeitig zwei oder drei Cloud-Plattformen verschiedener Anbieter verwenden.

Im Hinblick auf das Thema Sicherheit bieten die betrachteten Anbieter AWS, Azure und GCP eine Fülle an Möglichkeiten, die eigene Umgebung sicher zu betreiben. Alle drei bieten weitere Dienste an, die einen Mehrwert für die Sicherheit der Umgebung bringen. In vielen Fällen offerieren die Cloud-Anbieter sogar Sicherheitsfunktionen, die in der On-Premises-Welt in diesem Umfang gar nicht möglich wären.

Mindestens genauso wichtig wie die Entscheidung darüber, welchen Anbieter man wählen soll, ist jedoch auch das zugrunde liegende Sicherheitskonzept der Cloud-Kunden. Dieses sollte genau definieren, wie der Kunde die Cloud-Umgebung nutzen möchte und welche Vorgaben gelten. Die Vorgaben kann man sowohl bei AWS als auch bei Azure und GCP granular konfigurieren. Verwendet man die Konzepte dieser Anbieter korrekt, bieten sie allesamt ein höheres Sicherheitsniveau als On-Premises-Umgebungen. (mig@ix.de)

Joshua Tiago

arbeitet als Leitender Berater bei der cirosec GmbH.