rer Hinsicht an ihre Grenzen: Häufig konzentrieren sich die eingesetzten Sicherheitswerkzeuge auf ganz bestimmte Aspekte, was zu Informationssilos und unzähligen Alarmen führt.

Ohne Kontextinformationen und Priorisierung ist eine sinnvolle Verarbeitung der anfallenden Datenmengen in Multi-Cloud-Umgebungen nicht mehr menschenmöglich. Weitere Probleme für die Angriffsanalyse entstehen durch die begrenzte Sichtbarkeit von Microservices, Data Caches und temporären IP-Adressen, die oftmals nur wenige Minuten aktiv sind und dann gelöscht werden. Alle Aktivitäten, die nicht in dieser kurzen Zeit erfasst werden, gehen für Sicherheitsanalysen verloren.

Verhaltensbasierte Sicherheit eliminiert Regeln

Die künftige Entwicklung scheint absehbar: DevOps, Container und Technologien wie Serverless Computing drehen die Komplexitätsspirale weiter und erfordern gleichzeitig immer schnellere Reaktionen von der IT-Sicherheit. Dadurch entstehen fast unweigerlich nicht erkannte Sicherheitslücken in der Multi-Cloud, die von professionellen Angreifern ausgenutzt werden.

Um dieser Entwicklung zuvorzukommen, ist eine wachsende Zahl von Unternehmen bereit, den eigenen Sicherheitsansatz für die Cloud-Welt auf den Prüfstand zu stellen. Zwei Überlegungen stehen dabei im Fokus: Erstens muss ausnahmslos jede Multi-Cloud-Komponente zentral überwacht werden, blinde Flecken sind absolut inakzeptabel. Zweitens muss die Überwachung vollständig automatisiert ablaufen, denn die produzierten Datenmengen können manuell nicht ausgewertet werden. Händische Regeldefinitionen und Log-Auswertungen sind ausgeschlossen.

Diese Vorgaben lassen sich durch ein lückenloses Monitoring der Cloud-Prozesse und eine Machine-Learning-gestützte Analyse des Normalzustandes erreichen. Prozesse bilden die kleinsten vom Betriebssystem unterstützten Einheiten und sind verantwortlich für die gesamte Kommunikation, sowohl miteinander als auch mit externen Hosts. Sie haben zudem nachverfolgbare Startumstände, Hashwerte, Zwecke und Lebenszyklen und werden nicht zwischen unterschiedlichen Applikationen gemischt.

Baseline zeigt Normalzustand

In Echtzeit werden alle Interaktionen zwischen Prozessen erfasst, auch wenn sie innerhalb derselben Datei stattfinden. Das Monitoring erstreckt sich auf Prozesshierarchien, Prozesse/Machine-Kommunikation, Änderungen an Anwender-Privilegien, interne und externe Datentransfers und alle anderen Cloud-Aktivitäten. Auf Basis dieser lückenlosen Überwachung kann mittels Machine Learning eine temporale Baseline erstellt werden, die Aufschluss gibt über das normale Verhalten von Anwendern, Applikationen und Workloads in der Multi-Cloud.

Die gesammelten Daten werden zudem entsprechend der zugehörigen Cloud-Entität in Analysegruppen organisiert. Verhaltensbasiertes Machine Learning vergleicht das aktuelle Verhalten einer Cloud-Entität einerseits mit ihrem bekannten Verhalten im Zeitverlauf, andererseits aber auch mit dem bekannten Verhalten ähnlicher Cloud-Entitäten in der jeweiligen Analysegruppe. Anomalien, also alle abweichenden Aktivitäten, heben sich vor diesem Normalzustand deutlich ab.

Wert für die Sicherheitspraxis

Der automatisierte Abgleich mit dem bekannten Verhalten und der Analysegruppe identifiziert bekannte und unbekannte Bedrohungen. Viele Aktivitäten, die sich mit Regeln nur schwer erfassen lassen, können jetzt im Kontext bewertet werden. Dazu gehören zum Beispiel der Ab- oder Zufluss ungewöhnlicher Datenmengen in Amazon S3 Buckets, unerwartete Verbindungen von Applikationen, auffällige API-Aufrufe durch Container sowie jedes nicht normale Anwender-Verhalten.

Weil die Technologie den Normalzustand kennt, kann sie zudem viele reguläre Aktivitäten im Cloud-Datacenter als Bedrohung ausschließen. Das senkt die Zahl der False Positives und Alarme. Diese drastische Reduktion der Komplexität ermöglicht es der IT-Sicherheit, Multi-Cloud-Initiativen aktiv zu unterstützen, ohne Kompromisse beim Schutz einzugehen.

Bernd Mährlein

Bernd Mährlein, Area Director Central Europe, Lacework

Sichere Cloud dank zertifiziertem Schutz

Die Rolle von Cloud- und Multi-Cloud-Umgebungen in Unternehmen wächst stetig – verstärkt auch durch die Corona-Pandemie und den damit verbundenen Auswirkun-gen auf Unternehmen und Unternehmenskulturen. Viele Arbeitgeber haben bereits verlauten lassen, nach den Einschränkungen und Schutzmaßnahmen gegen Covid-19 vermehrt auf ‚Work from anywhere' zu setzen und den eigenen Mitarbeitern mehr Homeoffice zu ermöglichen. Zur Umsetzung dieser Pläne bedarf es allerdings einer entsprechenden Infrastruktur und eines dafür optimierten technologischen und pro-zessualen Ökosystems. Der Grad der Digitalisierung, besonders in kleinen und mittle-ren Unternehmen (KMU), muss entsprechend angehoben werden, um in der neuen Arbeitswelt wettbewerbsfähig zu bleiben.

Cloud- und Multi-Cloud-Lösungen bieten nicht nur einen schnelleren Zugriff auf Un-ternehmens-daten, als es viele VPN-Lösungen können, sondern die Verlagerung von Anwendungen und Services in Cloud-Umgebungen erleichtert oftmals die tägliche Arbeit der eigenen Mitarbeiter erheblich. Neben diesen Vorteilen birgt die Migration in die Cloud allerdings auch diverse Stolpersteine, besonders in Sachen der

Sicherheit und des Datenschutzes, die vor dem Start von solchen Projekten beachtet und nach Abschluss regelmäßig geprüft werden müssen, um die Entstehung von Sicherheitslü-cken und Datenlecks zu verhindern bzw. auf diese schnellstmöglich zu reagieren.

Alexander Häußler, Product Compliance Manager ISO/IEC 27001, TÜV SÜD Management Service

Identitätsmanagement und Zero Trust sorgen für Sicherheit im Homeoffice

Neben möglichen Fehlkonfigurationen bleibt ein weiterer Angriffsvektor ein Problem für die Cloud: Zugangsdaten und Identitätsmanagement. Phishing ist nach wie vor eine der größten Cyber-Bedrohungen, die Mitarbeiter in Unternehmen unmittelbar betreffen. Die Bedrohungsakteure haben sich zudem das Homeoffice als neues An-griffsziel ausgesucht, um ihre Opfer mit falschen Liefer-Meldungen oder ausgefeilten Social-Engineering-Attacken auszutricksen und sich Zugangsdaten zu beschaffen. Durch die physische Trennung vom Unternehmensnetzwerk - und Kollegen - steigt die Verantwortung, die der einzelne Mitarbeiter als Teil einer Art menschlichen Fire-wall zur Bedrohungsabwehr trägt, enorm. Das erfordert nicht nur einen größeren Fo-kus auf Security Awareness, den es von Unternehmensseite zu setzen gilt, sondern eine Adaption von Least-Privilege- und Zero-Trust-Ansätzen. Dabei wird für jeden Nutzer initial und anschließend regelmäßig genau evaluiert, welche Rollen und Rechte er benötigt, und ob diese eventuell zu einem späteren Zeitpunkt nicht mehr benötigt werden. Das schränkt nicht nur dessen Bewegungsfreiheit innerhalb des Systems ein, sondern dadurch wird dafür gesorgt, dass selbst bei einem erfolgreichen Einbruch eines Kriminellen in das Netzwerk der dabei entstandene Schaden in Gren-zen gehalten werden kann.

Ein starkes Identitätsmanagement zur eindeutigen Identifikation, bei Bedarf durch ei-ne Mehr-Faktor-Authentifizierung, hilft ebenfalls, um Einbrüche und Datenlecks zu verhindern. Sogar wenn somit einmal Anmeldedaten und die dazugehörigen Pass-wörter durch Phishing abhandengekommen sein sollten, so helfen diese zusätzlichen Sicherheitsmaßnahmen dabei, die Kriminellen auszusperren.

Fehlkonfiguration als Gefahrenquelle in der Cloud

Eine Mehrheit der Sicherheitslücken in Cloud-Lösungen und der dadurch entstehen-den Schäden lässt sich auf initiale Fehlkonfigurationen bei der Migration zurückfüh-ren. Unternehmen, beziehungsweise deren IT-Abteilungen, gehen nach wie vor zu häufig davon aus, dass die Verantwortung für die Sicherheit von Daten und Anwen-dungen innerhalb der Cloud lediglich beim Anbieter der IaaS-Lösung (Infrastructure-as-a-Service) liegt. Allerdings garantiert dieser zumeist nur die Sicherheit der Cloud selbst. Sollten also unternehmen Anwendungen oder Services dorthin verschieben, so sind sie auch selbst für die Absicherung dieser verantwortlich.

Im Zuge der Covid-19-Maßnahmen war es für viele KMU notwendig, schnell zu han-deln, um die Geschäftskontinuität zu gewährleisten. Während nun IT-Sicherheitsabteilungen oftmals die Kräfte fehlen, um sich dem Problem der Fehlkonfi-gurationen anzunehmen, haben die Cyber-Kriminellen bereits reagiert: Mehr Malwa-re und Ransomware wird über Sicherheitslücken in der Cloud in Unternehmen ein-geschleust. Eine aktuelle Studie von IDG Research zeigt: Jedes dritte Unternehmen hat in den vergangenen 12 Monaten einen wirtschaftlichen Schaden durch Angriffe auf die von ihnen genutzten Cloud-Dienste erlitten – wiederum ein Drittel der be-troffenen Unternehmen hatte sogar mit einem kompletten Stillstand aufgrund der An-griffe zu kämpfen.

Normen schaffen Vertrauen

Einer der zuverlässigsten Wege zur sicheren Nutzung der Cloud ist die Überprüfung des Systems durch unabhängige Experten. Diese können dabei helfen, die IT-Sicherheitsabteilungen zu entlasten und die Daten und Anwendungen innerhalb der Cloud-Umgebung zu sichern. Dabei helfen ihnen unter anderem die Normen ISO / IEC 27001 und deren Erweiterung 27701. Die Normenreihe fordert beispielsweise die Implementierung eines Informationssicherheits-Managementsystems (Information Security Management System, ISMS) zur Sicherung des technologischen Ökosystems von Unternehmen. Dabei handelt es sich um eine Aufstellung von Regelungen, Maß-nahmen und Programmen, die innerhalb eines Unternehmens angewendet werden sollten. Wichtig ist, dass dabei aber mehr als nur die verwendete Technologie und die digitale Infrastruktur eines Unternehmens betrachtet wird. Dabei setzt ein ISMS be-reits auf der Prozessebene an, um sein Ziel der Informationssicherheit im gesamten Unternehmen zu erreichen. Durch diesen ganzheitlichen Ansatz helfen die Normen dabei, jeden Aspekt der Arbeit mit Cloud-Lösungen sicherer zu gestalten: von der Migration über die Datenspeicherung bis hin zu den Zugriffen der Nutzer auf Anwen-dungen und Informationen.

Wer also dafür sorgt, dass eigene Lösungen nach den entsprechenden Normen zerti-fiziert sind, der kann wirklich von einer sicheren Cloud sprechen. Zudem hilft die Zerti-fizierung im Schadens- oder Haftungsfall: die Normenreihe ISO / IEC 2700x bietet Un-ternehmen im Falle eines Rechtsstreits ein solides Fundament für die Argumentation.

Nur eine sichere Cloud bringt Vorteile

Laut einer Umfrage von Gartner setzen nicht nur mehr Unternehmen auf Cloud-Lösungen, um ihre bestehenden technologischen Ökosysteme zu erweitern, sondern 75 Prozent der Unternehmen, die diese bereits verwenden, spekulieren, in Zukunft einen Cloud-First-Ansatz zu verfolgen. Viele dieser Un-

ternehmen erkennen den Stel-lenwert der Sicherheit von Daten und Informationen innerhalb der Cloud an – daher steigt der Wunsch, diesen Schutz bestätigt zu bekommen. Eine Zertifizierung der ver-wendeten Cloud-Lösungen und -Dienste nach den Normen ISO / IEC 27001 und 27701 hilft dabei, das entsprechende Vertrauen zu schaffen, und somit den Weg zu einem sicheren ‚Work from anywhere' als Prinzip und einer sicheren, neuen Arbeits-welt zu schaffen.

Alexander Häußler

Viel zu komplex? Wie Unternehmen Multi-Cloud-Umgebungen effektiv absichern können

Die Bereitstellung von Daten und Anwendungen im Rahmen einer verteilten Workforce, geplante Kostenreduktion, verbesserte Skalierbarkeit und die Grundlage für die digitale Transformation: Seit dem Beginn der Pandemie sehen immer mehr Unternehmen die Vorzüge des Cloud Computings und haben Ihre Digitalisierung hier teilweise schneller vorangetrieben als ursprünglich geplant. Oft werden hierbei Multi-Cloud Umgebungen eingesetzt, um auf die individuellen Bedürfnisse der einzelnen Unternehmensbereiche besser eingehen zu können. Doch wo sich Vorteile ergeben, lassen sich auch Nachteile finden: In Multi-Cloud-Umgebungen nehmen diese die Form von Undurchsichtigkeit, wodurch schnell Sicherheitslücken zum Beispiel durch Fehlkonfigurationen entstehen können. Tanja Hofmann, Lead Security Engineer bei McAfee, spricht über die Risiken in der Multi-Cloud und die notwendigen Sicherheitsmaßnahmen.

Fast alle Cloud-Angriffe sind das Ergebnis von Fehlkonfigurationen für die Unternehmen selbst verantwortlich sind. So ergeben sich für die IT ganz neue Herausforderungen, um einen sicheren Betrieb der eingesetzten Lösungen zu ermöglichen. Andererseits sollte Mitarbeitern das Arbeiten von zu Hause ermöglicht werden. Hierzu wurde die Transformation in die Cloud vorangetrieben: Weltweit stieg der Einsatz von Cloud Services und -Anwendungen um 50 Prozent. Nun – nach einem Jahr – ist eine Rückkehr zu alten Prozessen kaum mehr denkbar. Was neben den Vorteilen einer dezentralen IT-Infrastruktur jedoch ebenfalls bleibt, sind die Cyber-Schwachstellen, die mit der Umstellung auf Cloud-Systeme einhergegangen sind. Das liegt vor allem daran, dass der Sicherheitsaspekt aufgrund des spontanen und schnellen Wandels in vielen Unternehmen zu kurz gekommen ist. Die Beseitigung dieser Schwachstellen sollte nun eine hohe Priorität einnehmen, da sich dieses Vorhaben – besonders in wachsenden Multi-Cloud-Umgebungen – als herausfordernd herausstellen kann.

Wenn Fehlkonfigurationen das Bedrohungspotenzial steigern

Immer mehr Unternehmen verbinden verschiedene Cloud Services, -Anwendungen und -Plattformen miteinander, die in der Regel von unterschiedlichen Providern bereitgestellt werden. Laut einer Untersuchung der IDC betonen 87 Prozent der Befragten, dass sie bereits auf Multi-Cloud setzen beziehungsweise sich in der Planungsphase befinden. Der Vorteil einer solchen Umgebung: Jeder Anforderung wie Speicher, Skalierbarkeit oder Datenschutz wird ein passender Cloud Service oder eine -Anwendung, die aus voneinander unabhängig agierenden, miteinander gekoppelten Microservices besteht, zugeordnet. Durch solch eine modulare Architektur erhalten Unternehmen genügend Flexibilität, Cloud-native Anwendungen zu entwickeln und zu hosten.

Doch je mehr Komponenten die Cloud-Infrastruktur erhält, desto undurchsichtiger und unübersichtlicher kann sie werden. Mit schwindender Transparenz steigt das Risiko, Schwachstellen und akute Bedrohungen nicht rechtzeitig zu erkennen sowie zu beheben – für Cyber-Kriminelle eine willkommene Möglichkeit, um schnell und unbemerkt in das Multi-Cloud-Geflecht einzudringen. Ein Beispiel für eine solche Schwachstelle ist die Fehlkonfiguration von Cloud-Systemen, wie zum Beispiel durch (fehlerhafte) Berechtigungsprotokolle oder Systeme, die nicht regelmäßig von der IT gepatcht werden. Unternehmen begünstigen solche Fehlkonfigurationen, indem sie die betroffenen (Cloud-) Systeme nicht an ihre eigenen Anforderungen anpassen, sondern Standardeinstellungen anstandslos übernehmen. Auch in diesem Fall trüben viele Cloud-Systeme den Blick für das Wesentliche: IT-Admins müssen mehrere Cloud-Konfigurationen auf einmal verwalten können.

Tanja Hofmann, Principal Security Engineer, McAfee

360°-Sicherheit: Jeder trägt einen Teil der Verantwortung

Die richtige Sicherheitsstrategie hilft dabei, das volle Potenzial der Multi-Cloud ausschöpfen zu können, und sorgt gleichzeitig dafür, dass Schwachstellen, wie zum Beispiel Fehlkonfigurationen, rechtzeitig vor Cyber-Kriminellen und ihren Intentionen abgesichert werden. Das 360° Shared Responsibility Model gibt hierfür eine eindeutige Orientierung vor, mit der sich Verantwortlichkeiten einteilen und Sicherheitsmaßnahmen entwickeln sowie umsetzen lassen. Wichtig zu bedenken ist, dass die Verantwortung über die Sicherheit von Cloud-Umgebungen nicht allein bei den Cloud Service Providern liegt. Diese konzentrieren ihre Sicherheitsbestreben vornehmlich auf die physischen Bestandteile des Netzwerks sowie die Hosting-Infrastruktur.

Das Identity and Access Management (IAM) hingegen liegt primär in den Händen der Unternehmen, die den Cloud Service beanspruchen. Sprich: