Sicherheitsanalysen für Ihre Multicloud-Bereitstellungen

IBM Security QRadar SIEM-Lösung

Inhalte

01

Die Multicloud-Revolution gewinnt an Dynamik

Moderne Unternehmen brauchen intelligente Sicherheit

Die Hybrid-Multicloud-Nutzung verbreitet sich rapide. In der Folge werden Daten, Anwendungen und Workloads in zunehmendem Umfang in die Cloud verlagert. Während immer mehr Beschäftigte von zuhause arbeiten und die Interaktionen verstärkt online statt persönlich ablaufen, dürfte die Cloudnutzung auf neue Rekordwerte steigen.[1]

Laut Schätzungen von Gartner wird die Public-Cloud-Servicebranche bis 2022 ein exponentielles Wachstum aufweisen. Das am schnellsten wachsende Cloud-Marktsegment wird Infrastructure as a Service (IaaS) sein, dem Gartner bis 2022 einen Anstieg auf 76,6 Mrd. USD prognostiziert.[2]

Im Zentrum aller Cloudinitiativen muss die Sicherheit stehen. Cloudsicherheitsverletzungen in Unternehmen können in weniger als einer Stunde Kosten von 50.000 USD verursachen.[3] Unternehmen, die IaaS nutzen, müssen daher proaktiv ihr Betriebssystem absichern, die Netzkonfiguration verwalten und vor allem die in den Systemen befindlichen Daten schützen.

Zur sicheren Aufbewahrung von kritischen Geschäftsinformationen brauchen Sicherheitsanalysten lückenlosen Einblick in die gesamte IT-Infrastruktur – Netze, Anwendungen und Aktivitäten, die lokal und in der Cloud ausgeführt werden. Sie müssen imstande sein, Sicherheitsbedrohungen in Echtzeit zu erkennen, die Verwendung von nicht autorisierten Cloud-Services zu ermitteln und zu überprüfen, ob ihre Cloudkonten und -ressourcen ordnungsgemäß konfiguriert sind, um Sicherheit zu gewährleisten.

> 1 Milliarde abhanden gekommene Datensätze

Durch fehlerhafte Konfigurationen von Cloudumgebungen sind 2019 mehr als eine Milliarde Datensätze abhandengekommen.[3]

> 50.000 USD Verlust in weniger als einer Stunde

Cloudsicherheitsverletzungen in Unternehmen können in weniger als einer Stunde Kosten von 50.000 USD verursachen.[3]

02

Die Stärken der IBM Security QRadar-Lösungen nutzen

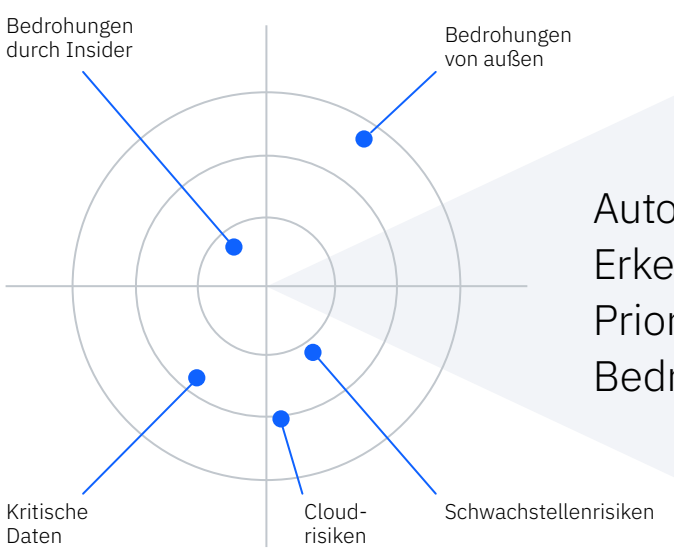
Gewinnen Sie übergreifende Einblicke in alle Cloud-Services

IBM Security QRadar ist eine moderne Security Information and Event Management-Lösung (SIEM), die sich nahtlos in zahlreiche Cloud-Services integrieren lässt, z. B. Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Salesforce.com, Microsoft Office 365, IBM Cloud und andere.

QRadar sammelt und normalisiert Sicherheitsinformationen aus cloudbasierten und lokalen Umgebungen und wendet erweiterte Analyseverfahren an, um automatisch Millionen von Ereignissen zu überprüfen. Die Lösung identifiziert kritische Sicherheitsrisiken und gibt bei potenziellen Vorfällen priorisierte aussagekräftige Alerts aus, um Hybrid-Multicloud- und On-Premises-Umgebungen zu schützen.

Darüber hinaus stellt die Lösung eine einheitliche Oberfläche bereit, auf der Sicherheitsanalysten kritische Bedrohungen sehen, die chronologische Ereigniskette zu jedem Alert überprüfen und einen unmittelbaren Überblick über potenzielle Angriffe gewinnen können. Leistungsstarke, sofort einsatzfähige Funktionen sorgen für eine schnelle Bereitstellung und flexible Skalierbarkeit in praktisch jeder unterstützten Umgebung.

Wie Sie mit der QRadar-Lösung auch Ihre Cloudumgebung schützen können →



Automatische Erkennung und Priorisierung von Bedrohungen

Die IBM Security QRadar SIEM-Lösung sammelt, analysiert und korreliert Daten aus den unterschiedlichsten Quellen zur Erkennung und Priorisierung von kritischen Sicherheitsbedrohungen, die eine Untersuchung erfordern.

03

Integration der QRadar-Lösung in Amazon Web Services (AWS)

Erhalten Sie Einblicke in AWS für ein höheres Sicherheitsniveau

Etwa 76 % der Unternehmen nutzen AWS in irgendeiner Weise.[1] Aufgrund des fortschreitenden Übergangs vom traditionellen On-Premises-Computing zum cloudbasierten Computing benötigen die Sicherheitsteams Einblick in ihre cloudbasierten Infrastrukturen, Anwendungen und Daten – wie es in einer On-Premises-Umgebung auch der Fall ist.

Aufdeckung von Risiken bei der Vertraulichkeit von Daten
Einige der umfangreichsten Integritäts-verletzungen in den letzten Jahren wurden nicht von böswilligen Angreifern verursacht. Vielmehr waren sie die Folge von versehentlichen Fehlkonfigurationen in Amazon S3-Buckets (Amazon Simple Storage Service), durch die vertrauliche Daten ungeschützt öffentlich zugänglich waren.

Mit der QRadar-Lösung können Sicherheitsteams ihre AWS-Umgebungen proaktiv scannen, entweder auf Ad-hoc-Basis oder im Rahmen eines regelmäßigen Scanprogramms, und somit aktiv nach fehlerhaften Konfigurationen suchen und bei Fehlern die Analysten alarmieren. Anhand dieser Alerts können die Sicherheitsteams dann schnell darauf reagieren, um Sicherheitslücken zu schließen und ihre Daten zu schützen.

Erkennung von Bedrohungen bei Clouddaten und Workloads
Je mehr vertrauliche Daten und geschäftskritische Assets in die Cloud verlagert werden, desto mehr wird AWS zum bevorzugten Ziel für Angreifer. Wenn die Integrität von AWS-Konten verletzt wird, sei es direkt durch Spear-Phishing oder infolge einer lateralen Ausbreitung, geraten AWS-Daten und -Workloads womöglich unter die Kontrolle eines Angreifers. Zur Verhinderung großer Schäden ist es wichtig, einheitliche, frühzeitige Warnungen vor Bedrohungen zu erhalten. Mit QRadar werden AWS-Sicherheitsdaten, z. B. von AWS CloudTrail, AWS CloudWatch und AWS Virtual Private Cloud (VPC) Flow-Protokollen, in einer zentralisierten Sicherheitsanalyselösung zusammengeführt, mit der die Security-Operations-Teams Bedrohungen von innen und außen in einer zentralen Managementkonsole überwachen und verfolgen können.

Die QRadar-Lösung erfasst Ereignisse aus Ihren Sicherheitsprodukten mithilfe einer Plug-in-Datei, einem sogenannten **Device Support Module.**

Über unterstützte Protokolle und Device Support Modules (DSMs) lässt sich QRadar für erweiterte Sicherheitsanalysen mit folgenden AWS-Komponenten verknüpfen:

AWS CloudTrail. Die QRadar-Integration bietet einen Überblick über die Benutzeraktivitäten durch Aufzeichnung der Aktionen auf Ihrem Konto. Sie unterstützt Prüfereignisse, die aus Amazon S3-Buckets sowie einer Protokollgruppe in den AWS CloudWatch-Protokollen erfasst werden.

AWS Security Hub. Ein integriertes System von Analysen und Abwehrmaßnahmen in Echtzeit bietet den Sicherheitsteams erweiterten Einblick in priorisierte Sicherheitsalerts und automatisierte Compliance-Prüfungen in einem zentralen Security Operation Center-Dashboard (SOC). Durch die Verknüpfung mit dem AWS Security Hub Amazon Findings Format (AFF) kann die QRadar-Lösung die Aggregation von Ereignissen aus verschiedenen AWS-Sicherheitsfunktionen, Instanzen sowie Sicherheitslösungen aus dem AWS Partner Network (APN) für tiefergehende Sicherheitsanalysen optimieren.

Amazon GuardDuty. Diese Integration ermöglicht den Benutzern die Analyse von kontinuierlich generierten Metadatenströmen aus ihrem Konto sowie von Netzaktivitäten, die in AWS CloudTrail-Ereignissen, Amazon VPC Flow-Protokollen und Domain Name Server-Protokollen (DNS) aufgezeichnet sind.

Amazon VPC-Flow-Protokolle. Mithilfe dieser Integration können Kunden Netzflussprotokolle sammeln, speichern und analysieren. Sie ermöglicht die Überwachung und Behebung von Konnektivitäts- und Sicherheitsproblemen, um die ordnungsgemäße Funktion der Netzzugriffsregeln sicherzustellen.

Amazon AWS Content Extension. Diese Inhaltserweiterung bietet neue Funktionen für das Ereignisdaten-Parsing in Ergänzung zu den in QRadar integrierten AWS-Funktionen und beschleunigt das Parsing von kritischen Ereignisdaten. Anhand sofort verfügbarer Daten wie Instanz-ID, Dateiname, Rollenname, Speichername usw. können die Benutzer Änderungen überwachen und Berichte zur relativen Sicherheit ihrer Cloudumgebungen erstellen.

IBM Security QRadar Cloud Visibility-App. Diese App stellt spezielle AWS-Dashboards und Erweiterungen wie die folgenden bereit:

- Vereinfachte Protokollquellenverwaltung
- Identity and Access Management (IAM) für Konten, Benutzer und IAM-Rollen
- Automatisches Füllen der QRadar-Netzhierarchie
- Amazon VPC Flow-Protokoll-Visualisierung
- Integration in AWS Security Hub und Amazon Detective

Welche Vorteile bietet die Überwachung der AWS-Umgebung mit QRadar?

- Zentralisierte Übersicht über Risiken und Bedrohungen in allen Cloudbereitstellungen
- Proaktive Suchoptionen für Sicherheitsanalysten für die Suche nach fehlerhaften Konfigurationen, die eine Intervention erfordern
- Vollständiger Überblick über die durchgängige Ereigniskette bei einem Vorfall durch Beseitigung von Silos
- Schnellere Identifizierung von Risiko-benutzern und Erkennung von Insider-Bedrohungen durch maschinelles Lernen

Weitere Informationen zur IBM Security QRadar Amazon AWS Content Extension →

04

Integration der QRadar-Lösung in Microsoft Azure

Verbessern Sie die Transparenz und verarbeiten Sie Ereignisse von Millionen Geräten

Die Nutzung von Microsoft Azure hat in den letzten Jahren stetig zugenommen. Inzwischen geben 61 % der Unternehmen an, dass sie diesen Service verwenden.[1] Wenn immer mehr Daten und Workloads auf Azure verlagert werden, müssen auch die Sicherheitsverfahren angepasst werden, um die Assets in dieser neuen Umgebung zu schützen. Die QRadar-Lösung bietet leistungsstarke, sofort einsatzfähige Funktionen zum Übertragen der Azure-Sicherheitsdaten in ein unternehmensweites Sicherheitsanalyseprogramm.

Über unterstützte Protokolle und DSMs lässt sich QRadar für erweiterte Sicherheitsanalysen mit folgenden Azure-Komponenten verknüpfen:

Azure-Aktivitätsprotokolle. Dieser native Azure-Ereignisaufzeichnungsservice erfasst große Mengen von Telemetriedaten and Ereignissen. Diese Daten können problemlos an die QRadar-Lösung gesendet werden, um den Sicherheitsteams aussagekräftigere Informationen über potenzielle Risiken und Bedrohungen in Azure-Umgebungen bereitzustellen.

Azure Active Directory. Die Integration von QRadar in Azure Active Directory bietet Sicherheitsteams die Möglichkeit, Identitäts-, Zugriffsmanagement- und Sicherheitsereignisse von externen Ressourcen wie Microsoft Office 365 und Microsoft Azure zu überwachen.

Microsoft Graph-Sicherheits-API. Über das QRadar Microsoft Graph-Sicherheits-API-Protokoll können Unternehmen Alerts von der Microsoft Graph-Sicherheits-API erfassen. Dies hilft Sicherheitsanalysten, Angriffe schnell zu untersuchen.

QRadar Cloud Visibility-App. Die QRadar-Lösung kann potenzielle Probleme in Azure-Umgebungen erkennen und vielfältige Sicherheitsanwendungsfälle bewältigen. Werden Verstöße festgestellt, hilft die QRadar Cloud Visibility-App den Benutzern, auf diese Verstöße im Azure Offense Overview Dashboard zu reagieren.

In diesem Dashboard werden Daten zu aktiven Verstößen in folgenden Diagrammen angezeigt:

- All users by magnitude
- All users by related rule
- Most severe offenses
- Al users by number of offenses
- Magnitude level indicator

IBM Security QRadar Content Extension for Azure. Die QRadar Content Extension for Azure erweitert die bestehenden QRadar-Funktionen für das Ereignisdaten-Parsing um neue Regeln, Berichte und gespeicherte Suchen für Azure-Bereitstellungen.

Diese Inhaltserweiterung ist speziell für das Netzsicherheitsmanagement, die Änderung von Sicherheitsregeln und das virtuelle Netzmanagement konzipiert.

Welche Vorteile bietet die Sicherung und Überwachung der Azure-Umgebung mit QRadar?

- Erkennung abnormaler Verhaltensmuster in der gesamten IT-Infrastruktur mithilfe von Sicherheitsregeln
- Überwachung und Diagnose des Netzverkehrs durch Azure-Netzsicherheitsgruppen
- Effizienteres Management von virtuellen Netzen
- Erfassen von Ereignisprotokoll- und Netzfluss-Sicherheitsdaten in lokalen Netzgateways
- Überwachung der Leistung und Nutzung von Webanwendungen auf Azure.

Weitere Informationen zur QRadar Content Extension for Azure →

05

Integration der QRadar-Lösung in die Google Cloud Platform

Erkennen Sie Anomalien und Bedrohungen in Echtzeit

Die Google Cloud Platform ist eine der führenden Cloudlösungen mit einer wachsenden Benutzerbasis von derzeit 35 %.[1] Die Lösung stellt eine Suite von Cloud-Services auf Basis der Google-Infrastruktur bereit. Die IBM Security QRadar-Lösung umfasst eine erweiterte, integrative Verknüpfung mit der Google Cloud Platform. Sie schafft einen zentralen Überblick, indem sie umgebungsübergreifend Hunderte Daten von Workloads sammelt, durchsucht und analysiert. Dadurch können Ihre Sicherheitsteams Bedrohungen besser erkennen und beantworten, unabhängig davon, wo sie auftreten.

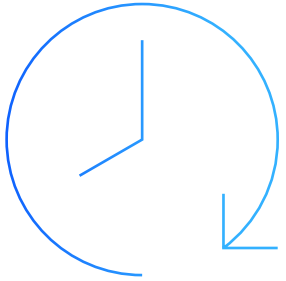
Über unterstützte Protokolle und DSMs lässt sich QRadar für erweiterte Sicherheitsanalysen mit folgenden Google Cloud Platform-Services verknüpfen:

Google G Suite-Aktivitätenberichte. Die QRadar-Lösung bietet Einblick in Prüfaktivitätenereignisse, die innerhalb der Google G Suite-Plattform generiert werden, z. B. Anmeldung, Benutzerkonto, Google Drive und Google Admin.

Damit kann Ihr Sicherheitsteam Erkenntnisse zu folgenden Anwendungsfällen gewinnen:

- Konto inaktiviert aufgrund verdächtiger Aktivitäten
- Benutzerdaten heruntergeladen als CSV-Datei (durch Kommas getrennte Werte)
- Administratorberechtigung vom Benutzer widerrufen
- Akteur hat geheime Frage oder Antwort zur Kontowiederherstellung geändert
- Akteur hat gemeinsame Nutzungs-berechtigungen eines Benutzers geändert
- Akteur hat ein Element vom Quellenordner zum Zielordner verschoben
- Benutzer wurde vorläufig gesperrt

Google Cloud Pub/Sub-Protokoll. Mit dem QRadar-Protokoll für Google Cloud Pub/Sub erhalten die Benutzer bessere Einblicke in alle Prozesse, die eine Senke in Pub/Sub erstellen. Sicherheitsteams können somit reaktionsschneller handeln.



06

Einblicke in SaaS

Überwachen Sie Daten aus Ihren SaaS-Anwendungen mithilfe von QRadar DSMs

Viele Unternehmen nutzen bereits Software-as-a-Service-Anwendungen (SaaS), um agiler zu werden, Arbeitsabläufe zu beschleunigen und umsatzgenerierende Projekte zu unterstützen – und es werden ständig mehr. Nach Prognosen von Gartner werden diese servicebasierten Cloudlösungen bis 2022 einen Marktwert von 143,7 Milliarden USD erreichen.[2]

Die QRadar-Lösung hilft Unternehmen, einen Überblick über die SaaS-Anwendungsnutzung zu gewinnen, und versetzt Sicherheitsteams in die Lage, Bedrohungen effektiver zu erkennen und zu blockieren. Vordefinierte DSMs ermöglichen eine nahtlose Integration in andere Lösungen in Ihrer Umgebung. Alle DSMs werden vor der Implementierung vom IBM Security-Team getestet und validiert.

QRadar unterstützt Ihr Team effektiv bei der Überwachung von Daten aus Ihren SaaS-Anwendungen einschließlich Salesforce.com, Office 365, Box und anderen. Die Daten können in Ihr Sicherheitsanalyseprogramm übernommen werden, sodass Ihr Team einen breiten Überblick über mögliche Sicherheitsbedrohungen erhält und potenzielle Vorfälle im Zusammenhang mit Daten in diesen Lösungen erkennen kann. Dadurch können Ihre Sicherheitsanalysten böswillige Insiderangriffe frühzeitiger entdecken und Integritätsverletzungen an schutzwürdigen Daten verhindern, die in diesen Anwendungen und Services gespeichert sind.

Erfahren Sie mehr über DSMs, die von der QRadar-Lösung unterstützt werden →

QRadar unterstützt mithilfe von DSMs die Integration in die meisten gängigen SaaS- und IaaS-Services.

- Amazon CloudTrail
- Amazon CloudWatch
- Amazon VPC Flows
- Microsoft Azure Event Hubs
- Microsoft Office 365
- Box.com
- Netskope Active
- Cloudera Navigator
- CloudPassage Halo
- Skyhigh Networks
- OpenStack
- Cisco Cloud Web Security
- VMware
- Salesforce
- Okta
- Google Cloud Platform
- Red Hat® Ansible® Platform

07

Die richtigen Tools für Ihre Sicherheitsteams

Entdecken Sie die QRadar-Produktfamilie

Zusammenfassend lässt sich sagen, dass IBM Security QRadar-Lösungen Ihnen den Überblick verschaffen, den Sie für Ihre wachsenden Cloudumgebungen benötigen. Mit dieser Lösungsfamilie lassen sich isolierte Datensilos auf einer zentralen Plattform zusammenführen, um einen umfassenden Überblick zu erhalten, durchgängige Sicherheitsanalysen zu ermöglichen und eine lückenlose Bedrohungserkennung zu implementieren. Durch Erkennung von Unregelmäßigkeiten können Sie sich gegen innere und äußere Sicherheitsbedrohungen schützen, Sicherheitslücken identifizieren, die den Schutz vertraulicher Daten gefährden, und die Nutzung von nicht autorisierten Cloud-Services aufdecken.

In Kombination liefern diese Funktionalitäten ein umfassendes Bild der System-, Netz- und Benutzeraktivitäten in Ihrem Unternehmen und stellen intelligente Erkenntnisse zur proaktiven Bekämpfung von Risiken und Bedrohungen bereit.

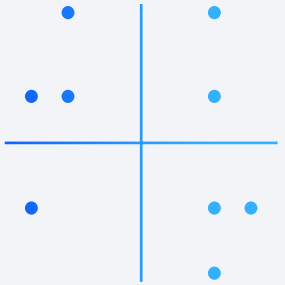
Die QRadar-Lösung sammelt und analysiert zentral Datenfeeds und Bedrohungserkenntnisse aus Quellen in verschiedenen Umgebungen, z. B. AWS, Azure, IBM Cloud, SaaS-Anwendungen, Private Clouds und herkömmliche On-Premises-Infrastrukturen. Sie haben die Wahl, ob Sie Hardware oder Software vor Ort einsetzen, virtuelle Maschinen in IaaS-Umgebungen bereitstellen oder QRadar als Cloud-Service von IBM nutzen.

Auf Ihrem weiteren Weg in die Multicloud-können Sie dieselben Funktionalitäten für Sicherheit, Überwachung und Analysen im gesamten Unternehmen verwenden.

Weitere Informationen →

IBM wurde im neuesten Gartner Magic Quadrant für Security Information and Event Management (SIEM) **zum 11. Mal in Folge als „Leader“ geführt.**

Bericht lesen →



08

Warum IBM Security-Lösungen?

IBM betreibt eine der weltweit größten Organisationen im Bereich der Forschung, Entwicklung und Bereitstellung von Sicherheitslösungen

IBM Security-Lösungen sind ein innovatives, hochgradig integriertes Portfolio von Produkten und Services rund um das Thema Unternehmenssicherheit. Unterstützt von der weltweit anerkannten IBM X-Force-Forschungs- und Entwicklungsgruppe, liefert dieses Portfolio sicherheitsrelevante Informationen, die Unternehmen helfen, ihre Infrastrukturen, Daten und Anwendungen ganzheitlich zu schützen. Das Portfolio umfasst Lösungen für Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzsicherheit und vieles mehr. Mit diesen Lösungen können Unternehmen ihr Risikomanagement wesentlich effektiver gestalten und integrierte Sicherheitsmechanismen für Mobile-, Cloud-, Social-Media- und sonstige Geschäftsarchitekturen implementieren.

Darüber hinaus bietet Ihnen IBM Global Financing zahlreiche interessante Zahlungsoptionen, damit Sie die Technologie anschaffen können, die Sie für weiteres Wachstum in Ihrem Unternehmen brauchen. IBM erbringt für Sie außerdem das komplette Lifecycle-Management für IT-Produkte und Services, von der Beschaffung bis zur Außerbetriebnahme. Weitere Informationen finden Sie unter ibm.com/financing.

Weitere Informationen

Wenn Sie mehr über die QRadar-Sicherheitsinformationslösung erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter: ibm.com/security/security-intelligence/qradar.

IBM überwacht täglich **Milliarden** von Sicherheitsereignissen in über **130 Ländern** und hält mehr als **3000 Sicherheitspatente.**

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

Die in diesem Dokument enthaltenen Informationen sind zum Datum der Erstveröffentlichung des Dokuments aktuell und können von IBM jederzeit geändert werden. Nicht alle Angebote sind in allen Ländern verfügbar, in denen IBM tätig ist.

Die Verantwortung für die Auswertung und Prüfung des Betriebs von Produkten oder Programmen anderer Anbieter mit IBM Produkten und Programmen liegt beim Benutzer. Die Informationen in diesem Dokument werden auf der Grundlage des gegenwärtigen Zustands (auf „as-is“-Basis) ohne jegliche ausdrückliche oder stillschweigende Gewährleistung zur Verfügung gestellt, einschließlich, aber nicht beschränkt auf die Gewährleistungen für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter. Für IBM Produkte gelten die Gewährleistungen, die in den Vereinbarungen vorgesehen sind, unter denen sie erworben werden.

Erklärung zu geeigneten Sicherheitsvorkehrungen: Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Prävention, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter schützen.

1 10 Key Takeaways from RightScale 2020 State Of The Cloud Report From Flexera, *Forbes*, 2. Mai 2020

2 Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, *Gartner*, 2. April 2019

3 Cloud Threat Landscape Report 2020, *IBM Security X-Force®* Incident Response and Intelligence Services, Mai 2020