SOPHOS

Sicherheit für die **Public Cloud:** Sieben Best Practices

Sophos-Whitepaper Juni 2019

Inhaltsverzeichnis

Sicherheit für die Public Cloud: Sieben Best Practices

Was würden Sie beim Schutz von Anwendungen in der Public Cloud als Erfolg verbuchen?

Vielleicht ein Jahr ohne Datenpanne mit Negativschlagzeilen? Oder den Footprint der Cloud-Infrastruktur Ihres Unternehmens zu verstehen, damit Sie angemessene Schutzmaßnahmen ergreifen können? Vielleicht möchten Sie einfach sicherstellen, dass Compliance-Audits reibungslos über die Bühne gehen? Oder wollen Sie die Zusammenarbeit an Sicherheits- und Compliance-Problemlösungen mit silobasierter Compliance und Entwicklungsteams verbessern?

Egal, was Ihre Prioritäten sind: Dieser Guide hält nützliche Tipps für Sie bereit. Sie erfahren, welche sieben Schritte für die Sicherheit der Public Cloud am wichtigsten sind, und erhalten praktische Tipps, die Sie in Ihrem Unternehmen einfach umsetzen können. Forschungsergebnisse aus den SophosLabs veranschaulichen Ihnen zudem, mit welcher Häufigkeit Cyberkriminelle cloudbasierte Instanzen angreifen. Abschließend erfahren Sie, wie Sie die Nutzung der Public Cloud mit Sophos Cloud Optix sicherer und transparenter gestalten.

Neue Instanzen in Amazon Web Services (AWS), Microsoft Azure oder der Google Cloud Platform (GCP) einzurichten, ist einfach. Die Schwierigkeit für Operations-, Sicherheits-, Entwicklungs- und Compliance-Teams besteht darin, alle Daten, Workloads und Architekturänderungen in diesen Umgebungen im Blick zu behalten, um die Sicherheit gewährleisten zu können.

Public-Cloud-Anbieter müssen für die Sicherheit der Cloud sorgen (Sicherheit der physischen Rechenzentren sowie Trennung von Kundenumgebungen und Daten). Die Verantwortung für die Sicherheit der Workloads und Daten, die Sie in die Cloud verlagern, tragen jedoch allein Sie. Ihre Cloud-Umgebung müssen Sie genauso schützen wie Daten in Ihren lokalen Netzwerken. Missverständnisse über diese Zuständigkeiten sind weitverbreitet und die daraus resultierenden Sicherheitslücken haben cloudbasierte Workloads zur neuen Goldgrube für clevere Hacker gemacht.

Die größten Herausforderungen beim Thema Cloud Security

Betrachtet man die Benutzerfreundlichkeit und Kosteneffizienz der Public Cloud, verwundert es kaum, dass immer mehr Unternehmen Amazon Web Services, Microsoft Azure und die Google Cloud Platform nutzen. Innerhalb von Minuten können Sie neue Instanzen einrichten und Ressourcen ganz nach Bedarf skalieren. Sie zahlen immer nur für die Leistungen, die Sie tatsächlich in Anspruch nehmen und vermeiden hohe Anschaffungskosten für Hardware.

Die Public Cloud löst viele Ressourcen-Probleme der traditionellen IT, wirft jedoch neue Probleme auf. Das Erfolgsrezept für eine effektive Cybersecurity in der Cloud besteht darin, Ihren Sicherheitsstatus insgesamt zu verbessern: Ihre Architektur muss korrekt konfiguriert und sicher sein, Sie müssen die nötige Transparenz über Ihre Architektur haben und vor allem wissen, wer Zugriff darauf hat.

Was sich einfach anhört, ist in der Realität alles andere als das.

Die rasant wachsende Beliebtheit der Cloud hat dazu geführt, dass Daten auf verschiedenste Speicherorte verteilt sind und sich Workloads auf unterschiedlichen Instanzen und bei einigen Unternehmen auch auf verschiedenen Plattformen befinden. Unternehmen führen bereits jetzt im Schnitt Anwendungen in zwei Public Clouds aus und experimentieren mit weiteren 1,8 Public Clouds [1]. Die Nutzung mehrerer Clouds macht es für IT-Abteilungen noch schwieriger, den Überblick zu behalten, weil sie von einer Plattform zur nächsten wechseln müssen, um ein Gesamtbild aller cloudbasierten Assets zu erhalten.

Eine mangelnde Transparenz über cloudbasierte Workloads führt zu Sicherheits- und Compliance-Risiken:

Höhere Anfälligkeit

Mehr Agilität und eine kürzere Zeit bis zur Markteinführung (Time-to-Market) von Produkten und Services sind für Unternehmen ein großer Anreiz, in die Public Cloud zu migrieren. Hierfür wird in der Regel die Agilität und Reaktionsschnelligkeit eines DevOps-Ansatzes benötigt. Für viele bedeutet dieser neue Ansatz bei Entwicklung und Produkt-Releases, dass mehrere Entwickler auf verschiedenen Plattformen arbeiten, und das oft auch noch in verschiedenen Zeitzonen.

Die Nachverfolgung der Workloads war wesentlich einfacher, als Entwicklungszyklen noch Monate oder sogar Jahre dauerten – aber diese Zeiten sind vorbei. Heute müssen Sie mit zahlreichen Releases Schritt halten und das nicht selten an ein- und demselben Tag. Schnelllebige Architekturänderungen, Konfigurationsupdates und Sicherheitsgruppen-Einstellungen rund um die Uhr im Auge zu behalten, ist nahezu unmöglich. Als Folge sind Sie anfälliger für Cyberbedrohungen, da Schwachstellen schnell ausgenutzt werden können.

Bedrohungen für Daten, geistiges Eigentum und Services

Genau wie Unternehmen wissen auch Cyberkriminelle die Automatisierungsvorteile der Public Cloud zu schätzen. Angreifer spähen heutzutage immer häufiger Cloud-Umgebungen aus und nutzen systemeigene Cloud-Anbieter-APIs, um die Bereitstellung neuer Instanzen zu automatisieren, offene Datenbanken zu kompromittieren, Sicherheitseinstellungen zu ändern und legitime Benutzer auszusperren.

Um das Ausmaß der Problematik zu verdeutlichen, richteten die SophosLabs vor Kurzem in den weltweit 10 beliebtesten AWS-Rechenzentren Umgebungen ein. Das Ergebnis dieses Experiments:

- Innerhalb von 2 Stunden gab es bei allen 10 Rechenzentren Anmeldeversuche [2]
- Für jedes Gerät registrierten sie im Schnitt 13 Anmeldeversuche pro Minute, oder 757 pro Stunde

Diese Ergebnisse zeigen, wie häufig Cyberkriminelle cloudbasierte Instanzen mit hochentwickelten automatisierten Verfahren angreifen. Die Herausforderung für Sicherheitsteams besteht darin, potenzielle Schwachstellen zu beheben, bevor sie von Angreifern ausgenutzt werden, und ungewöhnliches (Angreifer-)Verhalten in Echtzeit zu erkennen, damit Angriffe frühzeitig gestoppt werden können.

Aufrechterhaltung von Compliance-Standards

Ganz gleich, wo sich Ihre Infrastruktur und Daten befinden: Sie müssen Compliance mit geltenden Vorschriften nachweisen, z. B. der DSGVO. Andernfalls riskieren Sie Compliance-Verstöße und entsprechende Strafen.

Die Herausforderung in der Cloud besteht darin, dass sich Umgebungen täglich, stündlich oder sogar minütlich ändern. Wöchentliche oder monatliche Compliance Checks mögen in lokalen Netzwerken funktioniert haben. Mit der Dynamik der Public Cloud können sie nicht mithalten. Für Teams, die Cloud-Umgebungen manuell oder mit nativen Tools verwalten, sind die kontinuierlich erforderlichen Compliance-Analysen oft kaum zu bewältigen. Hinzu kommt, dass es nach dem Erkennen eines Compliance-Verstoßes oft schwierig ist, schnell genug auf die Situation zu reagieren, weil die Sicherheits-, Entwicklungs- Operations- und Compliance-Teams in den meisten Unternehmen nicht entsprechend miteinander vernetzt sind.

In sieben Schritten zu einer sicheren Public Cloud

Schritt 1: Kennen Sie Ihre Verantwortung

So banal wie dies klingen mag, ist es nicht – denn in der Cloud gelten beim Thema Sicherheit spezielle Regeln. Public-Cloud-Anbieter wie Amazon Web Services, Microsoft Azure und die Google Cloud Platform setzen auf ein Shared-Responsibility-Modell – die Anbieter sorgen für die Sicherheit der Cloud, doch Sie selbst sind für die Sicherheit aller Inhalte verantwortlich, die Sie in die Cloud verlagern.

Der physische Schutz im Rechenzentrum sowie die virtuelle Trennung von Kundendaten und Umgebungen liegt im Verantwortungsbereich der Public-Cloud-Anbieter.

Eventuell erhalten Sie einige grundlegende Firewall-Regeln, mit denen Sie den Zugriff auf Ihre Umgebung regeln können. Wenn Sie diese jedoch nicht korrekt konfigurieren – z. B. Ports für die gesamte Welt offen lassen – haben Sie die Konsequenzen zu tragen. Sie müssen also wissen, für welche Bereiche der Sicherheit Sie verantwortlich sind.

Abbildung 1 gibt einen Überblick über die jeweiligen Verantwortlichkeiten. Alternativ können Sie auch unser Video ansehen.

Shared-Responsibility-Sicherheitsmodell	Lokal	Public Cloud	Zweck
Benutzer	■	■	Durchsetzung der Authentifizierung, Definition von Zugriffsbeschränkungen, Nachverfolgen der Verwendung von Zugangsdaten
Daten	■	■	Verhindern von Datenverlust, Definition und Durchsetzung, wer Zugriff auf welche Daten hat, sowie gleichzeitige Einhaltung von Compliance-Richtlinien
Anwendungen	■	■	Schutz vor einer Kompromittierung von Anwendungen durch Richtlinien, Patches und Sicherheitsmaßnahmen
Netzwerkkontrollen	■	◪	Nachverfolgung und Durchsetzung von Netzwerk-Zugriffsgenehmigungen
Host-Infrastruktur	■	◪	Verwaltung und Sicherheit von Betriebssystemen, Speicherlösungen und zugehörigen Systemen, um ungepatchte Schwachstellen und Rechteausweitungen zu verhindern
Physische Sicherheit	■	■	Beschränkung des physischen Zugriffs auf Systeme sowie redundante Auslegung, um einen einzelnen Ausfallpunkt (Single Point of Failure) zu verhindern

■ Kunde ■ Plattform-Anbieter

Abb. 1 Von Sophos zusammengefasste Darstellung des Shared-Responsibility-Modells. Versionen für die einzelnen Cloud-Anbieter finden Sie unter www.sophos.de/public-cloud.

Schritt 2: Planen Sie mehrere Clouds ein

Ein sogenannter Multi-Cloud-Ansatz ist heute nicht mehr bloß eine Option, sondern schlichtweg notwendig. Die Nutzung mehrerer Clouds ist aus vielen Gründen sinnvoll, z. B. im Hinblick auf Verfügbarkeit, mehr Agilität oder Funktionalität. Gehen Sie bei der Planung Ihrer Sicherheitsstrategie davon aus, dass Sie mehrere Clouds nutzen werden – wenn nicht jetzt, dann irgendwann in der Zukunft. So machen Sie Ihre Strategie zukunftssicher.

Überlegen Sie, wie Sie Sicherheit, Monitoring und Compliance für verschiedene Cloud-Anbieter in separaten Systemen und Konsolen verwalten wollen. Je einfacher die Verwaltung, desto schneller und besser können Sie auf Vorfälle reagieren, Bedrohungen erkennen und Compliance-Audits reibungslos über die Bühne bringen. So binden Sie auch wertvolle Mitarbeiter längerfristig, da eine komfortable Verantwortung für zufriedenes Personal sorgt.

Präferieren Sie agentenlose Lösungen, mit denen Sie die Umgebungen mehrerer Cloud-Anbieter in einer zentralen SaaA-Konsole kontrollieren können. So benötigen Sie weniger Tools, Zeit und Personal zur Verwaltung der Sicherheit mehrerer Cloud-Accounts und Regionen.

Schritt 3: Schaffen Sie Transparenz

Was Sie nicht sehen können, können Sie nicht schützen. Deshalb ist es für Ihre Sicherheit so wichtig, maximale Transparenz über Ihre gesamte Infrastruktur zu haben.

Nutzen Sie Tools, die die Netzwerktopologie und den Datenverkehr in Echtzeit abbilden und Ihr gesamtes Inventory aufschlüsseln, einschließlich Hosts, Netzwerken, Benutzerkonten, Speicherdiensten, Containern und serverlosen Funktionen.

Suchen Sie für maximale Transparenz nach Tools, die in der Lage sind, potenzielle Schwachstellen innerhalb Ihrer Architektur zu erkennen, damit Sie diese bereits vor einer Ausnutzung beseitigen können. Potenzielle Risikobereiche:

- Datenbanken mit offenen Ports zum öffentlichen Internet, über die sich Angreifer Zugriff verschaffen könnten
- Public Amazon S3 Simple Storage Services
- Verdächtige Benutzeranmeldungen und API-Aufrufe – z. B. mehrere Anmeldungen gleichzeitig am selben Konto oder Anmeldungen eines Nutzers aus unterschiedlichen Teilen der Welt am selben Tag

Schritt 4: Integrieren Sie Compliance in tägliche Abläufe

Bei einer Migration von Workloads in die Cloud müssen Sie Compliance-Vorschriften in einem weiter verteilten Netzwerk erfüllen, oft mit regelmäßigen Entwicklungs-Releases. Um die Compliance sicherzustellen, müssen Sie präzise Reports über Assets und Netzwerkdiagramme Ihres Cloud Footprint erstellen und dafür sorgen, dass die Kriterien Ihrer Compliance-Checkliste in einer dynamischen Umgebung erfüllt werden.

Um Audit-Fristen einzuhalten, ziehen viele Unternehmen als kurzfristige Lösung Ressourcen von rentablen Geschäftsprojekten ab. Dies ist jedoch keine Dauerlösung, da tägliche Snapshots schnell überholt sind und keine kontinuierliche Compliance-Prüfung erfolgt, die jedoch für Standards und Verordnungen wie ISO 27001, HIPAA und die DSGVO erforderlich ist.

Suchen Sie nach Lösungen, mit denen Sie die Compliance-Standards erhöhen können, ohne mehr Personal einstellen zu müssen. Die Lösungen sollten Ihnen Echtzeit-Snapshots Ihrer Netzwerktopologie liefern und Änderungen an Ihren Cloud-Umgebungen automatisch in Echtzeit erkennen. Achten Sie außerdem darauf, dass sich Richtlinien auf die spezifischen Anforderungen Ihrer Branche anpassen lassen.

Natürlich ist Reporting nur ein Compliance-Aspekt unter vielen. Sie müssen auch in der Lage sein, bei Compliance-Problemen entsprechend zu reagieren. Leider mangelt es oft an geeigneten Kollaborationskanälen, sodass sich eine Zusammenarbeit der zuständigen Mitarbeiter in Operations, Entwicklung und Compliance nur schwer realisieren lässt.

Um die Reaktion bei Compliance-Problemen reibungslos zu gestalten, sollten Sie sich für Lösungen entscheiden, die sich in Ihre bestehende Ticketing-Lösung integrieren lassen. Dazu gehören auch Warnmeldungen, auf deren Basis Problemfälle erstellt, zugewiesen und bis zur Erledigung nachverfolgt werden können. So gehen wichtige Aufgaben nie verloren, selbst während eines Release.

Schritt 5: Automatisieren Sie Ihre Sicherheitskontrollen

Die Möglichkeit, Prozesse zu automatisieren, ist einer der großen Vorteile von DevOps. Aber genau wie Ihre Teams gerne die Bereitstellung von Infrastrukturvorlagen und -skripten automatisieren und dadurch Stunden an Entwicklungszeit einsparen, sollten auch Sie überlegen, welche Sicherheitskontrollen Sie automatisieren können.

Im kollaborativen Framework von DevOps ist Sicherheit eine gemeinsame, durchgängig integrierte Verantwortung. Diese Denkweise führte zur Prägung des Begriffs „DevSecOps“: Er betont die Notwendigkeit, starke Sicherheitsgrundlagen in DevOps-Initiativen zu integrieren.

Das Bedürfnis nach automatisierter Sicherheit liegt auf der Hand, denn auch die Cyberkriminellen setzen bei ihren Angriffen zunehmend auf Automatisierung: Mit gestohlenen Benutzer-Anmeldeinformationen automatisieren sie beispielsweise die Bereitstellung von Instanzen für Aktivitäten wie Cryptojacking, das Ändern von Kontoeinstellungen oder die Sperrung legitimer Benutzer, um unerkannt zu bleiben. Das Ausspionieren von Cloud-Umgebungen nach Passwort-Schwachstellen, Sicherheitsgruppen-Einstellungen und Code gehört mittlerweile zum Alltag.

Es gibt zwei Hauptgründe, warum Angriffe auf Public-Cloud-Umgebungen gelingen: Die Architektur ist nicht sicher konfiguriert und die Reaktion auf Bedrohungen hinkt den Angreifern hinterher. Um diese Probleme in den Griff zu bekommen, ist eine Automatisierung von Sicherheitskontrollen entscheidend.

Eine Lösung zum Schutz Ihrer Public-Cloud-Umgebungen sollte Folgendes können:

- **Automatische Behebung von Schwachstellen in der Benutzer- und Ressourcen-Konfiguration**, unabhängig von Quelle oder Port
- **Erkennen verdächtiger Konsole-Anmeldungen und API-Aufrufe**, die darauf schließen lassen, dass ein Angreifer geteilte oder gestohlene Anmeldeinformationen nutzt
- **Melden von Auffälligkeiten im ausgehenden Datenverkehr**, um Ihr Unternehmen vor Aktivitäten wie Cryptojacking oder der Exfiltration von Daten zu warnen
- **Aufdecken verborgener Anwendungs-Workloads** vom Verhalten der Host-Computer-Instanz, um versteckte Schwachpunkte aufzuzeigen (z. B. Datenbanken)

Schritt 6: Schützen Sie ALLE Umgebungen (auch Entwicklung und QA)

Liest man Schlagzeilen über Datenpannen in einer Public Cloud, so ist in der Regel die Produktionsumgebung eines Unternehmens betroffen. Für Aktivitäten wie Cryptojacking nehmen sich Angreifer aber genauso gerne die Rechenleistung Ihrer Entwicklungs- oder QA-Umgebung vor.

Sie benötigen eine Lösung, die alle Ihre Umgebungen (Produktion, Entwicklung und QA) schützen kann, und zwar reaktiv und proaktiv. Die Lösung sollte in der Lage sein, Ihre Aktivitätsprotokolle (z. B. VPC-Flow- und CloudTrail-Protokolle) zu erfassen, um bereits aufgetretene Probleme zu identifizieren, beispielsweise wenn ein unerwünschter Port in der Firewall geöffnet ist. Gleichzeitig sollte die Lösung in der Lage sein, Infrastructure-as-Code-(IaC-)Vorlagen aus Ihren Repositories wie GitHub proaktiv zu scannen, und sie sollte sich in Ihre CI/CD Pipeline Tools wie Jenkins integrieren lassen. So können Schwachstellen im Code bereits frühzeitig erkannt werden – bevor sie auf Ihre Server gelangen und Sie damit in den Schlagzeilen landen.

Schritt 7: Setzen Sie auf Bewährtes

IT-Sicherheit für lokale Systeme ist das Ergebnis jahrzehntelanger Erfahrung und Forschung. Beim Schutz Ihrer cloudbasierten Server vor Infektionen und Datenverlusten sollten Sie also auf bewährte Verfahren zurückgreifen, die Sie bereits in Ihrer traditionellen Infrastruktur angewendet haben, und diese für die Cloud anpassen:

- Next-Gen Firewall: Sorgen Sie dafür, dass Bedrohungen gar nicht erst auf Ihre cloudbasierten Server gelangen können, indem Sie eine Web Application Firewall (WAF) an Ihrem Cloud Gateway installieren. Ziehen Sie auch ein IPS (zur Compliance-Unterstützung) und eine Kontrolle für ausgehende Inhalte in Betracht, um Ihre Server/VDI zu schützen.
- Server-Sicherheit: Installieren Sie auf Ihren cloudbasierten Servern effektive Cybersecurity, so wie auf Ihren physischen Servern.
- Endpoint-Sicherheit: Ihr Netzwerk haben Sie vielleicht in die Cloud migriert. Laptops und andere Geräte bleiben jedoch lokal, und eine Phishing-E-Mail oder Spyware reicht aus, um an Anmeldeinformationen für Ihre Cloud-Accounts zu gelangen. Sorgen Sie deshalb dafür, dass Endpoint- und E-Mail-Security auf Ihren Geräten auf dem neuesten Stand sind, damit sich niemand Zugriff auf Ihre Cloud-Accounts verschaffen kann.

Sophos Cloud Optix

Alles im Blick. Alles geschützt.

Transparenz ist das Fundament, auf dem alle Sicherheitsrichtlinien und Aktivitäten der Public Cloud aufbauen. Mit Sophos Cloud Optix lassen sich ganz einfach mehrere Cloud-Anbieter-Umgebungen überwachen, darunter Amazon-Web-Services-(AWS)-Konten, Microsoft-Azure-Subscriptions, Google-Cloud-Platform-(GCP)-Projekte, Kubernetes-Cluster und Entwicklungscode-Repositories. Durch diese Transparenz, mit Richtlinienkontrollen und Warnmeldungen für Compliance und DevSecOps, erhalten Teams die nötige Kontrolle und können ihre Cloud-Sicherheitsstrategie effektiv ausbauen.

Als agentenloser SaaS-basierter Service, der sich in die APIs nativer Public-Cloud-Anbieter integrieren lässt, bildet Cloud Optix automatisch die komplette Architektur ab: Sie erhalten eine vollständige Übersicht über Ihr gesamtes Inventory und eine Visualisierung der Netzwerktopologie in Echtzeit, einschließlich Hosts, Netzwerken, Benutzerkonten, Speicherdiensten, Containern und serverlosen Funktionen.

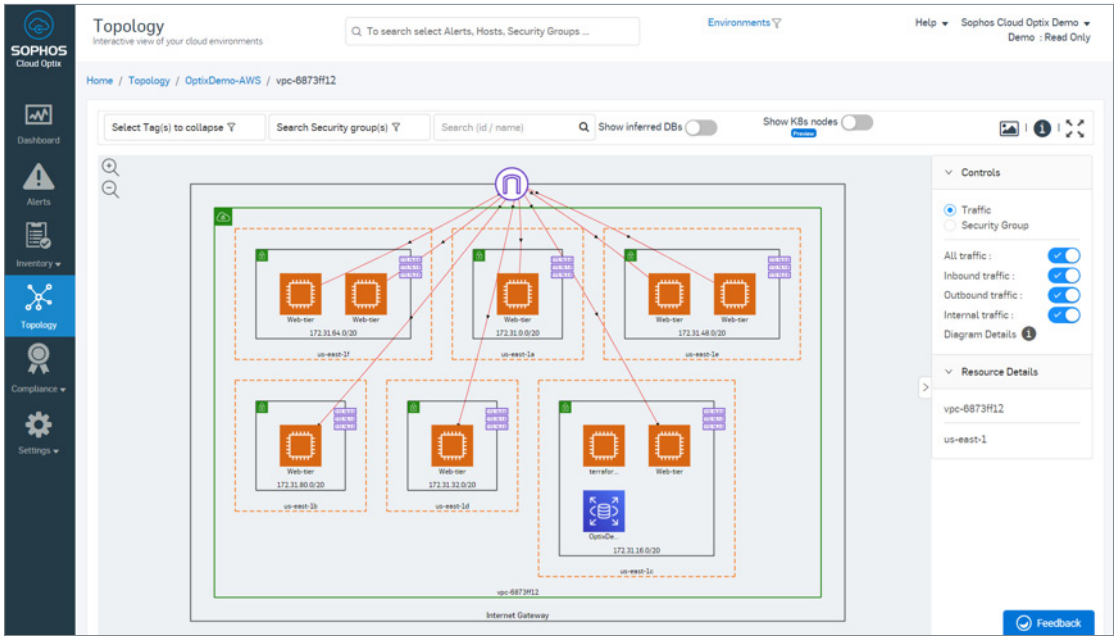

Abb. 2 Visualisierung der Netzwerktopologie in Sophos Cloud Optix mit eingehendem, ausgehendem und internem Datenverkehr in einer AWS-Umgebung

Mehr als einfache Konfigurationsprüfungen

Mittels Machine Learning und künstlicher Intelligenz spürt Cloud Optix Auffälligkeiten und Sicherheitslücken in Ihrer Plattform auf. Hierzu überwacht die Lösung u. a. den Netzwerkverkehr, Ressourcen-Konfigurationen, Benutzeranmeldungen und API-Aufrufe, den Compliance-Status sowie Infrastructure-as-Code (IaaC) Repositories und behebt automatisch versehentliche oder böswillige Änderungen in der Netzwerkkonfiguration.

Außerdem lässt sich mit Cloud Optix die Ursache von Sicherheits- und Compliance-Problemen einfach identifizieren – dank kontextueller Warnmeldungen mit Beschreibung des Problems, Schritten zur Behebung und betroffenen Ressourcen. So können Sie sich auf die wichtigsten Bereiche konzentrieren, in denen Sicherheitsupdates erforderlich sind.

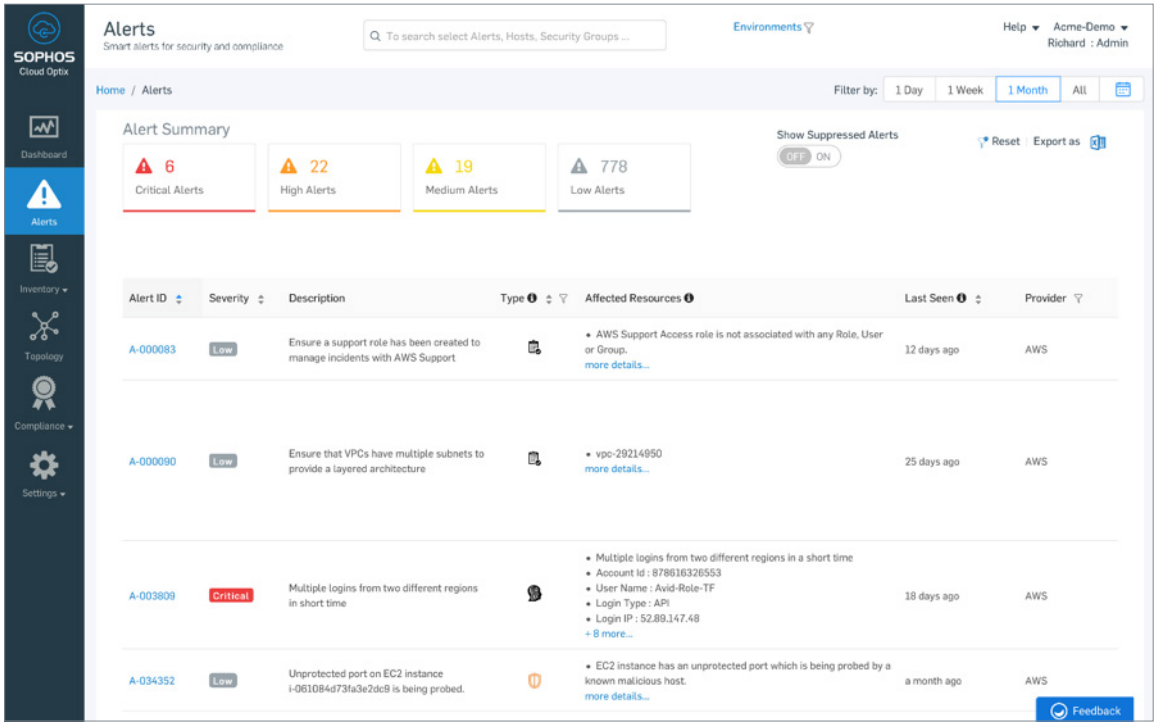

Abb. 3 Warnmeldungsübersicht von Sophos Cloud Optix mit kritischer Warnmeldung über mehrere gleichzeitige Account-Anmeldungen aus verschiedenen Regionen

Individuell anpassbar: Monitoring und Reaktion

Cloud Optix bietet eine Rest API und eine Integration mit Splunk, PagerDuty und Amazon GuardDuty, damit Sie Warnmeldungen in Echtzeit überall dort erhalten, wo Sie sie benötigen. Dank Integration in Jira und ServiceNow lassen sich Warnmeldungen sogar verwenden, um Tickets zu erstellen, die dann bis zur Erledigung der Aufgabe verfolgt werden können. So gehen wichtige Aufgaben nie verloren, selbst während eines Release.

In Kombination mit übersichtlichen Dashboards und On-Demand Reports sparen Sie Stunden oder sogar Tage bei der Verwaltung Ihrer Cloud Security und können die sieben wichtigsten Schritte für die Sicherheit der Public Cloud in die Tat umsetzen.

Mehr erfahren

Sophos Cloud Optix ist die optimale Lösung für Unternehmen, die bereits die Public Cloud nutzen oder eine Migration planen. Durch die leistungsstarke Kombination von künstlicher Intelligenz und Automatisierung erhält Ihr Unternehmen die kontinuierliche Transparenz, die zum Erkennen, Beseitigen und Vorbeugen von Sicherheits- und Compliance-Schwachstellen erforderlich ist.

Sie möchten Sophos Cloud Optix 30 Tage unverbindlich in Ihren eigenen Cloud-Umgebungen testen oder sofort in unserer Online-Demo-Umgebung kennenlernen? Mehr Infos unter www.sophos.de/cloud-optix.

Fazit

Die Umstellung von traditionellen auf cloudbasierte Workloads eröffnet Unternehmen jeder Größe enorme Chancen. Zur effektiven Abwehr von Cyberangriffen müssen Sie Ihre Public-Cloud-Umgebungen jedoch unbedingt hinreichend schützen. Wenn Sie die sieben Schritte in diesem Guide befolgen, können Sie Ihre Public Clouds effektiv schützen und gleichzeitig Ihre Verwaltung und Ihr Compliance Reporting vereinfachen.

Shared-Responsibility-Modell: Unterstützung durch Sophos

	Lokal	Public Cloud	Zweck	Wie Sophos Sie unterstützt
Benutzer	■	■	Durchsetzung der Authentifizierung, Definition von Zugriffsbeschränkungen, Nachverfolgen der Verwendung von Zugangsdaten	Die Sophos XG Firewall und Sophos UTM setzen eine ein-/ ausgehende Authentifizierung mit SSO und 2FA durch und bieten detaillierte Berichte über Zugriffe. Sophos Cloud Optix verfolgt die gemeinsame oder unbefugte Nutzung von Konto-Anmeldeinformationen.
Daten	■	■	Verhindern von Datenverlust, Definition und Durchsetzung, wer Zugriff auf welche Daten hat, sowie gleichzeitige Einhaltung von Compliance-Richtlinien	Sophos Cloud Optix bietet eine automatisierte Compliance, Governance und Sicherheitsüberwachung in der Cloud. Mit Sophos SafeGuard, DLP und Sophos Mobile können Sie Ihre Daten sichern und Zugriffsberechtigungen festlegen.
Anwendungen	■	■	Schutz vor einer Kompromittierung von Anwendungen durch Richtlinien, Patches und Sicherheitsmaßnahmen	Der IPS-Schutz der XG Firewall und der Sophos UTM sowie die in Server Protection enthaltene HIPS-Technologie und die Lockdown-Funktion schützen vor Angriffen auf Anwendungsebene und unbeabsichtigter Offenlegung von Anwendungen.
Netzwerkkontrollen	■	◪	Nachverfolgung und Durchsetzung von Netzwerk-Zugriffsgenehmigungen	Mit der bedienerfreundlichen Benutzeroberfläche der XG Firewall und der Sophos UTM, der leistungsstarken Packet Inspection und Synchronized Security (nur XG) sichern und verwalten Sie den Netzwerkzugriff und setzen Netzwerkberechtigungen durch.
Host-Infrastruktur	■	◪	Verwaltung und Sicherheit von Betriebssystemen, Speicherlösungen und zugehörigen Systemen, um ungepatchte Schwachstellen und Rechteausweitungen zu verhindern	Sophos Intercept X schützt durch Analyse von Exploit-Techniken vor Zero-Day-Bedrohungen. Sophos Server Protection Lockdown setzt Laufzeitbeschränkungen durch und Sophos XG Sandstorm stoppt die Ausbreitung von unbekanntem Code.
Physische Sicherheit	■	■	Beschränkung des physischen Zugriffs auf Systeme sowie redundante Auslegung, um einen einzelnen Ausfallpunkt (Single Point of Failure) zu verhindern	Sowohl die Sophos XG Firewall als auch Sophos UTM verfügen über High-Availability-Bereitstellungsoptionen für physische Appliances und Cloud-Plattformen.

■ Kunde ■ Plattform-Anbieter

Abb. 4. Wie Sophos mit dem Shared-Responsibility-Modell der Public Cloud hilft

„Mit Sophos Cloud Optix hat unser Team die von uns benötigte intelligente Transparenz über AWS-Umgebungen und den Compliance-Status von Konfigurationen immer in Echtzeit griffbereit. So behalten wir alle Vorgänge und Warnmeldungen in einer zentralen Ansicht im Blick, was vorher unmöglich war. Mit Sophos Cloud Optix erhalten wir einen umfassenden Überblick über Infrastruktur-Aktivitäten, sodass wir uns auf übergreifende Schutzmaßnahmen konzentrieren können."

Ryan Stinson
Manager of Security Engineering
HubSpot Inc.

1 RightScale 2019 State of the Cloud Report von Flexera

2 Automated attack data source: Exposed: Cyberattacks on Cloud Honeypots, Matt Boddy, Sophos, April 2019

Sophos Cloud Optix testen

www.sophos.de/cloud-optix

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

19-06-19 WP-DE (RP)

SOPHOS