Google Cloud-Whitepaper
Februar 2021

CISO-Leitfaden zur Cloud-Sicherheit

Google Cloud

Inhaltsverzeichnis

Inhaltsverzeichnis 1

Einleitung 2

Haftungsausschluss 2

Eine auf Cloud-Sicherheit abgestimmte Unternehmenskultur 3

Ein neuer Blick auf das Thema Sicherheit 4

Die Notwendigkeit einer Zero-Trust-Philosophie 4

Risikobewusstes Vorgehen 4

Ein Sicherheitsmodell, das mitwächst 5

Neue Arbeitsweisen für Ihr Unternehmen 6

Kürzere Zeitrahmen für die Entwicklung 6

Bereitstellung und Verwaltung von Infrastruktur als Code 6

Weiterentwicklung wichtiger Rollen und Zuständigkeiten in Sachen Sicherheit 7

Zusammenarbeit mit dem Cloud-Dienstanbieter 7

Veränderte Umsetzung von Sicherheitsrollen 8

Entwicklung eines Betriebsmodells für Sicherheit 10

Betriebsmodell „zentralisierte Sicherheit“ 10

Betriebsmodell „föderierte Sicherheit“ 11

Betriebsmodell „hybride Sicherheit“ 11

Bestimmung von Best Practices für Cloud-Sicherheit 13

Fazit 14

Einleitung

Dieses Whitepaper ist für Chief Information Security Officers (CISOs) bestimmt, die mit der Cloud mehr Sicherheit erreichen möchten, sowie für CISOs, die mit dem Wechsel des gesamten Unternehmens in die Cloud Schritt halten möchten.

Möglicherweise verfolgen Sie als CISO die Cloud-Sicherheitstransformation selbst aktiv oder Sie werden von anderen in Richtung Cloud bewegt. In jedem Fall sind Sie für den Schutz der Informationen des Unternehmens, seiner Partner und Kunden verantwortlich. Die Informationslandschaft wird immer komplexer und täglich treten neue Sicherheitsbedrohungen auf. Ihre Aufgabe, diese Informationen zu schützen und das Vertrauen im Unternehmen aufrecht zu halten, wird deshalb immer anspruchsvoller.

Angesichts dieser Herausforderungen setzen viele Unternehmen und CISOs in Sachen Sicherheit jetzt auf die Cloud. Cloud-Dienstanbieter können mehr in Mitarbeiter und Prozesse für sichere Infrastruktur und sichere Anwendungen investieren. Sie können Ihnen helfen, Ihre eigenen Sicherheitskonzepte zu rationalisieren und zu modernisieren und Ihre Daten einfach besser zu schützen.

Rationalisierung und Modernisierung der Sicherheit bedeutet in der Cloud mehr als nur den Austausch von Technologien und Sicherheitsimplementierungen. Sie bedeutet, dass das ganze Unternehmen anders denken und arbeiten muss.

Das kann für Cloud-Einsteiger abschreckend wirken. Aber Google nimmt in Sachen Cloud-Sicherheit schon seit Jahren eine führende Rolle ein und tut sich durch zahlreiche Innovationen hervor. Wir wissen, wie man eine digitale Transformation vorbereitet, wie man die Abläufe bei Cloud-Sicherheit effektiv und nachhaltig gestaltet und wie man mit Cloud-Sicherheitsanbietern zusammenarbeitet. In diesem Whitepaper erläutern wir die Sichtweise von Google auf Cloud-Sicherheit. Wir möchten Ihnen damit konkrete Maßnahmen zur Bewältigung der kulturellen, organisatorischen und betrieblichen Veränderungen an die Hand geben, die Ihnen dabei helfen, einen reibungslosen und erfolgreichen Übergang zu Cloud-Sicherheit zu erzielen.

Beim Verlagern Ihrer IT-Sicherheit in die Cloud sollten Sie daran denken, dass die Cloud nicht nur eine Ansammlung von Servern ist. Mit der Cloud ändert sich auch die Betrachtungsweise des ganzen eigenen Geschäfts und die eigene Arbeitsweise. Die Cloud ist eine neue und bessere Herangehensweise an das Thema Sicherheit.

Haftungsausschluss

Der Inhalt dieses Dokuments entspricht dem Stand von Februar 2021 und spiegelt den Status quo zum Zeitpunkt der Erstellung wider. Die Sicherheitsrichtlinien und -systeme von Google Cloud können sich in Zukunft ändern, da wir den Schutz unserer Kunden kontinuierlich verbessern.

Eine auf Cloud-Sicherheit abgestimmte Unternehmenskultur

Organisationen, die große Veränderungen jeder Art erfolgreich bewältigen, besitzen eine starke Kultur und starke Werte, an denen sie sich bei ihrer Transformation orientieren. Damit die digitale Transformation Ihr Unternehmen und Ihre Sicherheitsabläufe auf ein neues Level bringen kann, brauchen Sie im gesamten Unternehmen eine starke Sicherheitskultur.

Wie sieht eine starke Sicherheitskultur aus? Jedes Unternehmen ist anders, aber Unternehmen mit einer starken Sicherheitskultur legen normalerweise großen Wert auf folgende Punkte:

- **Eine Kultur, für die Sicherheit etwas Selbstverständliches ist:** Sicherheit ist kein Punkt, der erst im Nachhinein bedacht wird. Sie ist kein nettes Beiwerk und auch keine Funktion, die erst am Ende des Entwicklungszyklus hinzugefügt wird. Sicherheit ist vielmehr ein Aspekt, der bei jedem IT-Projekt von Anfang an zu berücksichtigen ist. Google verlangt beispielsweise in allen Entwicklungsphasen ein eine Überprüfung der Sicherheitsstandards, von den ersten Entwurfsdokumenten bis zur Markteinführung.

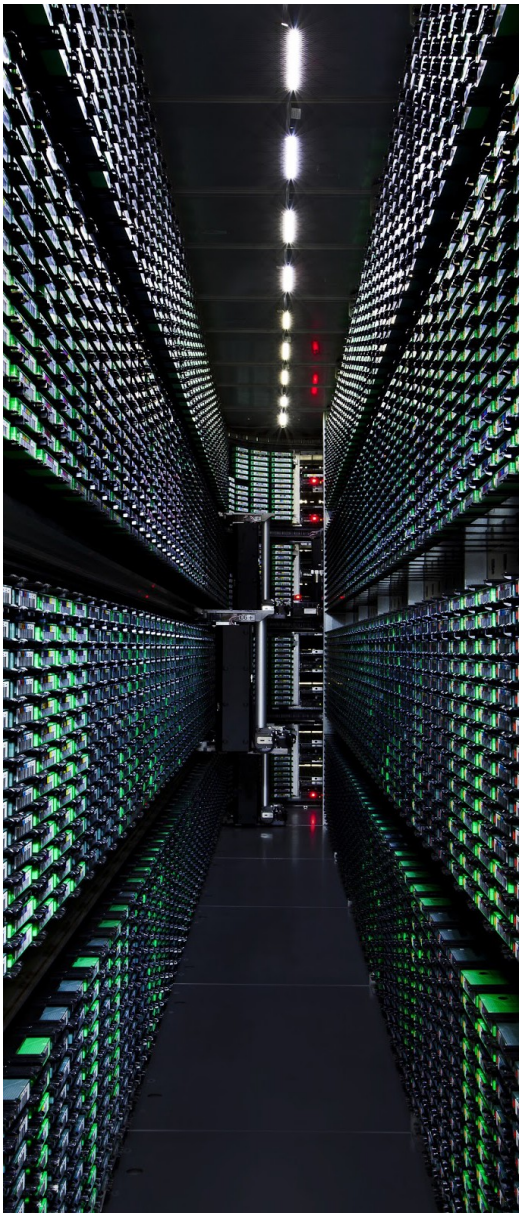
- **Eine Kultur der Verantwortung:** Sicherheit ist kein „Problem anderer Leute“ und auch keine Zusatzarbeit, die das Sicherheitsteam dem Entwicklungsteam aufbürdet. Alle sind mitverantwortlich für die Entwicklung sicherer Produkte und Funktionen.

- **Eine Kultur des Bewusstseins:** Schulung, Dokumentation und Informationsaustausch zum Thema Sicherheit sind im gesamten Unternehmen allgegenwärtig. Die Teammitglieder informieren sich gegenseitig ständig über Best Practices in puncto Sicherheit. Die Google-Sicherheitsteams führen zum Beispiel unternehmensweite und teamspezifische Sicherheitsschulungen durch.

- **Eine Kultur der Unvermeidlichkeit:** Sie sind auf das Schlimmste vorbereitet und bereit zu handeln, wenn der Fall eintritt. Ausfallszenarien sind etwas, mit dem man rechnet, und die Reaktionspläne werden umfassend diskutiert und sind allgemein bekannt. Bei Google hat die Simulation von Notfallszenarien lange Tradition. Wir bereiten uns damit auf genau diese Art unvermeidlicher Ereignisse vor.

- **Eine Kultur der Revision:** Offene, transparente und konstruktive Überprüfungen zu Code und Design sind im gesamten Unternehmen die Norm. Das Thema Sicherheit ist bei diesen Checks ein wichtiger Punkt.

- **Eine Kultur der Nachhaltigkeit:** Die Arbeit im IT-Bereich berücksichtigt das Tagesgeschäft und Verbesserungen für die Zukunft gleichermaßen.



Ein neuer Blick auf das Thema Sicherheit

Die Zusammenhänge im Bereich IT werden immer komplexer und täglich treten neue Bedrohungen und Schwachstellen auf. Als CISO müssen Sie sich in Sachen Sicherheit von Denkweisen der Vergangenheit lösen. Sie müssen moderne Bedrohungen genauso wie moderne Sicherheitslösungen kennen und verstehen, damit Sie Ihre Daten schützen können. Mit diesen modernen Lösungen auf der Grundlage datenorientierter Cloud-Sicherheitsmethoden können Sie Ihre Daten effizient schützen, Risiken wirksam entschärfen sowie die Dienste und Nutzerbasis Ihres Unternehmens schnell skalieren.

Die Notwendigkeit einer Zero-Trust-Philosophie

Traditionelle Sicherheitskonzepte drehen sich darum, einen Sicherheitsperimeter zu härten und Bedrohungen von diesem Bereich fernzuhalten. Dieses Perimetermodell kann dazu führen, dass zu wenig in die Konfiguration und den Schutz interner Anwendungen und Infrastrukturen investiert wird. Es entspricht nicht mehr der Realität moderner Sicherheitsbedrohungen. Cloud-Sicherheit bedeutet, wie eigentlich jedes moderne Sicherheitskonzept, anders zu denken, denn die Grenzen moderner IT-Landschaften sind nicht klar definiert und mit herkömmlichen Mitteln nicht leicht zu schützen.

Für ein erfolgreiches Cloud-Sicherheitskonzept müssen Sie das Perimetermodell ad acta legen und stattdessen eine *Zero-Trust-Philosophie* einführen, also „Null Vertrauen“ gegenüber allem und jedem. Zero Trust bedeutet, dass Sie Daten und Transaktionen nicht schon deshalb vertrauen, weil diese den Sicherheitsperimeter passiert haben. Vielmehr werden alle Daten und alle Vorgänge außerhalb und innerhalb Ihres Systems überprüft. Die ständige automatisierte Überprüfung schützt Ihre Daten besser vor modernen Bedrohungen und ermöglicht die Entwicklung von Informationssystemen ohne die Beschränkungen eines unflexiblen Perimeters.

Risikobewusstes Vorgehen

Cloud-Sicherheit führt auch zu einem anderen Risikobewusstsein. Bei traditionellen Sicherheitskonzepten geht es oft darum, Risiken zu vermeiden und Bedrohungen vorsichtig zu umgehen, insbesondere solche, die die vorhandene Sicherheitsinfrastruktur nicht abwehren kann. Im heutigen Sicherheitsumfeld treten jedoch ständig neue Bedrohungen auf, die Angriffsfläche wird immer größer und vielen Bedrohungen kann man gar nicht mehr aus dem Weg gehen.

Bei Cloud-Sicherheit nimmt man zur Kenntnis, dass diese Bedrohungen unvermeidlich sind und geht daher beim Schutz der Daten *risikobewusst* vor. Grundlage eines risikobewussten Sicherheitskonzepts sind Analyse und Bewertung von Risiken und der anschließende bewusste Umgang mit diesen Risiken. So könnten Sie beispielsweise eine „Risikotaxonomie“ entwickeln, also eine Art Systematik der größten Risiken für Sie und Ihr Unternehmen. Danach ordnen Sie alle Risiken in der Taxonomie den Kontrollen zu, mit denen Sie diese Risiken entschärfen. Mit diesem risikobewussten Vorgehen packen Sie gezielt die wichtigsten Sicherheitsrisiken an, anstatt sich mit Risiken zu befassen, von denen Sie bereits wissen, wie sie abzuwehren sind.

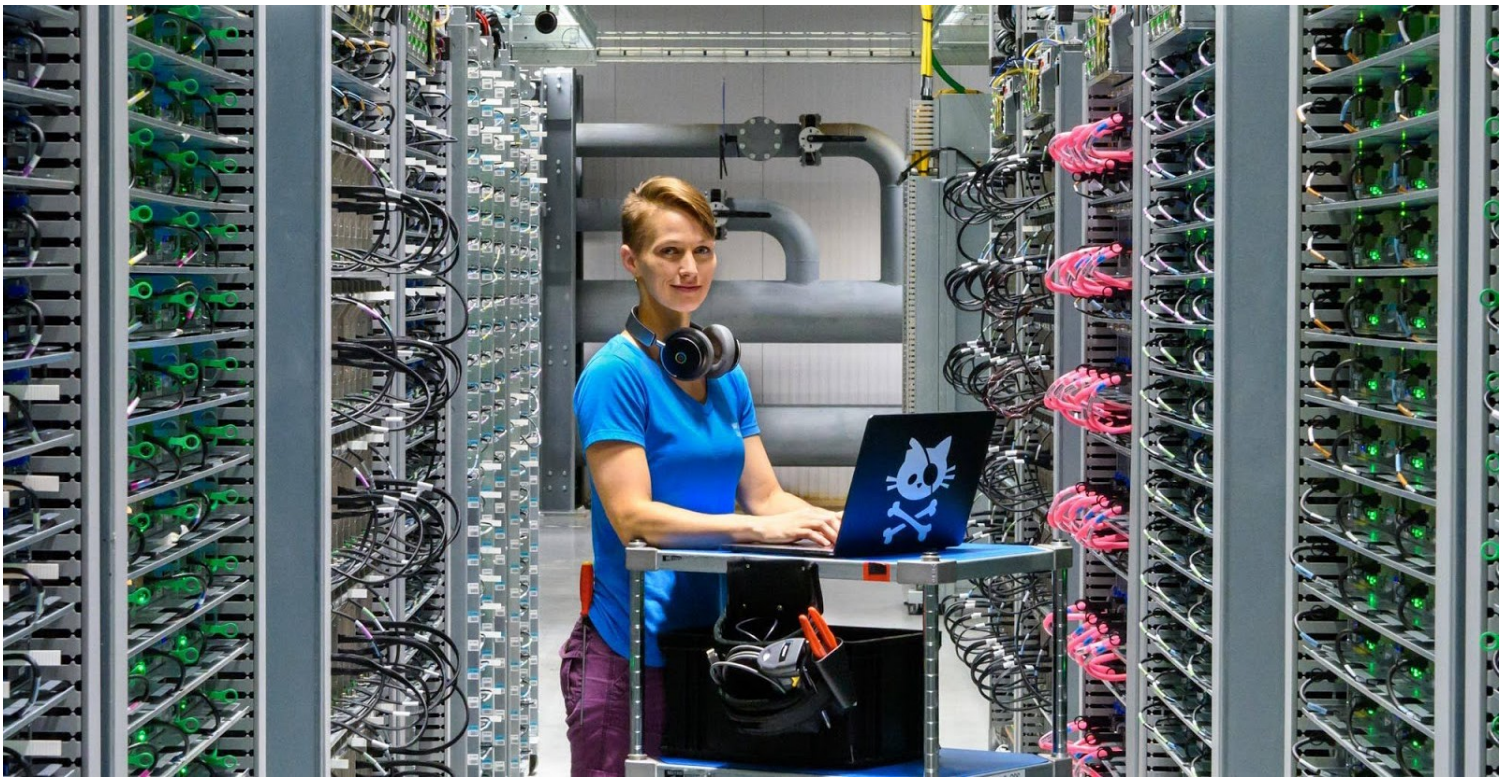
Cloud-Dienstanbieter machen Ihnen dieses risikobewusste Vorgehen leichter, denn sie entwickeln und pflegen viele Kontrollmechanismen und Tools, die Sie zur Eindämmung moderner Sicherheitsbedrohungen brauchen. So unterstützen Cloud-Dienstanbieter beispielsweise wichtige Schlüsselsicherheitsfunktionen wie Zugriffs- und Firewall-Logs, deren Entwicklung in einer lokalen Umgebung schwierig und teuer sein kann. Cloud-Dienstanbieter bringen ihre robusten Sicherheitsprozesse für Authentifizierungs- und Autorisierungsschlüssel außerdem ständig auf den neuesten Stand.

Bedenken Sie zudem, dass die Cloud bestimmte Eigenschaften besitzt, durch die Sie mit dem Thema Sicherheit und anderen mit der Cloud verbundenen Risiken anders und besser umgehen können. Eine sauber durchgeführte Migration in die Cloud kann deshalb insgesamt zu weniger Risiken bei Sicherheit, Technologie und anderen operativen Bereichen führen[1].

Ein mitwachsendes Sicherheitsmodell

Traditionelle Sicherheitskonzepte können die Skalierungsmöglichkeiten der Systeme begrenzen, die sie schützen sollen. Schließlich sind kleinere und einfachere Systeme auch weniger Bedrohungen und Risiken ausgesetzt, oder? Mit der skalierbaren und datenorientierten Cloud-Sicherheit können Sie sich jedoch von diesen Annahmen lösen und Ihre Systeme auf Millionen von Nutzern und Petabytes an sicheren Daten hochskalieren. Mit sicheren Diensten von Cloud-Dienstanbietern können Sie beispielsweise die Identitäts- und Zugriffsverwaltung (IAM) auf gewaltige Ausmaße ausdehnen.

Traditionelle Sicherheitskonzepte können auch den Umfang selbst entwickelter Sicherheitskontrollen einschränken oder verzerren. So beruht eine herkömmliche Sicherheitsinfrastruktur vielleicht etwa auf unvollständigen oder ungenauen Datenbanken über IT-Assets, stützt sich in großem Umfang auf manuelle Überprüfungen (was dazu führt, dass Sicherheitsmodelle sich an Stichproben orientieren und keine vollständige Sicherheitsabdeckung bieten) oder geht von einer kleinen und relativ statischen IT-Struktur aus. Mit ihrem datenorientierten Konzept kann Cloud-Sicherheit eine wesentlich breitere Sicherheitsabdeckung und größere Flexibilität beim Schutz aller relevanten Assets bieten.



[1] Stärkung der Betriebsstabilität im Bereich Finanzdienstleistungen durch die Migration zu Google Cloud

Neue Arbeitsweisen für Ihr Unternehmen

Wenn ein Unternehmen in die Cloud wechselt, ändert sich die Arbeitsweise des gesamten Unternehmens, nicht nur des Sicherheitsteams. Als CISO müssen Sie sich mit diesen neuen Arbeitsweisen vertraut machen. Nur so können Sie gemeinsam mit Ihren Partnern und dem ganzen Unternehmen im neuen, veränderten Geschäftsumfeld für Informationssicherheit sorgen.

Kürzere Zeitrahmen für die Entwicklung

Entwicklung und Deployment in der Cloud können die Abstände zwischen einzelnen Releases erheblich verkürzen. Oft entsteht so ein kontinuierlicher, iterativer Releasezyklus. Mit der Umstellung auf diesen Entwicklungsprozess - oftmals Agile, DevOps oder auch anders genannt - können Sie auch Entwicklung und Release neuer Sicherheitsfunktionen beschleunigen.

Um diese Chance einer beschleunigten Entwicklungsumgebung erfolgreich zu nutzen, müssen Sicherheitsteams den neuen Releaseprozess und die zeitlichen Abläufe kennen oder sogar selbst steuern, eng mit Entwicklungsteams zusammenarbeiten und bei der Entwicklung in puncto Sicherheit iterativ vorgehen. Diese Vorgaben stehen für eine deutliche Abkehr von der Rolle der Sicherheitsteams im traditionellen Softwareentwicklungszyklus. Die Umsetzung dieser Änderungen kann jedoch hinsichtlich der Sicherheitsentwicklung und der schnellen Bereitstellung neuer Sicherheitsfunktionen und -korrekturen enorme Vorteile bringen.

Bereitstellung und Verwaltung von Infrastruktur als Code

Die Transformation hin zur Cloud führt dazu, dass Unternehmen anders über Infrastruktur denken, sie anders bereitstellen und verwalten. Wenn Server, Schränke und Rechenzentren in der Cloud für Sie verwaltet werden, wird der Code zur Infrastruktur.

Wenn Sie Infrastruktur als Code bereitstellen, können Sie Sicherheitsrichtlinien direkt in den Code integrieren. So stellen Sie die Sicherheit in den Mittelpunkt des Entwicklungsprozesses in Ihrem Unternehmen und auch jeder von Ihrem Unternehmen entwickelten Software. Sicherheitsrisiken werden dadurch minimiert. Gehen wir einmal davon aus, dass Ihr Unternehmen Hunderte oder Tausende von Sicherheitsrichtlinien verwalten muss. Für viele dieser Richtlinien müssen Sie vermutlich anhand von Playbooks arbeiten und Menschen müssen manuell in Sicherheitsinfrastruktur und an entsprechenden Konsolen eingreifen. Traditionelle Sicherheitsmethoden sind bei der Verwaltung und Aktualisierung von Sicherheitsrichtlinien oft arbeitsintensiv und fehleranfällig.

Bei der Bereitstellung und Verwaltung dieser Sicherheitsrichtlinien in Form von Code können Sie menschliche Fehler hingegen minimieren, Inkonsistenzen und Richtlinienverstöße verringern und eine ordnungsgemäße Prüfung von Updates vor dem Deployment gewährleisten. Mit verwalteten Skripts beispielsweise lassen sich Sicherheitsrichtlinien auf vorhersehbare und testbare Weise bereitstellen und aktualisieren, während menschliche Eingriffe oft uneinheitlich sind. Mit ausgereiften Prozessen für das Veränderungsmanagement, die für die Softwareentwicklung aufgebaut wurden, können Sie sensible Aspekte der Sicherheitsinfrastruktur vor dem Deployment einem Peer Review unterziehen und gewährleisten, dass die Sicherheitsinfrastruktur mit der Software des Unternehmens im Einklang bleibt.

Weiterentwicklung wichtiger Rollen und Zuständigkeiten in Sachen Sicherheit

Die Umstellung auf die Cloud verändert auch die Arbeitsweise der Sicherheitsorganisation. Manuelle Sicherheitsarbeiten werden automatisiert. Es gibt neue Rollen und Zuständigkeiten und Sicherheitsexperten arbeiten enger mit Entwicklungsteams zusammen. Ihre Organisation bekommt außerdem einen neuen Partner: Ihren Cloud-Dienstanbieter. Wie bei jeder organisatorischen Veränderung müssen Sie als Führungskraft diese Veränderungen klar kommunizieren und das Team dabei unterstützen, sich möglichst reibungslos auf die neue Arbeitsweise einzustellen.

Zusammenarbeit mit dem Cloud-Dienstanbieter

Die Partnerschaft mit Ihrem Cloud-Dienstanbieter ist tatsächlich einer der größten Vorteile der Umstellung auf die Cloud. Der Cloud-Dienstanbieter entwickelt nicht nur Tools für Sicherheit und Monitoring und erstellt Dokumentationen zu Best Practices für die Cloud. Er übernimmt auch viele wichtige Sicherheitsaufgaben für Ihr Unternehmen.

Beim Modell der gemeinsamen Verantwortung in der Cloud sind die Zuständigkeiten so verteilt:

- Der Cloud-Dienstanbieter ist für die **Sicherheit der Cloud** zuständig, also für den Schutz der Cloud-Infrastruktur einschließlich Hardware und Netzwerken.
- Sie sind für die **Sicherheit in der Cloud** zuständig, also für den Schutz Ihrer Daten und die Auswahl des Sicherheitsmodells.

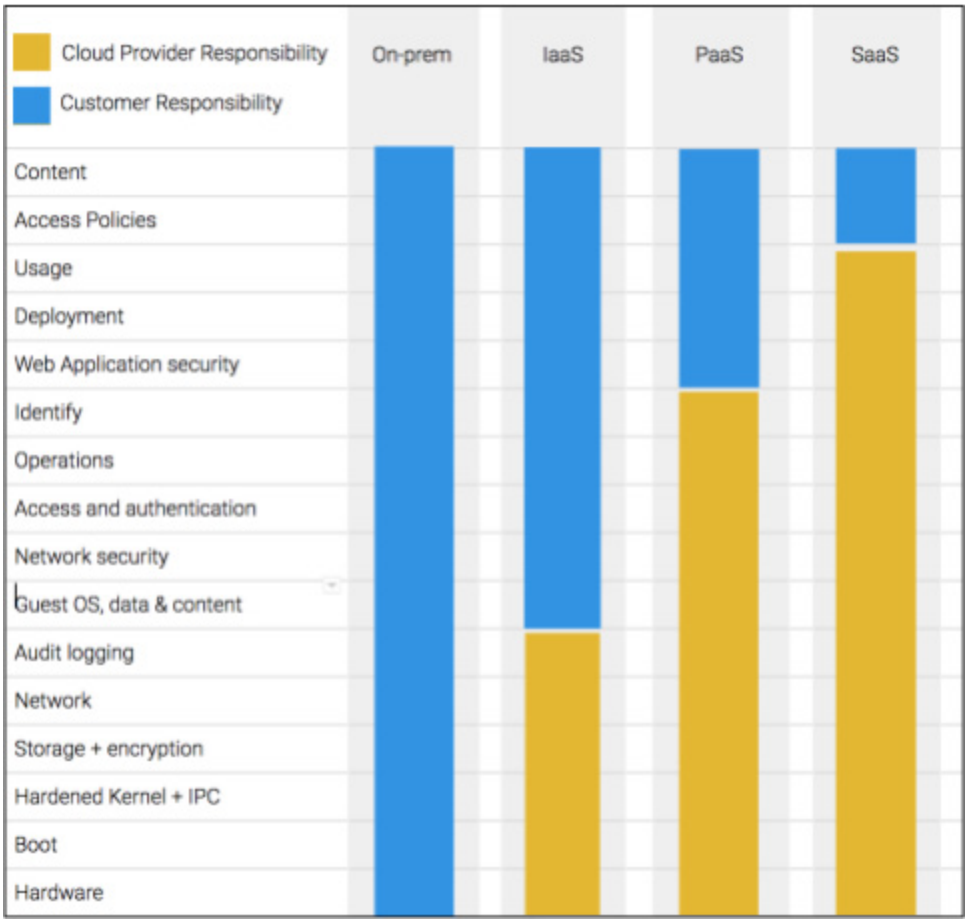


Abbildung 1: Die Verteilung der Sicherheitsverantwortung zwischen Ihnen und Ihrem Cloud-Dienstanbieter im Rahmen des Modells der gemeinsamen Verantwortung in der Cloud.

Wie in Abbildung 1 dargestellt, hängen viele Zuständigkeiten davon ab, ob Ihre Architektur als Infrastructure as a Service (IaaS), Platform as a Service (PaaS) oder Software as a Service (SaaS) aufgebaut ist. In einer PaaS-Architektur sind Sie beispielsweise für die Sicherheit von Webanwendungen zuständig, in einer SaaS-Architektur hingegen der Cloud-Dienstanbieter.

Welche Architektur Sie auch auswählen, es kommt entscheidend auf die Zusammenarbeit mit Ihrem Cloud-Dienstanbieter an. Klären Sie gemeinsam, wer wofür zuständig ist, entwickeln Sie wirksame Kommunikationsprotokolle für den Umgang mit Sicherheitsproblemen und etablieren Sie eine Aufsicht, die gewährleistet, dass der Cloud-Dienstanbieter seinen Sicherheitsverpflichtungen nachkommt.

Veränderte Umsetzung von Sicherheitsrollen

Ihre Sicherheitsorganisation arbeitet nicht nur mit einem neuen Partner in der Cloud zusammen. Sie muss auch die eigenen Arbeitsweisen verändern. Jede Organisation ist anders, aber Google hat einige typische Änderungen bei den Sicherheitsrollen und Zuständigkeiten identifiziert, mit denen Sie beim Umstieg in die Cloud rechnen müssen. In der folgenden Tabelle haben wir die Art der Arbeit in diesen Rollen während der Transformation hin zur Cloud und die zukünftigen neuen Zuständigkeiten in diesen Rollen beschrieben.

Rolle	Zuständigkeiten in der Cloud
Richtlinien- und Risikomanagement	Sie klären unabhängig von existierenden Frameworks und Implementierungen Ziele beim Richtlinien- und Risikomanagement. Sie gliedern Sicherheitsrichtlinien und -standards neu, damit bei den Kontrollen die richtigen Schwerpunkte gesetzt und Cloud-Sicherheitsmodelle genutzt werden.
Sicherheitsarchitektur und -design	Sie stellen eine umfassende Definition der gesamten Vorgehensweise des Unternehmens zum Thema Sicherheit in der Cloud auf. Sie entwickeln Pläne mit Leitlinien zur schnellen und effektiven Implementierung von Cloud-Sicherheit.
Sicherheitstests	Sie arbeiten während des gesamten Lebenszyklus der Softwareentwicklung eng mit dem Entwicklungsteam zusammen. Sie führen sicherheitsorientierte Tests für häufige iterative Releases durch.
Sicherheitsabläufe	Sie dehnen das Monitoring auf die Cloud aus und setzen cloudnative Telemetrie ein, um Ereignis-, Vorfall- und Bedrohungsdaten zu erkennen und darauf zu reagieren.
Sicherheitsgarantien	Sie implementieren Monitoring durch kontinuierliche Kontrollen, um mithilfe der Cloud-Konfiguration datenorientiert zu prüfen, ob die Architekturen eingehalten werden und die Kontrollen funktionieren.
Sicherheitstechnik	Sie entwickeln cloudnative Sicherheits-Toolkits. Sie definieren gemeinsam mit der Infrastrukturtechnik die Sicherheitsrichtlinien direkt im Code.
Infrastrukturtechnik	Sie entwickeln und betreiben Cloud-Infrastrukturen und unterstützende Dienste mit der Methode „Infrastructure-as-code“. Bei dieser Vorgehensweise werden Richtlinien direkt in den Code integriert und manuelle Fehler minimiert. Für den Erfolg in der Cloud ist das entscheidend. Möglicherweise haben Sie in der eigenen Sicherheitsorganisation niemanden mit diesen speziellen Fähigkeiten. Schulung und Weiterbildung sind deshalb für diese Rolle besonders wichtig.
Anwendungsentwicklung	Sie entwickeln Anwendungen für die Cloud-Infrastruktur. Entwicklungszeitpläne werden beschleunigt und Produktstarts erfolgen iterativ. Sie arbeiten während des gesamten Lebenszyklus der Softwareentwicklung eng mit Sicherheitsteams zusammen.

Jede dieser Rollen wird sich in Bezug auf die Herangehensweise und die verwendeten Tools und Technologien erheblich verändern. Schulungen sind während der Transformation hin zur Cloud deshalb besonders wichtig. Als CISO müssen Sie unter anderem Ihre Sicherheitsorganisation veranlassen, sich in die Cloud einzuarbeiten, neue Rollen und Zuständigkeiten wie Infrastrukturtechnik auszufüllen und mit der Softwareentwicklung und deren Lebenszyklus zusammenzuarbeiten. Planen Sie dabei erheblichen Zeitaufwand für interne Schulungen ein. Dieser anfängliche Aufwand zahlt sich aus, sobald Sie Ihre Sicherheitsrichtlinien in der Cloud implementieren.

Entwicklung eines Betriebsmodells für Sicherheit

Die Transformation zur Cloud-Sicherheit ist eine Chance, das eigene operative Sicherheitsmodell zu überdenken. Wie sollen Sicherheitsteams mit Entwicklungsteams zusammenarbeiten? Sollen Sicherheitsfunktionen und -vorgänge zentral oder föderiert organisiert werden? Als CISO müssen Sie vor der Umstellung auf die Cloud diese Fragen klären und ein operatives Sicherheitsmodell entwickeln. In diesem Abschnitt möchten wir Sie bei der Auswahl eines für die Cloud geeigneten operativen Sicherheitsmodells unterstützen. Dazu stellen wir die Vor- und Nachteile von drei Modellen gegenüber: zentralisiert, föderiert und hybrid.

Betriebsmodell „zentralisierte Sicherheit“

Das zentralisierte Sicherheitsmodell kann als traditionelles bzw. klassisches Modell betrachtet werden. Bei diesem Modell liefert ein zentrales Sicherheitsteam umfassende Sicherheitslösungen einschließlich Sicherheitsrichtlinien, Sicherheitslösungen und Vorfallmanagement für andere Teams im Unternehmen. Über wohldefinierte Prozesse, häufig mit Ticketsystemen zum Workflowmanagement, setzt sich das Sicherheitsteam mit diesen anderen Teams auseinander, zum Beispiel den Entwicklungsteams. Abbildung 2 zeigt, wie Sicherheitsrollen und -zuständigkeiten im zentralisierten Sicherheitsmodell verteilt sind.

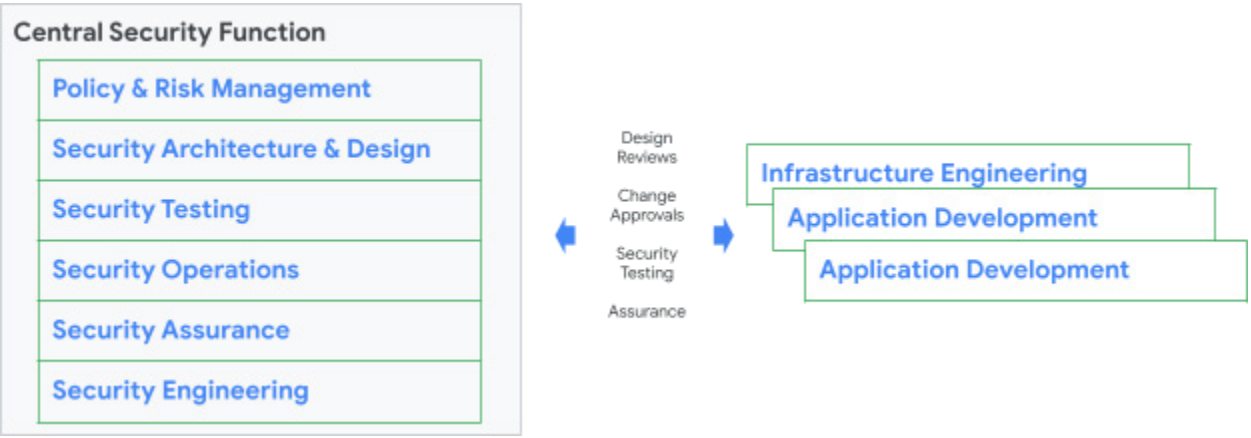


Abbildung 2: Verteilung von Rollen und Zuständigkeiten im zentralisierten Sicherheitsmodell. Bei diesem Modell werden die meisten sicherheitsbezogenen Tätigkeiten von einer zentralen Sicherheitsabteilung erledigt, die mit Technik- und Entwicklungsteams im gesamten Unternehmen zusammenarbeitet.

Vorteile: Mit dem zentralisierten Modell können Sie eine starke, einheitliche Kontrolle über die Sicherheit im eigenen Unternehmen beibehalten. Sie profitieren auch von einigen Kostenvorteilen durch zentrale Entwicklung von Sicherheitsrichtlinien und -lösungen und deren unternehmensweite Einführung.

Nachteile: Das zentralisierte Modell ist am besten geeignet, wenn nach dem Wasserfall-Modell entwickelt wird und die IT-Auslieferung entsprechend langsam erfolgt. Für den schnelleren Entwicklungstakt in der Cloud ist es normalerweise nicht schnell bzw. agil genug. Außerdem kann sich beim zentralisierten Modell außerhalb des zentralen Sicherheitsteams der Gedanke festsetzen, dass für Sicherheit jemand anders zuständig ist.

Betriebsmodell „föderierte Sicherheit“

Beim föderierten Sicherheitsmodell werden die meisten Sicherheitsfunktionen aus einem zentralen Sicherheitsteam heraus in einzelne Technik- und Entwicklungsteams verlagert. Dieses föderierte Modell wird häufig in Konzernorganisationen eingesetzt, in denen ein zentrales Team nicht alle Teams in der Organisation adäquat versorgen kann. Dieses Modell wird auch in kleinen Organisationen eingesetzt, die schnell vorankommen und Sicherheitskompetenz in Technik- und Entwicklungsteams integrieren möchten. Abbildung 3 zeigt, wie Sicherheitsrollen und -zuständigkeiten im föderierten Sicherheitsmodell verteilt sind.

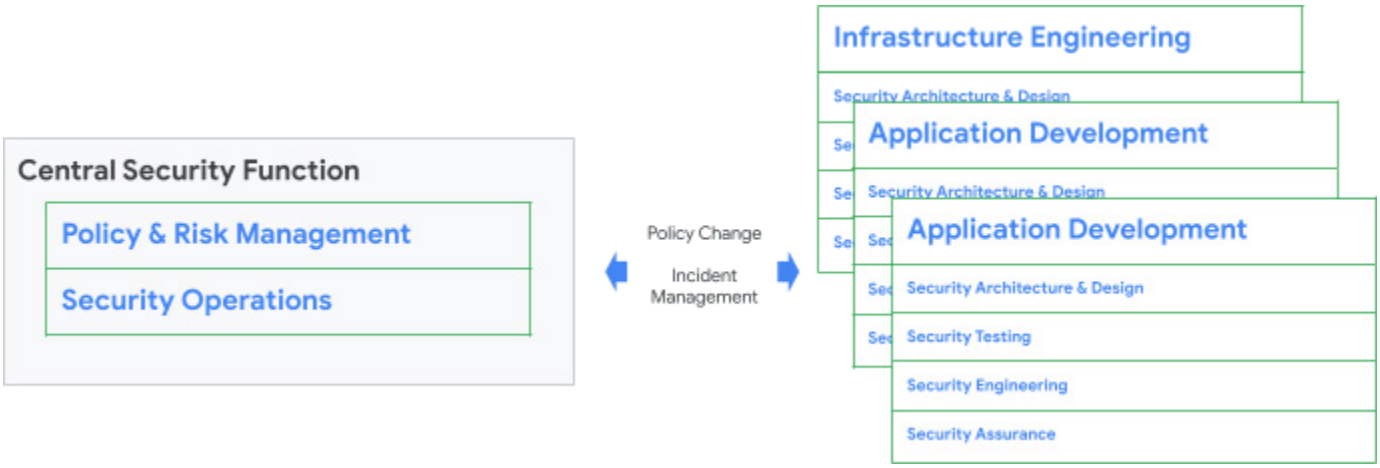


Abbildung 3: Verteilung von Rollen und Zuständigkeiten im föderierten Sicherheitsmodell. Bei diesem Modell werden die meisten sicherheitsbezogenen Tätigkeiten innerhalb einzelner Technik- und Entwicklungsteams erledigt.

Vorteile: Bei einem föderierten Modell können Teams schnell vorankommen und Sicherheit wird zu einem integrierten Bestandteil des beschleunigten Entwicklungsprozesses. Sicherheitsexperten verstehen die Details der Teams, mit denen sie zusammenarbeiten, und bieten ein „gerade ausreichendes Maß“ an Sicherheit für die Bedürfnisse dieser Teams.

Nachteile: Das föderierte Modell ist mit höheren Risiken verbunden, da es kein zentrales, unabhängiges Sicherheitsteam als Sicherheitsgarantie gibt und keine robusten Sicherheitslösungen für allgemeine Sicherheitsbedrohungen entwickelt werden. Die Teams entwickeln vielmehr maßgeschneiderte Sicherheitslösungen, die spezielle Probleme lösen, übersehen aber oft andere Sicherheitsbedrohungen dabei.

Betriebsmodell „hybride Sicherheit“

Das dritte operative Sicherheitsmodell, das Hybridmodell, stellt einen Mittelweg dar. Beim hybriden Modell bestimmen Größe, Umfang und Komplexität der jeweiligen Entwicklungsteams den Grad der Zentralisierung oder Föderation der Sicherheitsfunktionen. Abbildung 4 zeigt zwei Arten von Hybridmodellen.

Das Team für Infrastrukturtechnik und das erste Team für Anwendungsentwicklung verwenden ein **leichtes „Hybridmodell“** wie es die meisten Unternehmen einsetzen, wenn sie ein Hybridmodell verwenden. Bei einem leichten Hybridmodell nutzen Technik- oder Entwicklungsteam standardisierte Tools, Prozesse und Methoden, die vom zentralen Sicherheitsteam entwickelt wurden. Ein Sicherheitskoordinator im Technik- oder Entwicklungsteam stellt die Schnittstelle zum Sicherheitsteam dar.

Eine Person kann ausschließlich für Sicherheitskoordination zuständig sein oder auch an anderen Aspekten der Entwicklung arbeiten.

Das zweite Team für Anwendungsentwicklung verwendet ein **schweres „Hybridmodell"** das eher von großen Teams mit komplexen Sicherheitslandschaften eingesetzt wird. Bei einem schweren Hybridmodell nutzen Technik- oder Entwicklungsteam viele standardisierte Tools, Prozesse und Methoden des zentralen Sicherheitsteams. Das Technik- oder Entwicklungsteam konzipiert und entwickelt jedoch auch einige eigene Sicherheitslösungen und kommuniziert dabei mit dem zentralen Sicherheitsteam. Bei dem schweren Hybridmodell integriert das Technik- oder Entwicklungsteam einige Fähigkeiten des Sicherheitsteams direkt in das eigene Team, um Schritt zu halten und den Bereich Sicherheit mit Fachwissen über das Produkt des Teams auszustatten.

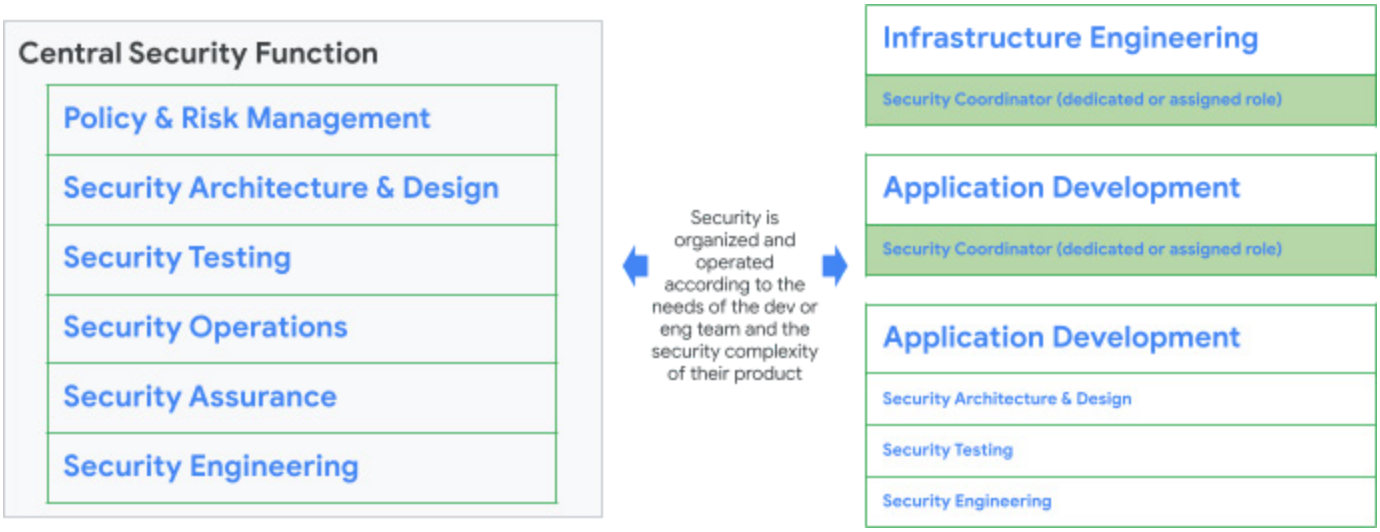


Abbildung 4: Verteilung von Rollen und Zuständigkeiten im hybriden Sicherheitsmodell. Bei diesem Modell hängen Zentralisierung bzw. Föderation von Sicherheitsfunktionen von den Bedürfnissen der Entwicklungs- bzw. Technikteams und der Komplexität ihrer Produkte bezüglich Sicherheit ab.

Vorteile: Das Hybridmodell lässt sich sehr gut anpassen. Da bei diesem Modell ein zentrales Sicherheitsteam eingesetzt wird, können die Technik- und Entwicklungsteams standardisierte Sicherheitslösungen verwenden, sind aber auch flexibel genug, individuelle Lösungen für ihre speziellen Anforderungen zu entwickeln. Das zentrale Sicherheitsteam im hybriden Modell bietet ebenfalls unabhängige Sicherheit, kann sich aber für mehr Sicherheitsabdeckung und Effizienz auf produktspezifisches Sicherheitswissen stützen.

Nachteile: Das hybride Modell erfordert starke, kontinuierliche Kommunikation und Zusammenarbeit, damit die Entwicklungs- und Technikteams und das zentrale Sicherheitsteam immer wissen, wer wofür zuständig ist. Der Sicherheitskoordinator sowie die Sicherheitsspezialisten, die in die Entwicklungs- und Technikteams integriert sind, sind für diese Zusammenarbeit besonders wichtig und müssen sehr gut kommunizieren, damit das Hybridmodell erfolgreich ist.

Best Practices für die Cloud-Sicherheit identifizieren

Ein häufiger Fehler bei der Transformation in die Cloud besteht darin, die bisherigen Sicherheitsverfahren und -richtlinien in der Cloud-Umgebung weiter anzuwenden. Aber Sicherheitsmethoden, die in lokalen und anderen traditionellen Umgebungen funktionieren, eignen sich nicht unbedingt für die Cloud.

Als CISO sollten Sie die Cloud-Transformation des Unternehmens als Chance für eine Sicherheitstransformation nutzen. Verabschieden Sie sich von den Annahmen, die Sie auf der Grundlage Ihrer vorhandenen Sicherheitsinfrastruktur getroffen haben. Denken Sie neu über Ihre *Sicherheitsziele* nach. Was möchten Sie erreichen? Und wie kann die Größe und Geschwindigkeit der Cloud es möglich machen?

Wenn Sie sich anlässlich der Transformation Ihrer Sicherheitsinfrastruktur diese Fragen stellen, sollten Sie übliche Anti-Patterns vermeiden, die auf traditionellen Sicherheitsimplementierungen basieren. Identifizieren Sie stattdessen Best Practices für Cloud-Sicherheit anhand der folgenden Tabelle.

✗ Don'ts	✓ Do's
Die Annahme, dass die vorhandenen Kontrollmechanismen wirksam sind.	Überprüfen Sie zuerst die *Ziele* der Kontrollen. Führen Sie die Implementierung dann anhand dieser Ziele durch.
Die Annahme, dass bisherige Prozesse, insbesondere zentralisierte Prozesse, in der Cloud funktionieren werden.	Geben Sie Teams die Möglichkeit, flexible Cloud-Prozesse zu implementieren, statt nach Workarounds für vorhandene Prozesse zu suchen.
Nutzung lokaler Modelle, etwa einer virtuellen Sicherheitsanwendung wie eines Intrusion Prevention Systems (IPS), für Sicherheitskontrollen in der Cloud.	Nutzen Sie cloudnative Methoden, z. B. Log-Monitoring und Zugriffsverwaltung.
Einsatz historischer Methoden zur Einhaltung von Richtlinien und Standards.	Führen Sie datengestützte Methoden ein, um die Skalierung und die Geschwindigkeit zu erreichen, die für kontinuierliches Kontroll-Monitoring erforderlich sind.

Fazit

Die Umstellung auf die Cloud ist eine große Chance für eine Sicherheitstransformation des Unternehmens. Für eine erfolgreiche Transformation der Sicherheitsorganisation und des ganzen Unternehmens sollten Sie Arbeitsweisen, Risikomanagement und die Bereitstellung von Sicherheitsinfrastruktur neu überdenken. Als CISO sollten Sie eine Sicherheitskultur im gesamten Unternehmen etablieren und das Sicherheitsdenken des Unternehmens gezielt verändern.

Für eine erfolgreiche Transformation empfiehlt Google folgende Merkpunkte für Sicherheit in der Cloud:

- Steigen Sie frühzeitig in die Sicherheitsplanung ein.
- Vertrauen Sie auf ein risikobewusstes Vorgehen anstatt die vollständige Risikovermeidung.
- Setzen Sie auf Zero-Trust und vergessen Sie den Perimeter.
- Machen Sie Automatisierung zur Priorität, um manuellen Aufwand zu verringern und schneller zu werden.
- Planen Sie Weiterbildung, Umschulung und Reorganisation des Sicherheitspersonals ein.
- Arbeiten Sie auf der Grundlage gemeinsam geklärter Risiken und Ziele partnerschaftlich mit Cloud-Dienstanbietern zusammen.
- Hinterfragen Sie bisherige Sicherheitsannahmen und setzen Sie auf cloudspezifische Best Practices.

Die Kernpunkte und Empfehlungen in diesem Whitepaper sind das Ergebnis der langjährigen Führungsrolle und der Innovationen von Google im Bereich Cloud-Sicherheit. Gern beantworten wir Ihre Fragen zum Thema Cloud-Sicherheit und beraten Sie bei Ihrer eigenen Cloud-Sicherheitstransformation.