Zscaler™ CSPM

zscaler™

Inhaltsverzeichnis

Einleitung

Unsere Welt befindet sich im rapiden Wandel. Branchenübergreifend setzen immer mehr Unternehmen auf digitale Transformation. Die schnelle Entwicklung neuer Anwendungen wird damit zum entscheidenden Wettbewerbsfaktor – und die öffentliche Cloud zur einzigen Umgebung, die das erforderliche Tempo der Veränderungen unterstützt.

Indes sehen sich Sicherheits- und Risikobeauftragte sowie Unternehmensleiter mit zahlreichen Problemen konfrontiert:

1. Sicherheitslücken durch Fehlkonfigurationen der Cloud-Infrastruktur führen zu Datenschutzverletzungen, die große Mengen vertraulicher Kundendaten betreffen. Dadurch entstehen Haftungsansprüche und finanzielle Verluste.
2. Die kontinuierliche Konformität mit allen relevanten gesetzlichen und aufsichtsrechtlichen Vorschriften lässt sich mit herkömmlichen lokal installierten Tools und Prozessen nicht mehr gewährleisten.
3. Mit der unternehmensweit zunehmenden Nutzung der Cloud vervielfachen sich auch die mit der Cloud-Governance verbundenen Herausforderungen (Transparenz, abteilungsübergreifende Durchsetzung von Richtlinien, unzureichende Kenntnisse in Bezug auf Sicherheitsmaßnahmen).

In diesem Whitepaper wird die wachsende Kluft untersucht, die zwischen der zügigen Entwicklung von Cloud-Anwendungen einerseits und der zögerlichen Umsetzung von Sicherheitsmaßnahmen andererseits klafft. Dieses Problem betrifft auch die nativen Lösungen der Cloud-Anbieter, deren Funktionsumfang in der Regel sehr eingeschränkt ist. Hervorgehoben wird die Notwendigkeit einer erweiterten, dynamischen Übersicht über die Sicherheitsmaßnahmen sowie einer nahtlosen Zusammenarbeit zwischen Sicherheits- und Entwicklungsteams zur Durchsetzung der einschlägigen Richtlinien.

> Die Frage ist nicht so sehr, ob die Cloud sicher ist ... Die eigentliche Frage lautet, wie sicher Sie damit arbeiten.
>
> **– Gartner**

Die Cloud erfordert einen neuartigen Sicherheitsansatz

Datenschutzverletzungen haben erhebliche Auswirkungen aufs Geschäft

Dem 2019 veröffentlichten IBM-Bericht „Cost of a Data Breach"[1] zufolge belaufen sich die durchschnittlichen Kosten einer Datenschutzverletzung global auf geschätzte 3,9 Mio. USD – in den USA sind es sogar 8,2 Mio. USD. Den größten Posten machen dabei die finanziellen Einbußen infolge des verlorenen Kundenvertrauens aus.

Durchschnittl. Kosten einer Datenverletzung

Global

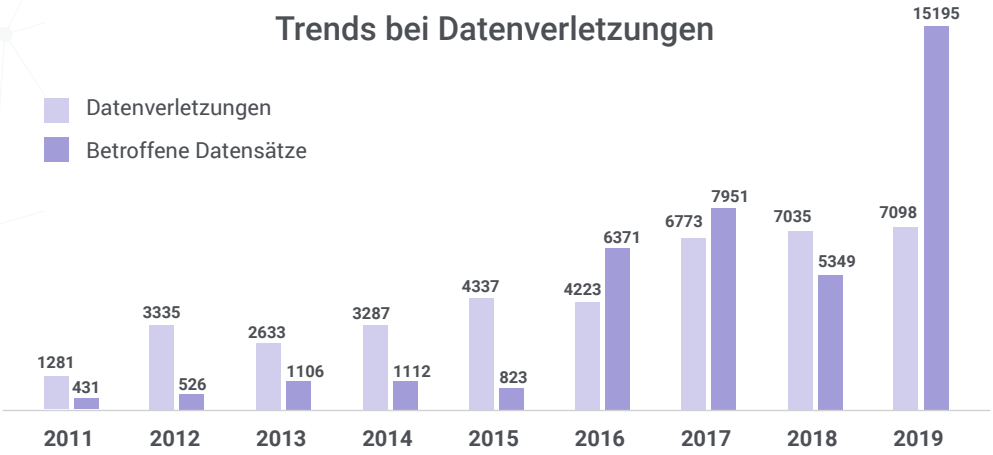
3,9 Millionen USD

USA

8,2 Millionen USD

[1] Cost of a Data Breach Report, IBM, 2019

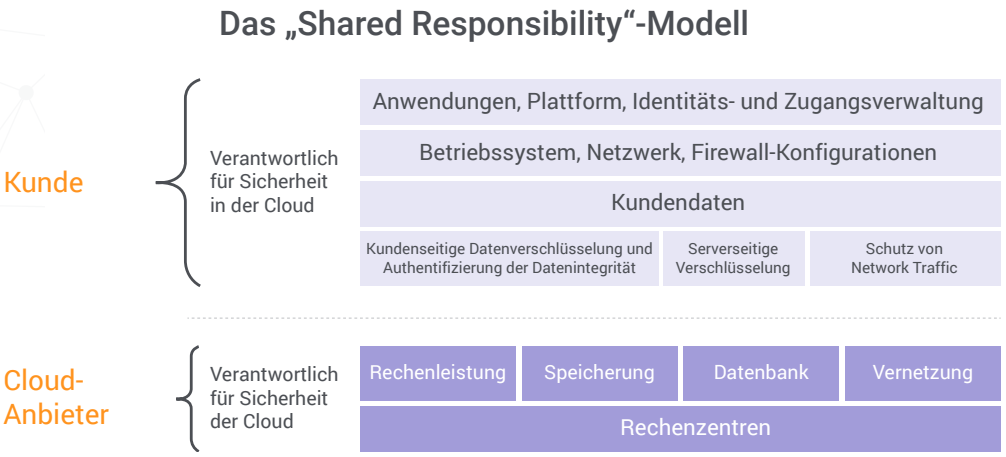
Laut eines Berichts von Risk Based Security[2] waren 15 Milliarden Datensätze 2019 von Datenschutzverletzungen betroffen – ein beträchtlicher Anstieg gegenüber den Vorjahren. Fast die Hälfte der betroffenen Datensätze (6,7 Milliarden) wurden bei vier Verletzungen im 4. Quartal kompromittiert, die durch falsch konfigurierte Datenbanken verursacht wurden.



Wie aus dem Threat Intelligence Index für 2020 von IBM X-Force [3] hervorgeht, hat sich die Anzahl der durch Fehlkonfigurationen kompromittierten Datensätze gegenüber dem Vorjahr verzehnfacht und macht 86 Prozent der Gesamtanzahl aller 2019 von Datenschutzverletzungen betroffenen Datensätze aus.

Geteilte Verantwortung für Cloud-Sicherheit

Cloud-Anbieter (CSPs) verwenden verschiedene Hardware- und Software-Komponenten (Rechenleistung, Speicherplatz, Datenbanken, Netzwerke) zum Aufbau ihrer Infrastrukturen. Cloud-Anbieter sind für die Sicherheit der Cloud verantwortlich. Sie haben massiv in die Sicherung ihrer Cloud-Infrastruktur investiert und weisen ihre Compliance durch die entsprechenden Zertifizierungen nach.



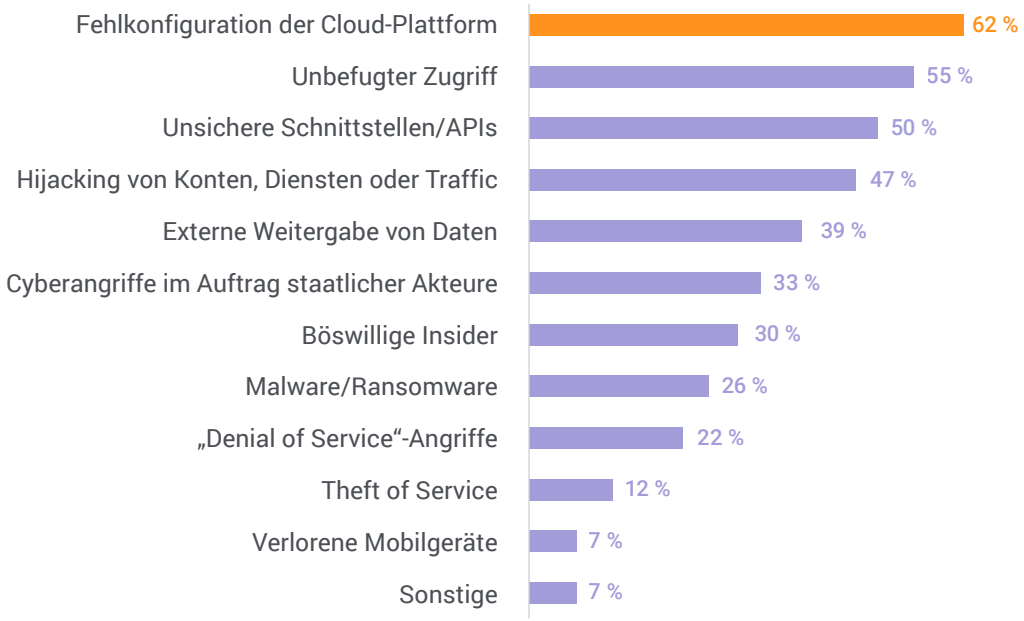
Während der Cloud-Anbieter für die Sicherung der zugrunde liegenden Infrastruktur zu sorgen hat, liegt die Verantwortung für die Sicherheit der Anwendungen und Konfigurationen beim Kunden selbst. Dieses Prinzip trifft auf sämtliche Cloud-Dienste zu, die der Kunde in Anspruch nimmt, einschließlich Hosting und Container-Cluster, IaaS, PaaS, SaaS und Sicherheitsangebote.

[2] 2019 Year End Data Breach QuickView Report, Risk Based Security, 2020
[3] IBM X-Force Threat Intelligence Index, 2020

Fehlkonfiguration als größte Sicherheitsbedrohung

Sicherheitsexperten zufolge stellen Fehlkonfigurationen die schwerste Sicherheitsbedrohung in der Cloud dar.[4] Verschärfend kommt hinzu, dass auch die Faktoren, die zu anderen möglichen Bedrohungen beitragen (wie z. B. unbefugter Zugriff, unzureichend gesicherte Benutzeroberflächen, Hijacking von Konten), zumeist auf Fehlkonfigurationen als wahrscheinlichste Ursache zurückzuführen sind.

Top-Bedrohungen für die Sicherheit in der Cloud



Forschungsanalysten warnen ebenfalls vor der Bedrohung, die durch Fehlkonfigurationen entsteht. „Fast alle erfolgreichen Angriffe auf Cloud-Dienste sind auf Konfigurations-, Verwaltungs- und andere Fehler zurückzuführen. Sicherheits- und Risikobeauftragte sollten in Prozesse und Tools zur Verwaltung der Sicherheitsmaßnahmen für die Cloud investieren, um diese Risiken pro- und reaktiv erkennen und beheben zu können", heißt es entsprechend im Gartner-Bericht „Innovation Insight for Cloud Security Posture Management".[5]

Herkömmliche Sicherheitsansätze greifen nicht mehr

Früher bildete das Netzwerk eines Unternehmens die Außengrenze, die es zu sichern galt, um wertvolle Daten in Datenbanken und Fileshares zu schützen. In der Cloud können einzelne Datenbanken mit ein paar einfachen Änderungen an der Konfiguration gehackt werden. Um die Arbeit der Entwickler nicht zu behindern, wird in der Entwicklungsphase gerne auf die Sperrung von Datenspeichern verzichtet. So kann es passieren, dass diese Konfigurationen versehentlich in die Produktivumgebung übernommen werden.

Herkömmliche Sicherheitsbewertungen sind zu langsam

Herkömmliche manuelle Sicherheits- und Konformitätsprüfungen sind umständlich und zeitaufwendig. Dabei befragen die Prüfer die IT-Mitarbeiter und erstellen als Konformitätsnachweis Screenshots der Konfigurationen der einzelnen Produkte. In der Cloud werden Infrastrukturen so häufig aktualisiert, dass sie längst völlig anders aussehen, wenn die Sicherheitsprüfung endlich abgeschlossen ist. Um mit dem Tempo der Entwicklung und Aktualisierung von Cloud-Anwendungen mitzuhalten, führt an der Automatisierung von Sicherheits- und Konformitätsbewertungen kein Weg vorbei.

[4] Cloud Security Report, Cybersecurity Insiders, 2018
[5] Innovation Insight for Cloud Security Posture Management, 2019

Herausforderungen beim Compliance-Nachweis

In regulierten Branchen (Einzelhandel, Gesundheits- und Finanzwesen usw.) sind die Unternehmen an branchenspezifische Standards gebunden. Bei der Konformitätsbewertung verlassen sich viele Unternehmen nach wie vor auf die mündliche Befragung der betreffenden Mitarbeiter. Die Erbringung der entsprechenden Nachweise nach den jeweiligen behördlichen Vorgaben wird damit zu einem umständlichen Unterfangen. Diese Vorgaben dienen als übergeordnete Kontrollen, deren Anforderungen jederzeit eingehalten werden müssen. Teilweise ist die dauerhafte Compliance darin ausdrücklich als Anforderung vorgeschrieben. Angesichts der Dynamik von Cloud-Workloads werden die beschriebenen Probleme weiter verschärft.

Cloud-Anbieter stellen grundlegende Funktionen bereit

CSPs bieten Tools zur Überwachung der Sicherheits- und Konformitätsmaßnahmen an. Diese Produkte bieten die grundlegende Abdeckung von Sicherheitsrichtlinien und unterstützen eine begrenzte Anzahl von Compliance-Frameworks. Ein erheblicher Integrations- und Entwicklungsaufwand ist erforderlich, um die effektive unternehmensweite Sicherheits- und Konformitätsüberwachung zu gewährleisten. Unternehmen, die Anwendungen in der öffentlichen Cloud bereitstellen, sind somit genötigt, Kompromisse bei der Abwägung zwischen Entwicklungstempo und Sicherheitsrisiken einzugehen. Großunternehmen mit Hunderten von Entwicklern, die ständig neuen Code für die Produktivumgebung freigeben, kommen nicht um die Implementierung einer vollständig automatisierten Lösung zur Sicherheits- und Konformitätsüberwachung herum.

Cloud Security Posture Management (CSPM) als neuer Ansatz

Gartner definiert Cloud Security Posture Management (CSPM) als eine neue Produktkategorie, die sich durch die Lösung mehrerer Probleme herkömmlicher Sicherheitsansätze durch Automatisierung der Sicherheits- und Konformitätsüberwachung und Gewährleistung adäquater Kontrolle über die Konfiguration von Cloud-Infrastrukturen auszeichnet. Die wachsende Nachfrage nach CSPM-Lösungen lässt die Prognose zu, dass innerhalb der nächsten Jahre eine Marktdurchsetzung von 25 Prozent erreicht werden kann. Bei den Unternehmen wächst das Bewusstsein, dass es sich hier um ein unverzichtbares Tool zur Gewährleistung der Cloud-Sicherheit handelt.

CSPM – die Zscaler-Methode

Bei vielen CSPM-Lösungen besteht das Problem, dass sie sich nicht in die vorhandenen Tools und Prozesse des Unternehmens zur Gewährleistung von Sicherheit und Datenschutz integrieren lassen. Sie liefern punktuelle Einblicke, die sich nicht ins Gesamtbild einfügen.

Zscaler CSPM ist die einzige Lösung, die das Integrationsproblem durch automatisches Erkennen und Beheben von Fehlkonfigurationen im Rahmen der zu 100 % cloudbasierten Datensicherungsfunktionen der Zscaler Cloud Security Platform löst.

Zscaler CSPM stellt Unternehmen ein breites Spektrum an Innovationen und Produktfunktionen zur automatischen Überwachung von Sicherheit und Compliance in der Cloud, Gewährleistung ständiger Transparenz und Durchsetzung von Sicherheitsrichtlinien und aufsichtsrechtlichen Vorgaben zur Verfügung.

Erfassen von Ist-Konfigurationen

Die CSPM-Anwendung von Zscaler ist zum Zugriff auf alle gängigen Cloud-Umgebungen (AWS, Azure, Office 365, Google Cloud usw.) berechtigt. Dadurch wird die Erfassung von Ist-Konfigurationen der Cloud-Infrastruktur über APIs ermöglicht. Bei bestimmten Richtlinien kann die Installation eines Agents erforderlich sein.

Erkennen von Fehlkonfigurationen

Zscaler CSPM gleicht die erkannten Konfigurationen mit integrierten Sicherheitsrichtlinien ab und findet etwaige Fehlkonfigurationen auf Richtlinien- und Ressourcenebene. Darüber hinaus wird die Zuordnung von Sicherheitsrichtlinien zu verschiedenen Compliance-Vorgaben unterstützt. Übersichtliche Dashboards und Berichte vereinfachen die Auswertung dieser Informationen.

Verwaltung von Sicherheit und Konformität

Zscaler CSPM stellt eine Vielzahl von Funktionen zur Unterstützung der Cloud-Governance bereit: u. a. risikobasierte Prioritätensetzung, Richtlinienverwaltung (Overrides, Ausnahmen, kompensierende Kontrollen usw.) und Konfiguration unternehmens-, abteilungs- bzw. architekturspezifischer Standards.

Beheben von Fehlkonfigurationen

Es können Schritte zur Problembehebung für jede einzelne Sicherheitsrichtlinie sowie automatische Problembehebung für die wichtigsten Sicherheitsrichtlinien eingerichtet werden.

Erfassen von Ist-Konfigurationen

Onboarding

Die Gewährleistung des Zugriffs auf die von den Kunden genutzten Cloud-Umgebungen (Onboarding) ist ein schneller und unkomplizierter Prozess. Dazu wird zunächst ein Benutzer mit Berechtigung zum Registrieren von Anwendungen (in Azure and Office 365) bzw. zur Durchführung von Sicherheitsprüfungen (in AWS) angelegt. In einem zweiten Schritt werden die erforderlichen Zugriffsberechtigungen eingerichtet. In der Mehrzahl der Fälle handelt es sich um schreibgeschützten Zugriff.

Für bestimmte Richtlinien stellen Cloud-Anbieter die entsprechenden APIs nicht bereit; deswegen sind in Zscaler CSPM Funktionen zur automatischen Erfassung von Metadaten inbegriffen, sodass eine lückenlose Einhaltung aller relevanten Sicherheitsrichtlinien gewährleistet ist.

Multicloud

Viele Unternehmen entscheiden sich für Multicloud-Infrastrukturen, um von marktführenden Cloud-Diensten in Bezug auf Kosten, Funktionsumfang, Sicherheit und Skalierbarkeit zu profitieren. Zscaler CSPM zieht hier mit und bietet Unterstützung für Multicloud-Umgebungen, die künftig weiter ausgebaut werden soll.

Multicloud

CSP	2018	2019	2020
Microsoft Azure	■	■	■
Office 365	■	■	■
aws		■	■
Google Cloud Platform			■

Multiregional

Neben der standardmäßigen Bereitstellung in der öffentlichen Cloud unterstützt Zscaler CSPM im Rahmen des Saas-Angebots auch die Bereitstellung in der privaten Cloud für Unternehmen, die mehr Kontrolle über ihre Daten benötigen. In Übereinstimmung mit den Anforderungen des Kunden in Bezug auf die Datensouveränität werden diese Bereitstellungen in unterschiedlichen Regionen (Geografien) gehostet.

Skalierbarkeit

Zur Sicherung größerer Umgebungen mit über 10.000 Cloud-Ressourcen muss eine Reihe von Voraussetzungen erfüllt sein:

- hohe Skalierbarkeit beim Erfassen von Metadaten zur Konfiguration aus einem breiten Spektrum an Cloud-Ressourcen;
- Kapazitäten zur Speicherung großer Mengen an erfassten Metadaten in der Datenbank;
- möglichst kurze Scan-Zeiten und
- zeitnahe Anzeige der Sicherheitsdaten in übersichtlichen Dashboards und Berichten.

Zscaler CSPM macht sich aktuelle Fortschritte im Cloud-Computing zunutze, u. a. serverlose Funktionen zur Erfassung von Metadaten und NoSQL-Datenbanken (Cosmos DB) zum Speichern von Informationen. Bei jedem Scannen der Cloud-Infrastruktur werden Tausende von parallel laufenden serverlosen Funktionen zum Erfassen und Speichern von Metadaten erstellt. Die NoSQL-Datenbank bietet eine hochgradig skalierbare und unübertroffen schnelle Methode zum Speichern und Abrufen von Daten in der Cloud. Zscaler CSPM scannt in Minutenschnelle die gesamte Infrastruktur und generiert Berichte zur weiteren Analyse.

Datensicherheit

Die Informationen, die im Zuge der Erfassung von Metadaten gespeichert werden, geben Auskunft über den Ist-Zustand der Konfigurationen in der Cloud-Infrastruktur. Diese Informationen müssen vor dem Zugriff durch Cyberkriminelle geschützt werden. Deswegen müssen CSPM-Produkte eine komplette Verschlüsselung aller Daten sowohl bei der Übertragung als auch im Ruhezustand gewährleisten, die den Anforderungen stringenter regelbasierter Zugriffskontrollen (RBAC) und eindeutiger Richtlinien zur Datenspeicherung entspricht.

Anbieter von CSPM als SaaS weisen die Einhaltung einschlägiger Best Practices sowie den Reifegrad ihres Leistungsangebots in der Regel durch Zertifizierung gemäß SOC 2 nach.

Erkennen von Fehlkonfigurationen

Abdeckung von Sicherheitsrichtlinien

Inwieweit CSPM-Lösungen in der Lage sind, sämtliche vom Kunden verwendeten Cloud-Dienste zu bewerten, hängt vom Umfang der angewandten Sicherheitsrichtlinien in Bezug auf die jeweils unterstützten Cloud-Dienste ab.

Zscaler CSPM wendet aktuell über 1.500 Sicherheitsrichtlinien (Best Practices zur Überwachung der Cloud-Sicherheit) an und plant diese Abdeckung in naher Zukunft weiter auszubauen.

Umfang der Sicherheitsrichtlinien

Cloud-Infrastruktur

IaaS Compute AWS EC2, Azure VMs, VM Scale Sets, Azure Service Fabric Cluster

PaaS und serverlose Funktionen, Lambdas, Web-Apps, API-Apps, Mobil-Apps

Vernetzung Azure Vnet AWS VPC, Cloud Firewall, NSG, Sicherheitsgruppen, DDoS, WAF, Ports, Protokolle

Datenanalyse HDInsight, Data Lake

Speicherung Azure Storage, AWS S3

PaaS-Datenbanken Azure SQL DB, SQL-Server, SQL DW, NoSQL DBs, AWS RDS, AWS RedShift, AWS Aurora DB, AWS Dynamo DB, Postgres SQL, MySQL

Backups Backup-Vaults, Aufbewahrung, Verschlüsselung, Zugriff

Protokollierung, Auditing und Überwachung Azure Monitor, Application Insights, CloudWatch, CloudTrail

Cloud Account Security Root-Account-Einstellungen, IAM-Einstellungen, Profilüberwachung, Security-Center/Hub-Konfigurationen

IAM-Zugangskontrollen MFA, integrierte Rollen, Gast-User

Virtual Machine OS Baseline Windows 2012 R2, Windows 2016

Kubernetes Control Planes AKS-Patching, ASC-Integrationen, AD-Integrationen

Schlüsselverwaltung Azure Key Vault, AWS KMS

Data-In-Transit TLS/SSL, Zertifikat-Authentifizierung, Applikation-Gateway, OWASP WAF-Konfigurationen

SaaS

Identität und Authentifizierung einfache und erweiterte Authentifizierung, Zurücksetzen von Passwörtern im Selfservice-Verfahren, globale Administratoren

Berechtigungen für Anwendungen SafeLinks, externe User, ATP

Nutzung von Anwendungen riskante Apps, Insider-Bedrohungen, Verbindung kompromittierter Konten

Auditing Protokollierung, Aktivitätsberichte

Daten und Datenverwaltung

Geräteverwaltung Verwaltung von Mobilgeräten, Intune-Konfigurationen, Richtlinien für Geräte-Passwörter

E-Mail-Sicherheit/Exchange

Dokumentaustausch Whitelisting von externen Domains

Angestrebt wird eine flächendeckende Abdeckung von Richtlinien für alle gängigen Cloud-Dienste sowie die Erfüllung darüber hinausgehender Sonderanforderungen einzelner Kunden. Jeder Cloud-Anbieter hat eigene Richtlinien. Zscaler CSPM ist seit jeher Branchenführer in Bezug auf die Abdeckung der Richtlinien für Microsoft Azure und Office 365 und zählt mittlerweile auch in Bezug auf AWS-Richtlinien zu den Spitzenanbietern.

Compliance-Frameworks

Zscaler CSPM unterstützt insgesamt 13 Compliance-Frameworks, einschließlich Cybersicherheits- und Branchenstandards sowie gesetzliche und aufsichtsrechtliche Vorschriften. Dieser Umfang wird aktuell weiter ausgebaut, sodass künftig auch regionale Compliance-Frameworks u. a. für Europa und Australien abgedeckt werden.

Compliance-Framework

Cybersicherheitsstandards

NIST CSF | NIST 800-53r4

CIS

cloud security alliance

Gesetze und Vorschriften

HIPAA COMPLIANCE

General Data Protection Regulation

Branchenstandards

NIST CSF | NIST 800-53r4

ISO 27001

PCI Data Security Standard V 3.2

AICPA SOC

SOC 2

FFIEC

GxP

Verwaltung von Sicherheit und Konformität

Zscaler CSPM stellt eine Vielzahl von Funktionen zur Unterstützung der Cloud-Governance bereit: u. a. risikobasierte Prioritätensetzung, Richtlinienverwaltung und Konfiguration unternehmens-, abteilungs- bzw. architekturspezifischer Standards.

Richtlinienverwaltung

Zscaler CSPM beinhaltet zahlreiche Funktionen zur Verwaltung der Anwendung von Sicherheitsrichtlinien auf die erkannten Assets.

- So können Kunden vorübergehende (zeitlich befristete) oder dauerhafte Ausnahmen für einzelne Richtlinien und Cloud-Konten definieren.
- Außerdem besteht die Möglichkeit, durch Overrides die Konformität in Fällen zu bestätigen, in denen kompensierende Kontrollen von Dritten zum Einsatz kommen, die vom CSPM-Produkt nicht erfasst werden.
- Wenn eine Automatisierung nicht möglich ist (z. B. weil Zscaler keine API bereitstellt oder das betreffende Unternehmen keinen Zugriff zum Scannen sensibler Daten gewährt), können Best Practices anhand manueller Richtlinien überwacht werden.

Unternehmensspezifische Standards

Je nach Unternehmensgröße und Branche können Sicherheitsanforderungen stark variieren. Kunden haben die Möglichkeit, sämtliche relevanten Compliance- und Best-Practice-Anforderungen in einem unternehmenseigenen Standard zusammenzufassen. Dieser Standard kann von verschiedenen Mitarbeitern gemeinsam erarbeitet und auf entsprechend definierte Cloud-Konten angewandt werden.

Zscaler CSPM stellt eine benutzerfreundliche Konfigurationsschnittstelle zur Einrichtung unternehmensspezifischer Standards bereit. Diese können entweder auf der Basis bestehender Standards oder der individuellen Anforderungen des Unternehmens definiert werden. Diese Standards sind versionskontrolliert und eignen sich daher auch zur Durchsetzung zunehmend höherer Standards im Zeitverlauf. So kann der ursprünglich festgelegte v1-Standard zur Verbesserung der Sicherheitsmaßnahmen für spätere Versionen durch einen v2-Standards ersetzt werden usw.

Risikomatrix

Die risikobasierte Prioritätenmatrix richtet sich nach der Norm ISO 27005. Sicherheitsrichtlinien werden automatisch nach Risikoauswirkungen und -wahrscheinlichkeit kategorisiert. Die *Risikowahrscheinlichkeit* wird als „Unwahrscheinlich“, „Niedrig“, „Mäßig“, „Hoch“ oder „Sehr hoch“ eingestuft. Die *Risikoauswirkungen* werden als „Sehr niedrig“, „Niedrig“, „Mäßig“, „Hoch“ oder „Kritisch“ eingestuft. Die Risikoauswirkungen werden für jede Sicherheitsrichtlinie vordefiniert. Die Risikowahrscheinlichkeit wird anhand unterschiedlicher Kennzahlen mithilfe eines ML-Algorithmus dynamisch berechnet.

Risikomatrix (gemäß ISO 27005)

Risikostufe

Hoch
109

Mäßig
150

Niedrig
201

Risikowahrscheinlichkeit	Risikoauswirkung: Sehr niedrig	Niedrig	Mäßig	Hoch	Kritisch
Sehr hoch	10	50	61	27	15
Hoch	0	0	0	1	0
Mäßig	0	0	0	2	5
Niedrig	0	0	0	0	0
Unwahrscheinlich	0	75	126	72	16

Farben zeigen Risikostufen an, Zahlen die Anzahl der Sicherheitsrichtlinien.

Die Risikomatrix verfügt über eine X- und eine Y-Achse; für jedes X/Y-Segment wird die Anzahl der relevanten Sicherheitsrichtlinien angezeigt. Entsprechend wird Sicherheitsrichtlinien mit hohen Risikoauswirkungen und hoher Risikowahrscheinlichkeit die Risikostufe „Hoch“ zugewiesen.

Beheben von Fehlkonfigurationen

Anleitungen zur Problembehebung

Bei der manuellen Bereitstellung von Cloud-Infrastrukturen ist eine regelmäßige Aktualisierung der Anleitungen zur Konfiguration und Problembehebung erforderlich, damit die Einhaltung sämtlicher im unternehmenseigenen Standard enthaltenen Sicherheitsrichtlinien gewährleistet werden kann. Zscaler CSPM stellt benutzerfreundliche Schritt-für-Schritt-Anleitungen zur Problembehebung – nach Möglichkeit mithilfe von Kommandozeilen oder Scripts über die Konsole des Cloud-Anbieters – bereit.

Automatische Problembehebung

Bei bestimmten Fehlkonfigurationen in Produktivumgebungen dauert es womöglich zu lange, bis ein Ticket der zuständigen Person zugewiesen bzw. durch diese das Problem behoben werden kann. Bei kritischen Sicherheitsproblemen ist eine sofortige Behebung erforderlich.

Zu diesem Zweck stellt Zscaler CSPM Richtlinien zur automatischen Problembehebung bereit, die bei Initiierung einer Änderung durch den Kunden (z. B. neue Bereitstellung oder manuelle Änderungen an der Konfiguration über die Konsolen des Cloud-Anbieters) augenblicklich ausgelöst werden. Zscaler CSPM stellt eine Governance-Ebene bereit, auf der Kunden Hunderte von Richtlinien zur automatischen Problembehebung zur Auswahl stehen. Nachdem diese Richtlinien in der Vorproduktion getestet wurden, können sie in Produktivumgebungen durchgesetzt werden.

Automatische Bereitstellung

Es ist wichtig, Fehlkonfigurationen zuverlässig zu erkennen, und ebenso wichtig ist es, dafür zu sorgen, dass sie in Produktivumgebungen gar nicht erst auftreten. Unternehmen, die Cloud-Infrastrukturen manuell bereitstellen, sollten die Bereitstellung für alle kritischen Ressourcen automatisieren.

Zscaler CSPM stellt QuickWin-Scripts und Empfehlungen zur Automatisierung bereit. Den Unternehmen wird empfohlen, ein zentrales Repository für die automatische Bereitstellung zu erstellen. Sobald die Bereitstellung der kritischen Ressourcen automatisiert wurde, kann das Unternehmen die Umstellung auf komplette DevSecOps-Automatisierung in Angriff nehmen.

Integration mit Ticketsystemen

Zscaler CSPM lässt sich mit den Ticketsystemen der Kunden integrieren, sodass Fehlertickets automatisch generiert und dem zuständigen CloudOps-Mitarbeiter zugewiesen werden. Diese Fehlertickets enthalten wichtige Angaben zu nicht-konformen Ressourcen sowie entsprechende Anleitungen zur Problembehebung. Zur Unterstützung des CloudOps-Teams weist Zscaler CSPM den Fehlertickets automatisch eine Priorität zu. Ein Administrator für Zscaler CSPM kann die Häufigkeit der automatischen Ticketerstellung konfigurieren bzw. reduzieren (z. B. nie, täglich, wöchentlich, monatlich usw.).

DevOps-Integration

Unternehmen, die Prozesse zur Sicherheits- und Konformitätsüberwachung ihrer Cloud-Infrastrukturen implementieren, merken schnell, das manuelle oder halbautomatische Bereitstellungen nach wie vor anfällig für menschliche Fehler sind.

Die Mehrzahl der Unternehmen steigt auf Automatisierung um, um ihre Releasezyklen zu beschleunigen. Durch häufige Änderungen kann es leicht passieren, dass bisherige Sicherheitsmaßnahmen unwirksam werden. Zur Gewährleistung einer kontinuierlichen Verbesserung der Sicherheitsmaßnahmen werden die entsprechenden Validierungen zunehmend in CI/CD-Pipelines (Continuous Integration/Continuous Delivery) integriert.

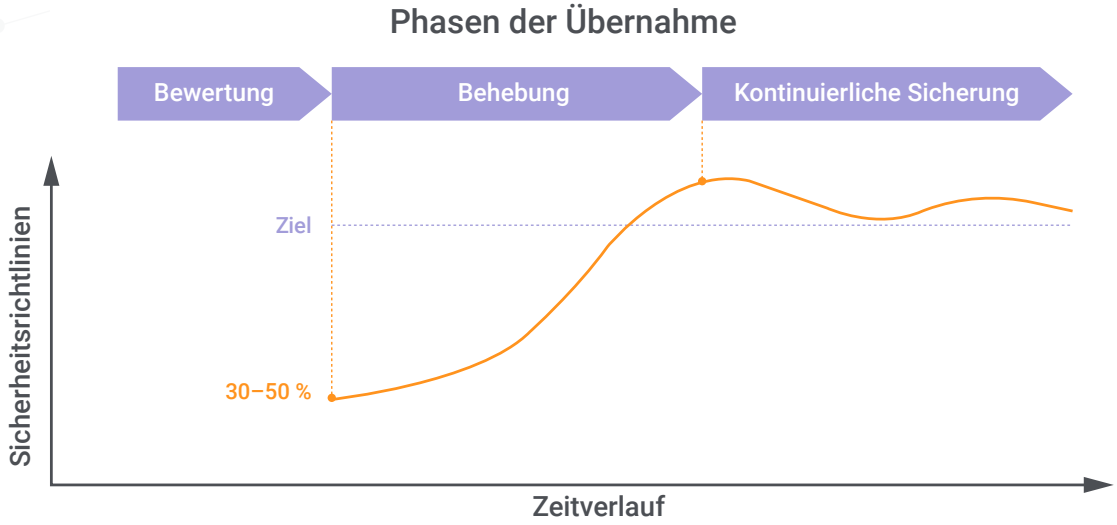
Zscaler CSPM unterstützt alle erforderlichen CI/CD-Integrationen. Das Onboarding neu erstellter Cloud-Konten erfolgt automatisch. Zur Initiierung von Sicherheitsscans und der Abfrage des Sicherheits- und Konformitätsstatus können entsprechende Anfragen abgeschickt werden. Anhand einer automatischen Analyse kann entschieden werden, ob eine Bereitstellung weiterhin in der Produktivumgebung eingesetzt wird. Diese DevSecOps-Funktionen stehen im Einklang mit der beabsichtigten Verlagerung der Sicherheitsüberwachung in frühere Entwicklungsstadien.

CSPM als teamübergreifende Aufgabe

Schrittweise Umstellung

Bewertung des Sicherheitsstatus

Unternehmen setzen CSPM-Lösungen zur Erfüllung der Nachweispflicht auf der Grundlage gängiger Cybersicherheits-Frameworks wie CIS oder NIST ein. In regulierten Branchen unterstützen sie branchenspezifische Compliance-Frameworks wie HIPAA für das Gesundheitswesen, SOC 2 für ISVs, PCI DSS für den E-Commerce, ISO 27001 für international tätige Unternehmen und FFIEC für Finanzdienstleistungen



CSPM-Lösungen können zur Bewertung der vorhandenen Cloud-Infrastruktur und Ermittlung des aktuellen Sicherheitsstatus eingesetzt werden. Im Normalfall wird dann in Zusammenarbeit mit dem InfoSec-Team ein Projekt zur Identifizierung unbedingt erforderlicher Sicherheitsrichtlinien und Behebung auftretender Probleme initiiert.

Problembehebung zur erfolgreichen Umsetzung

Für die Problembehebung müssen CloudOps-Teams in Best Practices und neuen Konfigurationsanforderungen geschult werden. Problembehebungen werden zunächst in Vorproduktionsumgebungen validiert, um sicherzustellen, dass sie weder Anwendungen beschädigen noch die Performance beeinträchtigen. Entwicklungs-, Test- und Vorproduktionsumgebungen werden in Übereinstimmung mit dem erwünschten Sicherheitsstatus neu konfiguriert. Dadurch werden die Ziele der Sicherheitsmaßnahmen erreicht oder übertroffen.

Laufende Überwachung

Nach der Problembehebung übernehmen CloudOps-Teams die Verantwortung für die laufende Sicherheits- und Konformitätsüberwachung. Der Sicherheitsstatus der Produktivumgebung wird täglich überwacht, um sicherzustellen, dass durch kurzfristige Fehlerkorrekturen oder Aktualisierungen keine Fehlkonfigurationen entstanden sind.

In Entwicklungs-, Test- und Vorproduktionsumgebungen kommen die Tools zur Sicherheitsüberwachung ebenfalls laufend zum Einsatz, um neue Anwendungsversionen vor der Freigabe auf Fehlkonfigurationen zu prüfen.

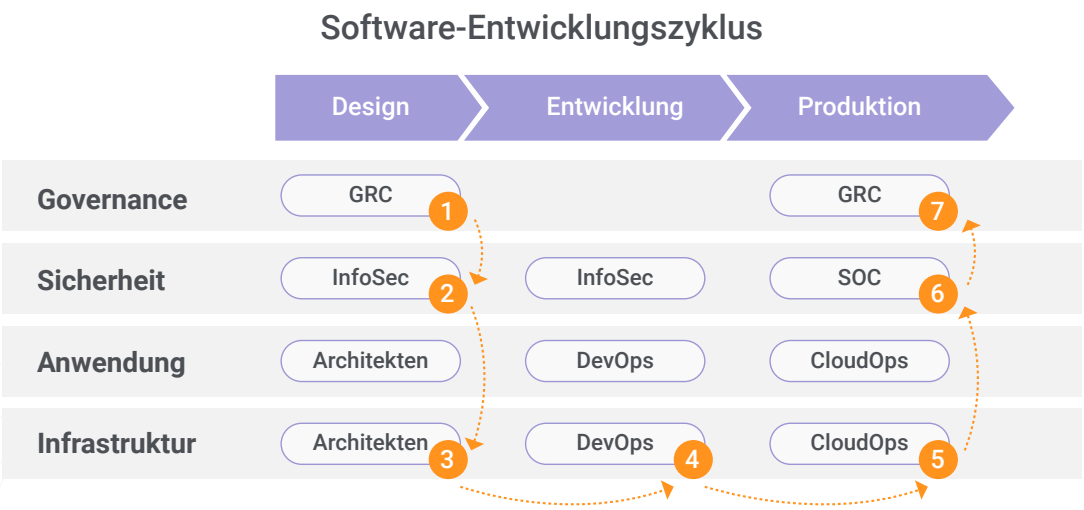
SOC-Teams sollten die Überwachung der Sicherheitsmaßnahmen in ihre Dashboards integrieren und kritische Fehlkonfigurationen in der Produktivumgebung schnellstmöglich eskalieren.

Abteilungsübergreifende Zusammenarbeit

Durch Implementieren eines CSPM verbessert sich die Zusammenarbeit zwischen InfoSec-, SOC und AppDev-Teams. Zwar liegt die Verantwortung für die Definition des Unternehmensstandards als Zielvorgabe beim InfoSec-Team. Die Umsetzung entsprechender Sicherheits- und Konformitätsstandards ist jedoch Aufgabe der für Anwendungsentwicklung und Infrastrukturverwaltung zuständigen Teams.

Der CSPM-Prozess umfasst folgende Schritte:

1. GRC gibt Compliance-Frameworks vor
2. InfoSec legt Unternehmensstandards für Datensicherheit fest
3. Cloud-Architekten erstellen sichere Konfigurationen für die Anwendungsarchitektur
4. DevOps implementiert Cloud-Infrastruktur
5. CloudOps behebt alle erkannten Fehlkonfigurationen
6. SOC überwacht Sicherheitsmaßnahmen
7. GRC erbringt Nachweis für dauerhafte Compliance



GRC: Compliance-Frameworks

GRC-Teams geben die jeweils erforderlichen Compliance-Frameworks vor (Branchenstandards, gesetzliche und aufsichtsrechtliche Vorschriften). Zscaler CSPM unterstützt verschiedene Compliance-Frameworks, und basierend auf Kunden-Anforderungen wird die Auswahl laufend erweitert.

InfoSec: Unternehmensstandard

Das InfoSec-Team ist für die Festlegung der unbedingt erforderlichen Sicherheitsrichtlinien für das Unternehmen zuständig. Hierzu zählen Cybersicherheitsstandards ebenso wie zusätzliche unternehmensspezifische Richtlinien. Zudem bietet Zscaler CSPM die Option zur Ergänzung unternehmenseigener Standards, deren Einhaltung von den Kunden nachverfolgt und durchgesetzt werden kann.

Cloud-Architekten: Konfigurationsanleitungen

Systemarchitekten planen die Cloud-Infrastruktur unter Berücksichtigung einschlägiger Best Practices und erstellen Anleitungen zur sicheren Konfiguration für CloudOps-Teams. Zscaler CSPM stellt detaillierte Definitionen für sämtliche Sicherheitsrichtlinien sowie Schritt-für-Schritt Anleitungen zur Konfiguration und Problembehebung bereit.

DevOps: Bereitstellen der Infrastruktur

In vielen Unternehmen werden Cloud-Infrastrukturen manuell von einem eigens dafür zuständigen Team bereitgestellt, bei anderen erfolgt die Bereitstellung der Cloud-Infrastrukturen automatisch und fällt in die Zuständigkeit des DevOps-Teams. In jedem Fall wird die Cloud-Infrastruktur vom jeweils zuständigen Team in der Vorproduktionsumgebung mithilfe von Zscaler CSPM gescannt. Sämtliche dabei erkannten Fehlkonfigurationen müssen vor Bereitstellung in der Produktivumgebung behoben werden. Die vollautomatisierte Variante wird im weiteren Verlauf dieses Dokuments im Abschnitt „DevSecOps“ beschrieben.

CloudOps: Beheben von Fehlkonfigurationen

Das CloudOps-Team initiiert unmittelbar nach der Bereitstellung für die Produktivumgebung einen Scan. Wenn die bereitgestellte Cloud-Infrastruktur den erforderlichen Standards entspricht, kann sie in der Produktivumgebung eingesetzt werden. Das CloudOps-Team ist zudem für die Planung der täglichen Scans der Cloud-Infrastruktur zuständig. Alle dabei erkannten Fehlkonfigurationen sind je nach Priorität und Risikostufe möglichst schnell zu beheben.

SOC: Laufende Überwachung

Zur Validierung manueller Konfigurationsänderungen sollten Produktivumgebungen täglich gescannt werden. SOC-Teams überwachen die Infrastruktur auf Abweichungen und eskalieren kritische Fehlkonfigurationen, die eine sofortige Behebung erforderlich machen.

GRC: Konformitätsnachweise

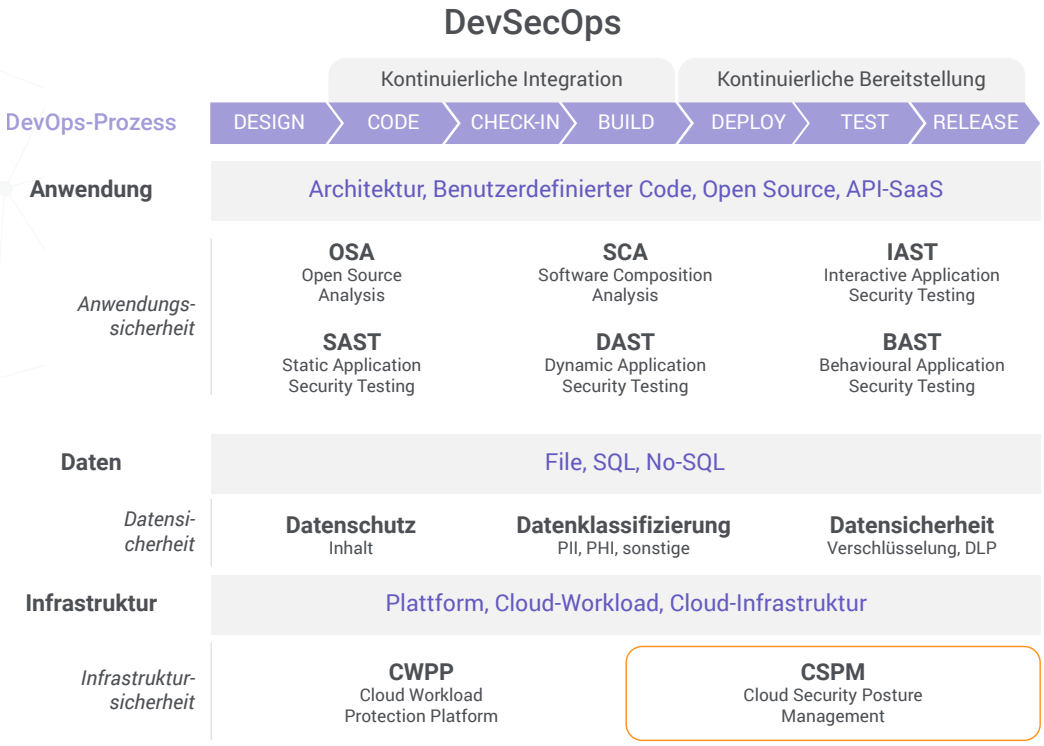
Compliance-Teams haben Zugriff auf tägliche Überwachungsberichte, die Aufsichtsbehörden und Prüfern als Konformitätsnachweise vorgelegt werden können.

Umsetzung von DevSecOps

Anwendungsbereiche für DevSecOps

Anwendungssicherheit: Der Begriff DevSecOps bezeichnet in der Regel die Integration von Sicherheitsvorkehrungen in den Produktentwicklungszyklus neuer Anwendungen. Mithilfe von Tools wie Static Application Security Testing (SAST) bzw. Dynamic Application Security Testing (DAST) werden Best Practices für die Programmierung überwacht, Sicherheitsprobleme erkannt und Fehler protokolliert. Zur Überprüfung der Sicherheit des Anwendungscodes vor der Freigabe für die Produktivumgebung werden Penetrationstests durchgeführt. Zudem können Selbstschutzmechanismen für Laufzeit-Anwendungen implementiert werden.

Datensicherheit: Mit Inkrafttreten der DSGVO wurde der Datensicherheit ein noch höherer Stellenwert eingeräumt. Verfahren zur Gewährleistung des Datenschutzes, Datenklassifizierung und Datensicherheit müssen im Rahmen von DevSecOps in der Vorproduktionsumgebung validiert werden.



Cloud-Infrastruktur: Cloud-Infrastruktur wird von einem Cloud-Anbieter bezogen; ihre Bereitstellung und Konfiguration kann mit Infrastructure as Code (IoC) erfolgen. Landläufig weniger bekannt ist, dass die Konfiguration von Cloud-Infrastruktur auch einen integralen Bestandteil des DevSecOps-Modells bildet.

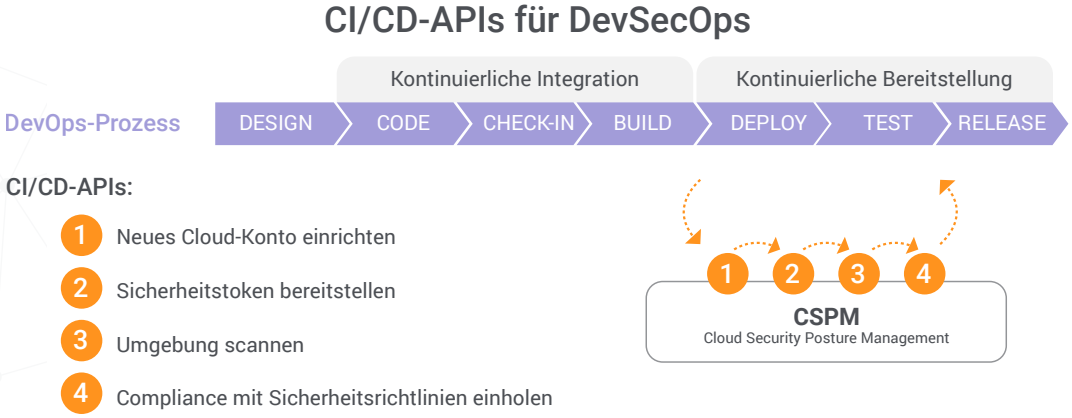
Letztlich kommen Unternehmen nicht um die Umstellung auf einen integrierten DevSecOps-Prozess herum, der die übergreifende Umsetzung und Überwachung sicherheitsrelevanter Best Practices für Anwendungen, Daten und Infrastruktur umfasst. Damit Fehlkonfigurationen bereits in Vorproduktionsumgebungen erkannt werden und gar nicht erst in die Produktivumgebungen gelangen, ist die Verlagerung der Sicherheitsmaßnahmen in frühere Entwicklungsstadien erforderlich.

Mit der Integration von automatischer Bereitstellung in die CI/CD-Pipeline wird die Validierung von Infrastruktur-Konfigurationen anhand von Best Practices für die Cloud-Sicherheit unbedingt erforderlich. Entsprechend müssen CSPM-Produkte relevante APIs bereitstellen, die von CI/CD-Pipelines abgerufen werden können.

Erforderliche CI/CD-APIs

CSPM-Produkte müssen sämtliche Schritte im Rahmen von End-to-End-Prozessen unterstützen:

1. Einrichten eines neuen Cloud-Kontos
2. Bereitstellen des Sicherheitstokens
3. Scannen der (Entwicklungs-, Test - oder sonstigen) Umgebung
4. Automatische Auskunft über Einhaltung oder Nicht-Einhaltung von Sicherheitsrichtlinien zum Abgleich mit den Unternehmensstandards



Nach dem Bau der Umgebung können DevOps-Teams über die CI/CD-APIs von Zscaler eine automatische Wiederholung des Scanvorgangs initiieren und erhalten dadurch Auskunft über den Compliance-Status für sämtliche Sicherheitsrichtlinien. Teams können die Ergebnisse des Scans auswerten und ihre IOC-Repositorien gemäß den Konfigurationsstandards aktualisieren. Zur Unterstützung dieser Aufgaben stellt Zscaler CSPM Anleitungen zur Problembehebung bereit.

Zscaler CSPM

Zscaler CSPM stellt Unternehmen ein breites Spektrum an Innovationen und Produktfunktionen für die automatische Überwachung von Sicherheit und Compliance in der Cloud, Gewährleistung ständiger Transparenz und Durchsetzung von Sicherheitsrichtlinien und aufsichtsrechtlichen Vorgaben im branchenweit größten Umfang bereit. Das Produkt wird als Multi-Tenant-SaaS angeboten. Kunden profitieren von nahtloser Integration mit der jeweiligen Cloud-Infrastruktur, schneller Datenerfassung sowie umfassenden Dashboards und Berichten. Zscaler CSPM unterstützt Integrationen mit CI/CD-Pipelines und Ticketsystemen, automatische Problembehebung und unternehmensspezifische Standards. Die übergreifende Durchsetzung unternehmensspezifischer Standards in AWS-, Azure und Office365-Umgebungen zur Verhinderung von Datenschutzverletzungen infolge von Fehlkonfigurationen ist problemlos möglich.

Marktführer

Zscaler CSPM automatisiert die übergreifende Überwachung von über 1.500 Sicherheitsrichtlinien und 13 Compliance-Frameworks in AWS-, Azure und Office365-Umgebungen. Darüber hinaus ermöglicht das Produkt die Erstellung unternehmensspezifischer Standards, unterstützt sehr umfangreiche Anwendungsumgebungen und gewährleistet die schnelle Umsetzung von DevSecOps-Verfahren.

Beheben von Fehlkonfigurationen

Fehlkonfigurationen der Cloud-Infrastruktur stellen das größte Sicherheitsrisiko für Cloud-Anwendungen dar. Durch Automatisierung der Sicherheits- und Konformitätsüberwachung für Cloud-Anwendungen können Unternehmen ihre Cybersicherheitsrisiken beträchtlich reduzieren und ihrer Nachweispflicht gegenüber den Aufsichtsbehörden einfacher nachkommen.

Implementieren von DevSecOps

Manuelle Prozesse zur Überwachung der Sicherheit und Konformität können mit der Dynamik von Cloud-Umgebungen nicht mithalten. Zscaler CSPM ist Branchenführer in Bezug auf den Umfang der bereitgestellten Sicherheitsrichtlinien und ermöglicht eine schnelle und unkomplizierte API-basierte Integration mit DevSecOps-Tools.

Beschleunigter Ausbau der Cloud-Nutzung

Die zuverlässige Überwachung von Sicherheit und Konformität ist Voraussetzung für einen schnelleren Ausbau der Cloud-Nutzung. Dadurch wird eine zügigere Umsetzung von Initiativen zur digitalen Transformation möglich, was Unternehmen, die auf Zscaler CSPM setzen, einen deutlichen Wettbewerbsvorteil verschafft.

Umstellung auf digitale Governance

CSPM ist ein entscheidender erster Schritt bei der Transformation der Funktionen zur Gewährleistung von Sicherheit, Risikomanagement und Datenschutz in dynamischen Cloud-Umgebungen. Digital ausgerichtete Unternehmen profitieren von automatisierten Governance-Prozessen.

Weitere Informationen finden Sie unter zscaler.com/CSPM

Über Zscaler

Zscaler ermöglicht weltweit führenden Organisationen die sichere Transformation ihrer Netzwerke und Anwendungen für eine mobile und Cloud-orientierte Welt. Zscaler Internet Access™ und Zscaler Private Access™, die Aushängeschilder des Unternehmens, stellen schnelle, sichere Verbindungen zwischen Benutzern und Anwendungen unabhängig von Gerät, Standort oder Netzwerk her. Die Services von Zscaler werden zu 100 % in der Cloud bereitgestellt und bieten Einfachheit, erhöhte Sicherheit und eine verbesserte Benutzererfahrung. Herkömmliche Systeme oder Hybridlösungen können dabei nicht mithalten. Zscaler betreibt eine mandantenfähige dezentrale Cloud-Sicherheitsplattform, die Tausende von Kunden in mehr als 185 Ländern vor Cyberangriffen und Datenverlusten schützt. Informieren Sie sich unter zscaler.com oder folgen Sie uns auf Twitter @zscaler.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134, USA
+1 408 533 0288
www.zscaler.com