Leitfaden für die Sicherheit von Cloud-Plattformen

Inhalt

Die wichtigsten Punkte

1 Im Idealfall sollte ein Cloud-Anbieter das Identitätsmanagementsystem Ihres Unternehmens in seine Plattform integrieren können; mindestens muss er Ihnen eine vertrauenswürdige Identitätsmanagement-Lösung bereitstellen.

2 Als Voraussetzung für ein Vertrauensverhältnis muss die Cloud-Plattform gut integrierte Firewalls, Sicherheitsgruppen und Optionen für die Mikrosegmentierung auf Basis von Workload und zuverlässigen Compute Hosts bietet.

3 Erwarten Sie vom Cloud-Anbieter BYOK-Lösungen, mit denen Ihr Unternehmen seine eigenen Schlüssel über alle Datenspeicher und Services hinweg verwalten kann.

4 Die beste Sicherheitsmaßnahme für Container besteht darin, sie vor der Implementierung und während des Betriebs auf Sicherheitslücken zu überprüfen.

5 Cloud-Plattform-Sicherheit muss über eine wirksame Zugriffskontrolle verfügen, auf Ebene der Workloads funktionieren, Aktivitäten detailliert rückverfolgen und sich nahtlos in On-Premises-Systeme eingliedern.

Überlegungen zur Sicherheit Cloud-basierter Applikationen

Da immer mehr Organisationen zu einem Cloud-nativen Modell für die Applikationsentwicklung und die Verwaltung von Arbeitslasten übergehen, schränken Cloud-Computing-Plattformen die Wirksamkeit des traditionellen, perimeterbasierten Sicherheitsmodells immer mehr ein. Zwar ist Perimetersicherheit nach wie vor notwendig, aber sie genügt nicht mehr. Da Daten und Applikationen in der Cloud jenseits der alten Unternehmensgrenzen liegen, sind andere Schutzmechanismen erforderlich.

Organisationen, die auf ein Cloud-natives Modell wechseln oder hybride Cloud-Applikationen planen, müssen die traditionelle Netzwerksicherheit auf Perimeter-Basis durch Technologien zum Schutz von Cloud-basierten Arbeitslasten ergänzen. Unternehmen müssen Vertrauen in die Art und Weise haben, wie ein Cloud-Service-Anbieter ihren Stack von der Infrastruktur aufwärts absichert. Überhaupt ist das Vertrauen in die Plattform-Security ist zu einem grundlegenden Faktor bei der Auswahl eines Anbieters geworden.

Cloud-Sicherheitstreiber

Datenschutz und die Einhaltung der gesetzlichen Auflagen gehören zu den wichtigsten Treibern der Cloud-Sicherheit – aber gleichzeitig sind sie auch Stolpersteine auf dem Weg zur Cloud. Um diesbezügliche Bedenken aus dem Weg zu räumen, müssen sämtliche Aspekte der Entwicklung und der operativen Abläufe miteinbezogen werden. Bei Cloud-nativen Anwendungen sind Daten über Objektspeicher, Datendienste und Clouds verteilt, womit sich eine Reihe von Einfallstoren für potenzielle Angriffe ergeben. Und die Attacken stammen nicht nur von raffinierten Cyber-Gangs und externen Quellen; laut einer kürzlich durchgeführten Umfrage meldeten 53 Prozent der Befragten, in den vergangenen 12 Monaten Insider-Angriffe erlebt zu haben.[1]

Fünf Prinzipien der Cloud-Sicherheit

Um die speziellen Sicherheitsanforderungen zu erfüllen, die mit der Nutzung von Cloud-Plattformen einhergehen, müssen Organisationen sich auf vertrauenswürdige Technologiepartner verlassen können. Deshalb sollten potenzielle Cloud-Anbieter auf der Basis dieser fünf Sicherheitsaspekte – angepasst auf ihre ganz konkreten Bedürfnisse – bewertet werden:

1. **Identitäts- und Zugriffsverwaltung:** Authentifizierung, Identitäts- und Zugangskontrollen
2. **Netzwerksicherheit:** Schutz, Isolierung und Segmentierung
3. **Datenschutz:** Datenverschlüsselung und Schlüsselverwaltung
4. **Applikationssicherheit und DevSecOps:** Einschließlich Sicherheitsprüfung und Containersicherheit
5. **Sichtbarkeit und Information:** Überwachung und Analyse von Protokollen, Datenflüssen und Ereignissen auf Muster

Identitäts- und Zugriffsmanagement auf einer Cloud-Plattform

Jede Interaktion mit einer Cloud-Plattform beginnt mit der Identitätsprüfung, die feststellt, wer oder was die Interaktion anstößt – ein Administrator, ein Benutzer oder ein Service. In der API-Ökonomie besitzen Services eine eigene Identität. Deshalb ist die Fähigkeit, einen API-Aufruf präzise und sicher an einen auf dieser Identität basierenden Service zu übermitteln, für die erfolgreiche Ausführung von Cloud-nativen Apps unerlässlich.

Halten Sie Ausschau nach Anbietern, die eine konsistente Methode zur Authentifizierung einer Identität für API-Zugriff und Service-Aufrufe anbieten. Außerdem benötigen Sie eine Möglichkeit, Endbenutzer, die auf in der Cloud gehostete Applikationen zugreifen, zu identifizieren und zu authentifizieren. IBM Cloud verwendet beispielsweise App ID als eine Möglichkeit für Entwickler, Authentifizierung in ihre Mobil- und Webanwendungen zu integrieren.

Eine starke Authentifizierung verhindert den Zugriff auf Cloud-Systeme durch Unbefugte. Da das Plattform-Identitäts- und Zugriffsmanagement (IAM) so grundlegend ist, sollten Organisationen, die über ein bestehendes System verfügen, von Cloud-Anbietern erwarten, dass sie dieses integrieren können. Oft wird dies durch eine Identitätsföderationstechnologie unterstützt, welche die ID und die Attribute einer Person über mehrere Systeme hinweg verknüpft.

Warum Service-Aufrufe authentifizieren?

In Mikroservice-Architekturen sind APIs die Schnittstellen, die dafür sorgen, dass Applikationen miteinander kommunizieren und Daten austauschen können; wenn eine Applikation für ihre Aufgaben Services aufrufen will, nutzt sie ebenfalls APIs. So ruft eine Applikation z.B. einen Objektspeicher-Service für Daten auf. Um der Anforderung nachzukommen, ruft der Objektspeicher-Service seinerseits dann einen Schlüsselmanagement-Service auf, um die für die Dekodierung der Daten benötigten Schlüssel zu erhalten. Und als Teil der Bereitstellung der Benutzererfahrung könnte eine App APIs verwenden, um auf Identitätsdaten zuzugreifen, Inhalte zwischen Apps zu posten (z. B. Inhalte aus einer App auf Twitter) und den Standort eines Benutzers zu ermitteln, dem standortspezifische Informationen bereitgestellt werden müssen. **All diese Integrationspunkte stellen potenzielle sicherheitstechnische Probleme dar.**

Cloud-Anbieter sollten also über ein einheitliches Verfahren zur Authentifizierung der Identität eines Benutzers oder eines Services verfügen, der auf eine API oder einen Service zugreifen muss. Als Teil der Authentifizierung sollten natürlich alle Zugangsanforderungen, die von Sitzungen und Transaktionen ausgehen, für Prüfungszwecke aufgezeichnet werden. **APIs und Services enthalten mit großer Wahrscheinlichkeit wertvolles geistiges Eigentum, weshalb sie nicht für jedermann zugänglich sein dürfen.**

Bitten Sie potenzielle Cloud-Anbieter, nachzuweisen, dass ihre IAM-Architektur und -Systeme alle diese Grundlagen abdecken. In der IBM Cloud basiert das Identitäts- und Zugriffsmanagement auf mehreren Schlüsselfunktionen (Abb. 1):

Identität

- Jeder Benutzer hat eine eindeutige Kennung
- Services und Anwendungen werden anhand ihrer Service-IDs identifiziert
- Ressourcen werden durch den Namen der Cloud-Ressource (CRN) identifiziert und adressiert
- Benutzer und Services werden authentifiziert und erhalten Token mit ihren Identitäten

Zugriffsmanagement

- Wenn Benutzer und Services auf Ressourcen zuzugreifen versuchen, bestimmt ein IAM-System, ob der Zugriff und die Aktionen genehmigt oder verweigert werden
- Services definieren Aktionen, Ressourcen und Rollen
- Administratoren definieren Richtlinien, die Benutzern Rollen und Rechte an verschiedenen Ressourcen zuweisen
- Der Schutz erstreckt sich auf APIs, Cloud-Funktionen und Back-End-Ressourcen, die in der Cloud gehostet werden

Bei der Beurteilung der Sicherheit eines Cloud-Anbieters, achten Sie auf Zugriffskontrolllisten, zusammen mit allgemeinen Ressourcennamen, mit denen Sie Benutzer nicht nur auf bestimmte Ressourcen, sondern auch auf bestimmte Vorgänge auf diesen Ressourcen beschränken können. Mit diesen Funktionen können Sie sicherstellen, dass Ihre Daten sowohl vor unbefugten externen als auch internen Zugriffen geschützt sind.

Die Erweiterung Ihres eigenen Enterprise Identity Providers (Enterprise IdP) auf die Cloud ist besonders dann sinnvoll, wenn Sie eine Cloud-native Anwendung auf eine bestehende Unternehmensanwendung aufsetzen, die den Enterprise IdP verwendet. Ihre Benutzer können sich problemlos sowohl bei den Cloud-nativen als auch bei den zugrunde liegenden Applikationen anmelden, ohne mehrere Systeme oder IDs verwenden zu müssen. Komplexität zu vereinfachen ist immer eine gute Sache.

Der wichtigste Punkt

Im Idealfall sollte ein Cloud-Anbieter das Identitätsmanagementsystem Ihres Unternehmens in seine Plattform integrieren können; zumindest muss er Ihnen eine vertrauenswürdige Identitätsmanagement-Lösung bereitstellen.

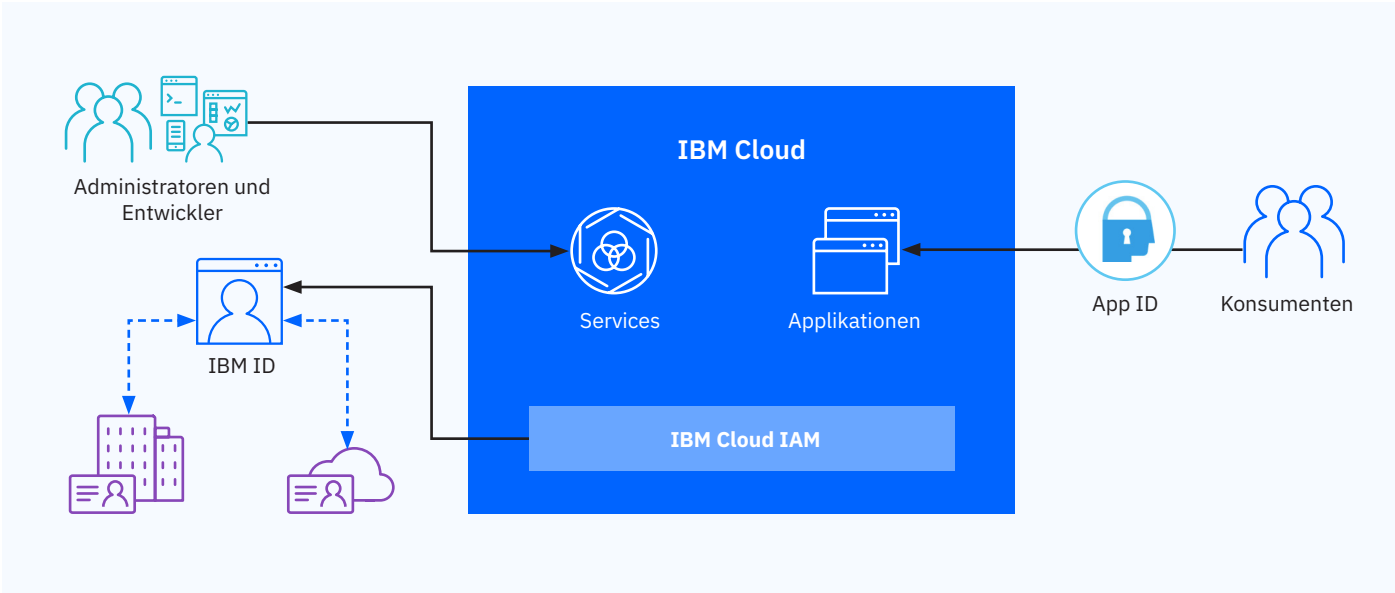


Abb. 1: Trennung von anbieter- und kundenverwalteten Cluster-Elementen.

Neudefinition von Netzwerkisolierung und -schutz

Viele Cloud-Anbieter verwenden Netzwerksegmentierung, um den Zugriff auf Geräte und Server im selben Netzwerk zu beschränken. Zusätzlich richten Anbieter auf der physischen Infrastruktur virtuelle isolierte Netzwerke ein und beschränken Benutzer oder Services automatisch auf ein bestimmtes isoliertes Netzwerk. Diese und andere grundlegende Netzwerksicherheitstechnologien sind wichtige Kriterien für das Vertrauen in eine Cloud-Plattform.

Cloud-Anbieter bieten Schutztechnologien – angefangen von Web-Anwendungs-Firewalls bis hin zu virtuellen privaten Netzwerken und Schadensbegrenzung im Fall von Denial-of-Service-Attacken – als Dienstleistungen für softwaredefinierte Netzwerksicherheit und mit einer Gebühr pro Nutzung an. Entscheidend für die Netzwerksicherheit in der Cloud Computing-Ära sind die folgenden Technologien.

Sicherheitsgruppen und Firewalls

Cloud-Kunden setzen häufig Netzwerk-Firewalls zum Schutz des Perimeters ein (Virtual Private Cloud/ Netzwerkzugang auf Subnetz-Ebene) und erstellen Netzwerksicherheitsgruppen für den Zugriff auf Instanzebene. Sicherheitsgruppen sind eine gute erste Verteidigungslinie für die Zuweisung von Zugangsrechten zu Cloud-Ressourcen. Anhand solcher Gruppen können Sie auf einfache Weise Netzwerksicherheit auf Instanzebene hinzufügen, um ein- und ausgehenden Datenverkehr in Public- und Private-Netzwerken zu verwalten.

Viele Kunden benötigen eine Perimeterkontrolle, um das Perimeternetzwerk und die Subnetze zu sichern. Hier sind virtuelle Firewalls eine einfach zu implementierende Möglichkeit, um genau dies zu erreichen. Firewalls sollen verhindern, dass unerwünschter Datenverkehr auf Servern landet, und auch die potenzielle Angriffsfläche reduzieren. Von einem Cloud-Anbieter dürfen Sie erwarten, dass er Ihnen sowohl virtuelle als auch Hardware-Firewalls anbietet, damit Sie rechtebasierende Regeln für das gesamte Netzwerk oder Teilnetze konfigurieren können.

VPNs bieten sichere Verbindungen von der Cloud zurück zu Ihren On-Premises-Ressourcen und sind deshalb in einer hybriden Cloud-Umgebung unentbehrlich.

Mikro-Segmentierung

Die Cloud-native Entwicklung von Anwendungen als ein Satz kleiner Services bietet den Sicherheitsvorteil, dass diese anhand von Netzwerksegmenten isoliert werden können. Suchen Sie also nach einer Cloud-Plattform, die durch die Automatisierung der Netzwerkkonfiguration und Netzwerkbereitstellung eine Mikrosegmentierung implementiert. **Containerisierte Anwendungen, die auf dem Mikrodienstmodell basieren, werden mittlerweile zu einem Standard, wenn eine skalierbare Workload-Isolierung unterstützt werden soll.**

Der wichtigste Punkt

Als Voraussetzung für ein Vertrauensverhältnis muss die Cloud-Plattform gut integrierte Firewalls, Sicherheitsgruppen und Optionen für die Mikrosegmentierung auf Basis von Workload und zuverlässigen Compute Hosts bietet.

Datenschutz mit Verschlüsselung und Schlüsselverwaltung

Der zuverlässige Schutz von Daten ist ein grundlegendes Sicherheitskriterium für jedes digitale Unternehmen – insbesondere in stark regulierten Branchen wie Finanzdienstleistungen und Gesundheitswesen.

Bei Cloud-nativen Anwendungen sind Daten meist über Objektspeicher, Datendienste und Clouds verteilt. Traditionelle Anwendungen haben oft eine eigene Datenbank, eine eigene VM und sensible Informationen in Dateien. Letztere müssen auf jeden Fall verschlüsselt werden, und zwar sowohl im Ruhezustand als auch beim Transit.

Unternehmen fürchten zu Recht, dass Cloud-Betreiber oder andere nicht autorisierte Benutzer ohne ihr Wissen auf ihre Daten zugreifen, und erwarten deshalb vollständige Transparenz bezüglich des Datenzugriffs. **Inzwischen sind die Kontrolle des Zugangs zu Daten, aber auch des Zugangs zu Kodierungsschlüsseln, zu einer Selbstverständlichkeit geworden.** Dies hat dazu geführt, dass das Bring-your-own-Keys-(BYOK-)Modell eine Sicherheitsvoraussetzung für die Cloud darstellt. Es ermöglicht Ihnen die Verwaltung von Kodierungsschlüsseln an einem zentralen Ort, bietet die Sicherheit, dass Root-Schlüssel niemals die Grenzen des Schlüsselverwaltungssystems verlassen, und ermöglicht Ihnen die Prüfung aller Aktivitäten im Lebenszyklus der Schlüsselverwaltung (Abb. 2).

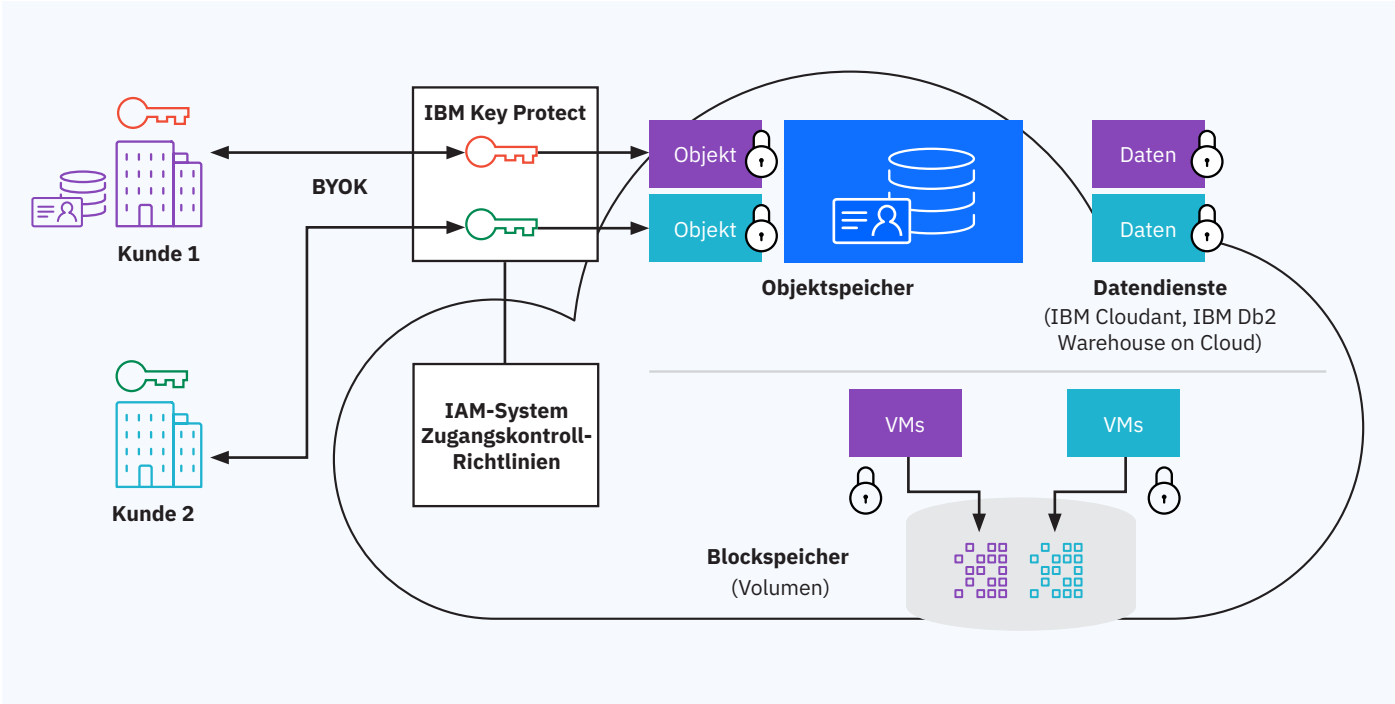
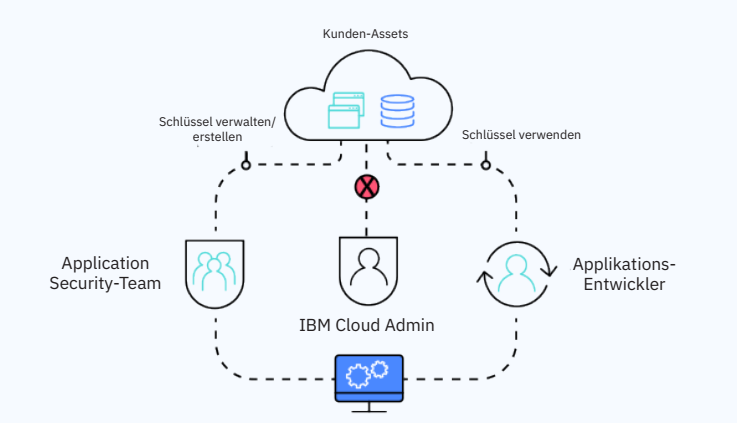


Abb. 2. Architektur einer BYOK-Lösung.

Keep your own key (KYOK)

Für die Einführung von Datensicherheit, die in der Public Cloud zu 100% privat bleibt, bietet IBM eine exklusive Lösung, mit der Sie der alleinige „Hüter“ Ihres Kodierungsschlüssels sind. Als einzige Services in der Branche auf Basis von FIPS 140-2 Level 4-zertifizierter Hardware bieten IBM Cloud Hyper Protect Crypto Services ein Schlüsselverwaltungs- und Cloud-Hardware-Sicherheitsmodul (HSM).



Vertrauenswürdige Host-Computer

Es kommt auf die Hardware an: Niemand will wertvolle Daten und Anwendungen auf einem nicht vertrauenswürdigen Host bereitstellen. Anbieter von Cloud-Plattformen, die Hardware mit Measure-Verify-Launch-Protokollen einsetzen, stellen High-Security-Hosts für Anwendungen innerhalb des Container-Orchestrierungssystems bereit.

Intel Trusted Execution Technology (Intel TXT) und Trusted Platform Module (TPM) sind Beispiele für Technologien auf Host-Ebene, die als Vertrauensanker für Cloud-Plattformen dienen. Intel TXT gewährt Schutz gegen softwarebasierte Angriffe, die auf sensible Informationen aus sind und zu diesem Zweck den System- oder BIOS-Code korrumpieren oder die Plattformkonfiguration verändern. Intel TPM ist ein hardwarebasierter Bootschutz, der die Systemumgebung auf Manipulationen überprüft, ehe die Kontrolle an das Betriebssystem übergeben wird.

Datenschutz im Ruhezustand und beim Transit.

Durch die integrierte Verschlüsselung mit BYOK behalten Sie die Kontrolle über Ihre Daten, egal ob diese vor Ort oder in der Cloud gespeichert sind. Dies ist eine ausgezeichnete Methode zur Kontrolle des Datenzugriffs in Cloud-nativen Anwendungsimplementierungen. Bei diesem Ansatz erzeugt das kundeneigene Schlüsselverwaltungssystem vor Ort einen Schlüssel und übergibt diesen dem Schlüssel-Managementservice des Anbieters. Dieser Ansatz umfasst die Verschlüsselung von Daten im Ruhezustand über Speichertypen wie Block-, Objekt- und Datenservices hinweg.

Für Daten im Transit findet die sichere Kommunikation und Übertragung über Transport Layer Security/ Secure Sockets Layer (TLS/SSL) statt. Die TLS/ SSL-Verschlüsselung ermöglicht es Ihnen auch, Konformität, Sicherheit und Governance nachzuweisen, ohne dass eine administrative Kontrolle über das Kryptosystem oder die Infrastruktur erforderlich ist. Die Fähigkeit, SSL-Zertifikate zu verwalten, ist ein weiteres Kriterium für das Vertrauen in eine Cloud-Plattform.

Erfüllung von Audit- und Compliance-Anforderungen

Indem Sie Ihre eigenen Kodierungsschlüssel in der Cloud verwahren – ohne dass der Dienstanbieter darauf Zugriff hätte – gewährleisten Sie die für CISO-Compliance-Audits erforderliche Transparenz und Kontrolle der Informationen.

Der wichtigste Punkt

Erwarten Sie vom Cloud-Anbieter BYOK-Lösungen, damit Ihr Unternehmen seine eigenen Schlüssel über alle Datenspeicher und Services hinweg verwalten kann.

Sicherheitsautomatisierung für DevOps

DevOps-Teams benötigen beim Aufbau von Cloud-native Services und beim Arbeiten mit Containertechnologien eine Möglichkeit, Sicherheitsprüfungen in eine zunehmend automatisierte Pipeline zu integrieren. Durch die Nutzung von Sites wie Docker Hub, die den offenen Austausch fördern, sind Einsparungen bei der Image-Vorbereitung möglich: Die Entwickler laden sich einfach herunter, was sie benötigen. Aber diese Flexibilität erzwingt eine routinemäßige Überprüfung aller Container-Images, die in einer Registry abgelegt sind, bevor sie eingesetzt werden.

Eigens zu diesem Zweck wurde ein automatisiertes Scanning-System entwickelt, das die Images auf mögliche Sicherheitsprobleme analysiert und so Vertrauen zementiert. Fragen Sie die Plattformanbieter, ob sie es Ihrer Organisation gestatten, Richtlinien (wie „Keine Images mit Sicherheitslücken verwenden“ oder „Vor Verwendung dieser Images in der Produktion eine Warnung ausgeben“) als Teil der Pipeline-Sicherheit von DevOps festzulegen.

IBM Cloud Container Service ist mit einem VA-System (Vulnerability Advisor) ausgerüstet, das sowohl statisches als auch Live-Container-Scannen ermöglicht. VA (Vulnerability Advisor) überprüft die einzelnen Schichten jedes Image in der privaten Registry eines Cloud-Kunden, um Sicherheitslücken oder Malware vor Bereitstellung des Image aufzuspüren. Da beim einfachen Scannen von Registry-Images Probleme wie Drift vom statischen Image zum eingesetzten Container übersehen werden können, scannt VA auch in Betrieb befindliche Container auf Anomalien. Ferner gibt es auch Empfehlungen in Form von Warnungen (verschiedene Stufen) aus.

Der wichtigste Punkt

Die beste Sicherheitsmaßnahme für Container besteht darin, sie vor der Implementierung und während des Betriebs auf potenzielle Sicherheitslücken zu überprüfen.

Weitere VA-Funktionen, die zur Automatisierung der Sicherheit in der DevOps-Pipeline beitragen, sind:

- **Einstellungen für Richtlinienverletzungen:** Mit VA können Administratoren Richtlinien für die Image-Bereitstellung festlegen, die auf drei Arten von Image-Problemsituationen basieren: installierte Pakete mit bekannten Sicherheitslücken, aktivierte Remote-Anmeldungen und aktivierte Remote-Anmeldungen durch Benutzer, deren Kennwörter leicht zu erraten sind.
- **Beste Praktiken:** VA prüft derzeit 26 Regeln, die auf ISO 27000 basieren, einschließlich Einstellungen wie minimales Kennwortalter und Mindestkennwortlänge.
- **Erkennung von Sicherheits-Fehlkonfigurationen:** VA kennzeichnet jedes Fehlkonfigurationsproblem, beschreibt es und empfiehlt eine Vorgehensweise zur Behebung.
- **Integration mit IBM X-Force:** VA bezieht Sicherheitsinformationen aus fünf Drittquellen und bewertet verletzliche Stellen anhand von Kriterien wie Angriffsvektor, Komplexität und Verfügbarkeit einer bekannten Lösung. Das Bewertungsschema (kritisch, hoch, mäßig oder gering) hilft den Administratoren, den Schweregrad von Sicherheitsproblemen schnell zu verstehen und Prioritäten für deren Behebung zu setzen.

Bei der Problembehebung verursacht VA keine Unterbrechungen für Patchingzwecke. Stattdessen korrigiert IBM das „goldene Image“ in der Registry und stellt dem Container ein neues Image zur Verfügung. Dieser Ansatz trägt dazu bei, sicherzustellen, dass alle künftigen Instanzen des Image dasselbe Patch aufweisen. VMs können immer noch auf herkömmliche Weise gehandhabt werden, nämlich unter Verwendung eines Endpunktsicherheitsservice zum Patchen von VM und zum Beheben von Linux-Sicherheitslücken.

Man spricht Kubernetes

Wenn Ihre DevOps-Teams mit der beliebten Kubernetes Container-Orchestrierungssoftware arbeiten, sorgen Sie dafür, dass sie weiterhin ihre Lieblings-Tools verwenden können. Achten Sie auch darauf, wie leicht es ist, auf einer Plattform neue Kubernetes-Cluster einzuführen und bestehende zu verwalten.

Fragen Sie nach, ob der Anbieter von Cloud-Plattformen Calico und Istio mit seinem Kubernetes-System unterstützt. Calico und Istio sind zwei wichtige Komponenten von Kubernetes, wenn es um Anwendungs- und Workload-Sicherheit geht. Calico hilft bei der Vereinfachung der Verwaltung von IP-Adressen, die den Arbeitslasten in einem Rechenknoten zugewiesen sind, und programmiert Zugriffskontrolllisten in jedem Rechenknoten zur Durchsetzung von Sicherheitsrichtlinien. Über Richtliniendefinitionen und Konfigurations-Labels bietet Istio eine zertifikatsbasierte Steuerung der Kommunikation zwischen Mikroservices innerhalb eines Kubernetes-Pods oder -Clusters.

Schaffung eines Sicherheitsimmunsystems durch intelligentes Monitoring

Beim Umzug in die Wolke machen sich CISOs oft Sorgen über mangelnde Visibilität und Verlust der Kontrolle. Da die gesamte Cloud des Unternehmens ausfallen kann, wenn ein bestimmter Schlüssel gelöscht wird oder eine Konfigurationsänderung versehentlich eine Verbindung zurück zu lokalen Ressourcen oder einem Enterprise Security Operations Center (SOC) unterbricht, warum sollten die Betriebsingenieure nicht darauf bestehen, volle Transparenz über cloudbasierte Arbeitslasten, APIs, Mikroservices – also eigentlich über alles – zu haben?

Zugriffswege und Prüfungsprotokolle

Alle Benutzer- und Verwaltungszugriffe, ob durch den Cloud-Anbieter oder Ihre Organisation, sollten automatisch protokolliert werden. Ein integrierter Cloud Activity Tracker kann eine „Spur“ aller Zugriffe auf die Plattform und Services legen, einschließlich API, Web- und Mobilzugriff. Ihr Unternehmen sollte in der Lage sein, diese Protokolle zu konsumieren und sie in das Security Operations Center (SOC) Ihres Unternehmens zu integrieren.

Unternehmenssicherheits-Informationen

Vergewissern Sie sich, dass die Möglichkeit besteht, alle Protokolle und Ereignisse in Ihr SIEM (Security Information and Event Management)-System vor Ort zu integrieren (Abb. 3). Manche Anbieter von Cloud-Diensten bieten auch Sicherheitsüberwachung mit Vorfallmanagement und Reporting, Echtzeitanalyse von Sicherheitswarnungen und eine integrierte Ansicht über hybride Implementierungen hinweg.

IBM QRadar zum Beispiel ist eine umfassende SIEM-Lösung mit einer Reihe von Sicherheits-Intelligence-Lösungen, die imstande sind, mit den Bedürfnissen eines Unternehmens zu wachsen. Seine maschinellen Lernfähigkeiten trainieren Bedrohungsmuster auf eine Weise, die ein prädiktives Security-Immunsystem aufbaut.

Managed Security mit Kompetenz

Wenn Ihre Organisation nicht selbst über viel Sicherheitskompetenzen verfügt, sollten Sie sich nach einem Anbieter umsehen, der für Sie das Sicherheitsmanagement übernimmt. Manche Anbieter können Ihre Sicherheitsvorfälle überwachen, Bedrohungsinformationen aus einer Vielzahl von Branchen abrufen und diese Informationen korrelieren, um geeignete Maßnahmen zu ergreifen. Fragen Sie, ob auch eine zentrale Konsole dabei ist, die interne und verwaltete Sicherheitsservices integriert.

Der wichtigste Punkt

Cloud-Plattform-Sicherheit muss über eine wirksame Zugriffskontrolle verfügen, auf Ebene der Workloads funktionieren, Aktivitäten detailliert rückverfolgen und sich nahtlos in On-Premises-Systeme eingliedern.

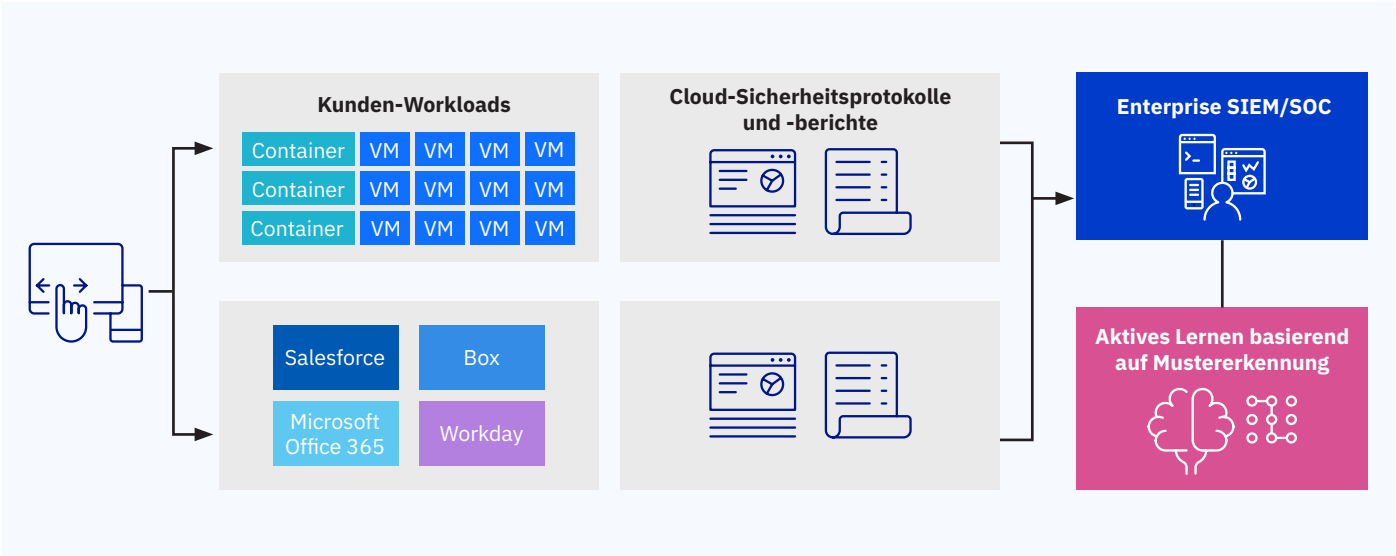


Abb. 3 Integration der Cloud-Visibilität in ein Unternehmens-SIEM/SOC.

Sicherheit als Treiber des geschäftlichen Erfolgs

Angesichts der Tatsache, dass Cloud-Technologie ein immer größerer und wichtigerer Teil des digitalen Unternehmens wird, lohnt es sich, nach einem Cloud-Anbieter Umschau zu halten, der die richtigen Funktionen und Kontrollen zum Schutz Ihrer Daten, Anwendungen und der Cloud-Infrastruktur bietet, von der die kundenseitigen Anwendungen abhängen. Achten Sie darauf, dass die Plattform-Sicherheitslösung die fünf wichtigsten Schwerpunktbereiche der Cloud-Sicherheit abdeckt: Identität und Zugriff, Netzwerksicherheit, Datenschutz, Anwendungssicherheit sowie Sichtbarkeit und Intelligenz. Denn schließlich wollen Sie sich nicht groß um die Technologie kümmern, sondern sich auf Ihr Kerngeschäft konzentrieren.

Eine gut abgesicherte Cloud bietet signifikante Geschäfts- und IT-Vorteile, darunter:

- **Weniger Zeit bis zur Wertschöpfung:** Da die Sicherheit bereits installiert und konfiguriert ist, können die Teams problemlos Ressourcen bereitstellen und schnell einen Prototyp der Benutzererfahrung erstellen, Ergebnisse auswerten und bei Bedarf iterieren.
- **Geringere Investitionen:** Durch die Nutzung von Sicherheitsdiensten in der Cloud können viele Anschaffungskosten, einschließlich Server, Softwarelizenzen und Appliances, eingespart werden.
- **Weniger Admin-Aufwand** Durch den erfolgreichen Aufbau und die Aufrechterhaltung des Vertrauens in die Cloud-Plattform übernimmt der Anbieter mit den richtigen Sicherheitsangeboten den größten Verwaltungsaufwand und senkt damit Ihre Kosten für Reporting und Ressourcenpflege.

Lesen Sie die Gartner Peer Insights für die Gründe, warum IBM Cloud:

die höchsten Bewertungen für Enterprise Integration (4,6 von 5 Sternen) erhalten hat

und unter den führenden Cloud-Anbietern insgesamt am höchsten bewertet wird (4,7 von 5 Sternen)

... basierend auf **90 Reviews in den letzten 12 Monaten, Stand 1. Juni 2020.**

https://www.gartner.com/reviews/market/public-cloud-iaas/vendor/ibm/product/ibm-cloud

Die Bewertungen von Gartner Peer Insights stellen die subjektiven Meinungen einzelner Endnutzer auf Basis ihrer eigenen Erfahrungen dar und repräsentieren nicht die Ansichten von Gartner oder seinen Partnern.

Weitere Informationen

Um mehr über die fünf Schlüsselbereiche der Cloud-Sicherheit und verwandte Technologien und Dienstleistungen von IBM zu erfahren, besuchen Sie: **ibm.com**/cloud/security

Bleiben Sie in Verbindung

IBM-Cloud-Blog

Folgen Sie uns

@IBMcloud
Facebook

Wir bleiben in Kontakt:

LinkedIn
YouTube

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

[1] Insider Threat 2018 Report, hg. im November 2017, http://crowdresearchpartners.com/portfolio/insider-threat-report