CyberCompare Whitepaper

Cybersicherheit in der Cloud – wie sehen sinnvolle erste Schritte aus?

Cloud Computing ist zweifellos einer der wichtigsten Trends der vergangenen zehn Jahre. Schätzungen zufolge werden die Ausgaben von Endnutzern für Cloud Computing bis 2025 600 Mrd. USD erreichen; die meisten Rechenzentren von Unternehmen werden vermut¬lich bis 2025 in die Cloud wechseln.

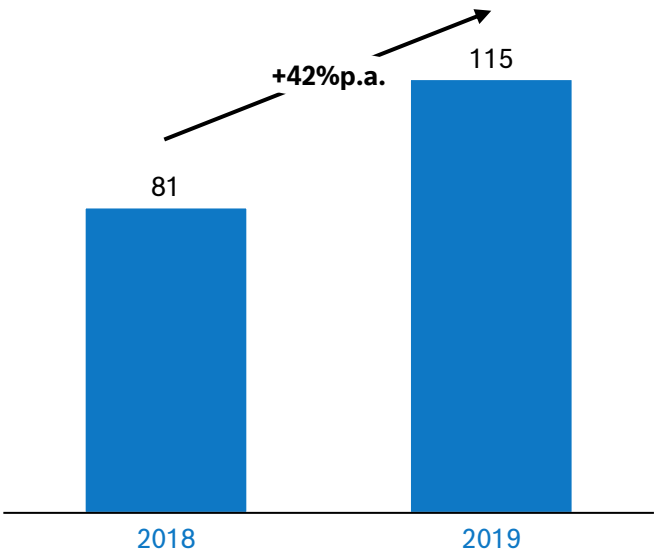
Vorstände und Entscheidungsträger aus der IT beobachten die Kosten und Prozesse einer Migration in eine Cloud mit Sorge. Den Risiken, die damit einhergehen, schenken sie dagegen deutlich weniger Aufmerksamkeit. Fälschlicherweise wird häufig angenom-men, dass sich Cloud-Anbieter auch sämtlicher Cybersicherheitsrisiken annehmen und diese lösen. Jüngste Erkenntnisse zeigen jedoch, dass 45% aller Datenschutzverlet-zungen mit Vorfällen in der Cloud zusammenhängen.

Daher erfordert die Migration in die Cloud einen neuen Sicherheitsansatz. In diesem Whitepaper legen wir dar, welche Cloud-Sicherheitskompetenzen benötigt werden und wie die Anbieter unterschiedlicher Cloud-Sicherheitslösungen Ihnen helfen können, Ihre Cloud zu schützen.

1. https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022
2. https://www.ibm.com/security/data-breach

Cloud-Sicherheit – aktiv steuern statt vollständig outsourcen

Security-Vorfälle, die auf Cloud-Fehlkonfigurationen zurückzuführen sind



> **Bis 2025 sind 99% der Cloud-Security-Fehler die Schuld des Kunden** und nicht die des Dienstleisters.
>
> **Gartner**

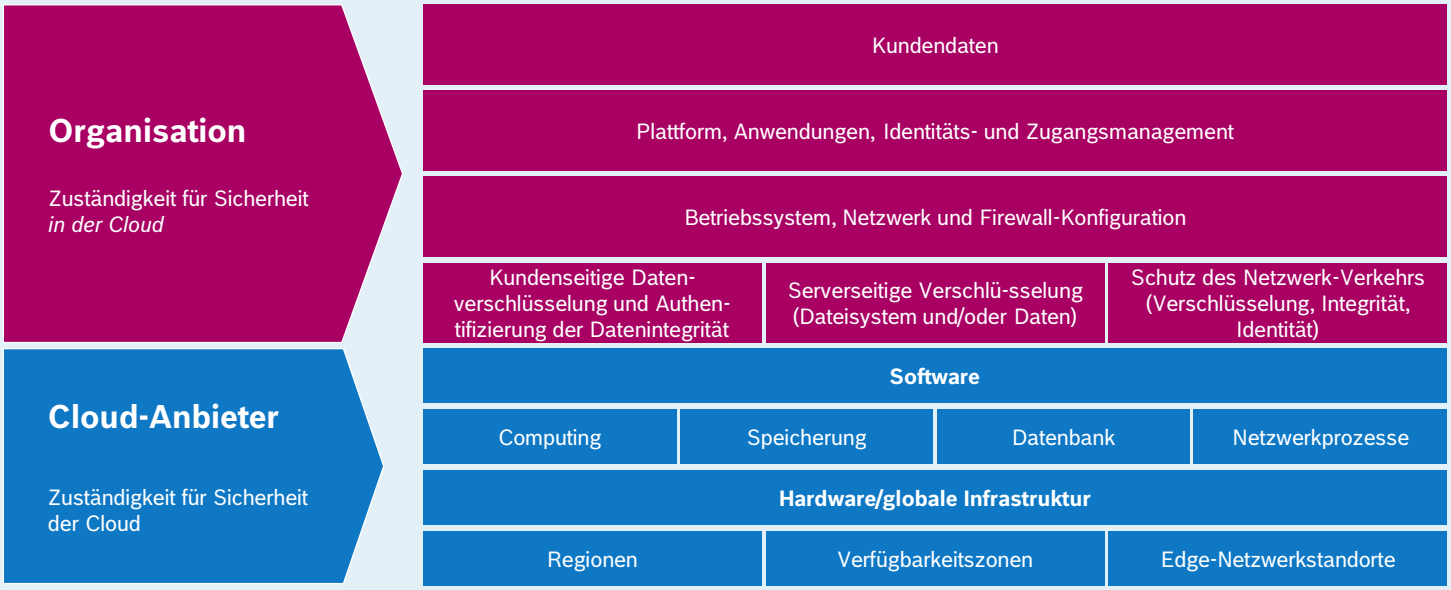
Das grundlegende Prinzip von Cloud Computing ist es, die Computing-Infrastruktur und Wartung outzusourcen und bei Bedarf sofortigen Zugang zu Ressourcen zu haben. Häufig geht dieses Prinzip mit einer irrtümlichen Annahme einher: So beobachten wir, dass Unternehmen, die auf eine Cloud-Infrastruktur migriert sind, davon ausgehen, dass sie damit auch automatisch ihre „Sicherheit“ outgesourct haben. Dabei trifft es nicht zu, dass Cloud-Anbieter auch die volle Verant¬wortung für den Schutz der Systeme übernehmen.

Häufig sind sich Organisationen ihrer eigenen Zuständigkeiten nicht bewusst. So ist es wenig überraschend, dass Fehl¬konfigurationen in der Cloud das größte Risiko in Bezug auf einen erfolgreichen Cyberangriff darstellen. Ein angemesse¬ner Umgang mit Schwachstellen in Cloud-Konfigurationen hätte zahlreiche Cloud-Cyberangriffe verhindern können – in allen Branchen und Regionen, die zum Opfer wurden.

Laut jüngster Medienberichte erlitt z.B. die Cyber-Analytics-Firma Cognyte im Jahr 2021 einen Cloud-basiertn Cybervorfall, von der mehr als 5 Mio. Kundenakten betroffen waren. Grund war eine ungesicherte Cloud-Datenbank ohne Authentifizierungsprotokolle. Ein weiteres Beispiel: Bei einer gemeldeten Cyberattacke auf die Choice Hotel Group wurde Zugang zu 700.000 Akten mit Reservierungsinformationen erlangt[2] (unter anderem hochsensible personenbezogene Informationen sowie Kreditkarten-informationen). In diesem Fall war die Ursache eine mangelhafte Konfiguration, die den öffentlichen Zugang zur Cloud-Datenbank zuließ.

Es bedarf eines neuen Sicherheitsansatzes. Aber wie sollte dieser aussehen? Zunächst einmal sollte geklärt werden, bei wem welche Verantwortung liegt. Organisationen müssen ihre Zuständigkeiten für Sicherheit, ihre Rolle bei der Konfiguration und auch die Zuständigkeiten ihrer Cloud-Anbieter kennen. Wichtig dabei: Die Sicherheit lässt sich nicht vollständig an externe Anbieter outsourcen – ganz gleich, wie das Servicemodell aussieht.

Cloud-Anbieter entwerfen in der Regel ein Modell, bei dem die Zuständigkeiten gemeinsam beim Anbieter und bei der Organisation liegen. Die Steuerung der beim Anbieter gekauften Computing-Ressourcen ist alleiniger Zuständigkeitsbereich der beauftragenden Organisation. Führende Cloud-Anbieter wie AWS skizzieren die Zuständigkeitsprinzipien in Schichten und unterscheiden dabei zwischen der Sicherheit in der Cloud und der Sicherheit der Cloud:



Quelle: https://aws.amazon.com/compliance/shared-responsibility-model/

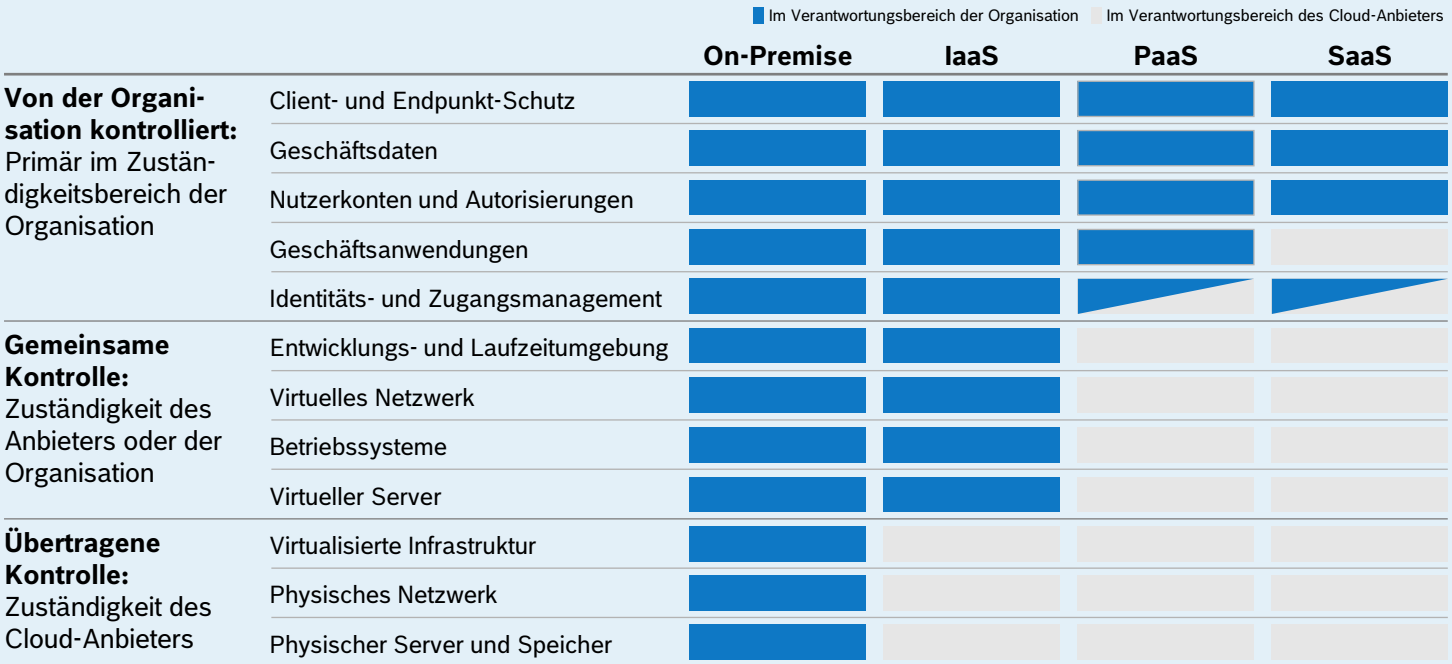
Sicherheit *in der Cloud*: Die Zuständigkeit der Organisation für Sicherheit hängt von den Cloud-Services ab, für die sich die Organisation entscheidet. Diese bedingen den Umfang der Konfigurationsarbeiten, die die Organisation im Rahmen ihrer Abläufe vornehmen muss. Organisationen sind z.B. verantwortlich für das Management ihrer Daten (z.B. Verschlüsselungsoptionen), die Klassifizierung ihrer Assets und den Einsatz von IAM-Tools zur Definition und Vergabe relevanter Genehmigungen.

Sicherheit *der* Cloud: Der Cloud-Anbieter ist zuständig für den Schutz der Infrastruktur, auf der alle in der Cloud angebotenen Services laufen. Dies umfasst Hardware, Software, Networking und die Räumlichkeiten, in denen die Cloud-Services betrieben werden.

1. https://www.comparitech.com/blog/information-security/breach-database-leak/
2. https://www.securitymagazine.com/articles/90733-choice-hotels-suffers-data-breach-exposing-700000-customer-records

Rolle und Zuständigkeiten der Organisation je nach Cloud-Deployment-Modell

Cloud-Services gehen mit unterschiedlichen Deployment-Modellen einher. Da die Serviceangebote je nach Modell voneinander abweichen, gilt dies auch für die Zuständigkeit für Sicherheit. Als Faustregel gilt: Der Cloud-Anbieter übernimmt lediglich die Verantwortung für die Services; die Organisation kann keine Änderungen vornehmen. In der Kategorie „Infrastructure as a Service“ z.B. kümmert sich ein Cloud-Anbieter um das physische Netzwerk, die Server, die Speicher sowie die virtuelle Infrastruktur, die die Cloud für Private und Public Cloud Deployments nutzt. Die jeweiligen Modelle und Zuständigkeiten für die Sicherheit können wie folgt dargestellt werden:



Quelle: https://cloudsecurityalliance.org/blog/terms/shared-responsibility-model/

Software as a Service (SaaS)

In einem SaaS-Kontext sind sich Unternehmen häufig nicht ihrer Zuständigkeiten für Sicherheit bewusst – auch bei einem vollständig gemanagten Service. Dabei sind sie zuständig für Datenbackups, Verschlüsselung, Identitäts- und Zugangsmanagement sowie Client- und Endpunktsicherheit.

Platform as a Service (PaaS)

Ein PaaS-Kontext ermöglicht Organisationen den Fokus auf ihre Anwendungen – die Ursache für viele größere Sicherheitsprobleme. Zusätzlich zu den Zuständigkeiten, die sich aus dem SaaS-Kontext ergeben, gehören zum Verantwortungsbereich der Orga-nisation die Vorbeugung von Datenverlust, das Identitäts- und Zugangsmanagement, die Sicherheit von Endpunkten und Webanwendungen sowie Firewalling und Verschlüsselung.

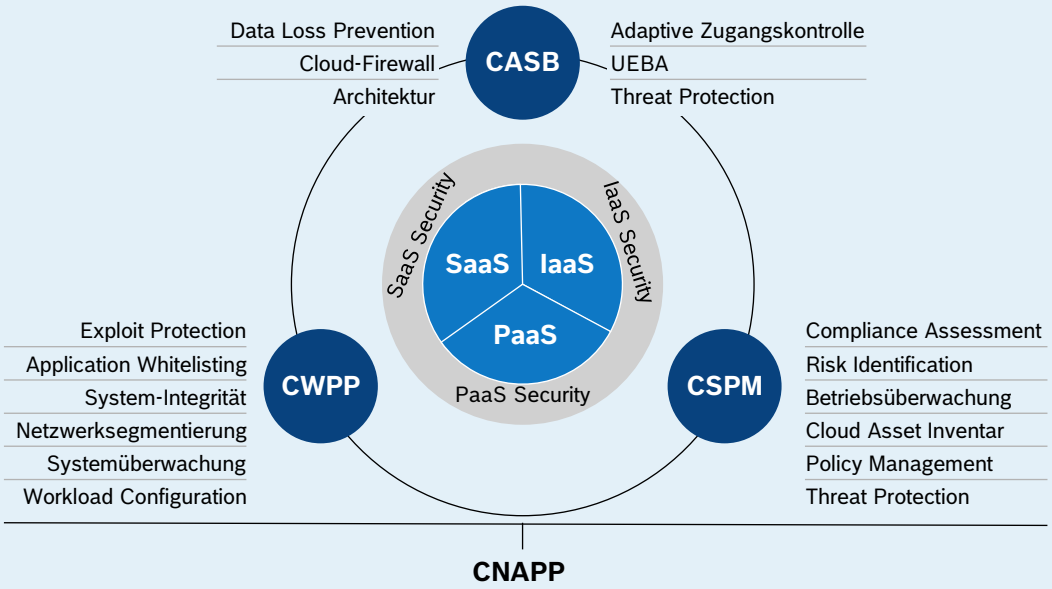
Infrastructure as a Service (IaaS)

In einem IaaS-Kontext müssen Organisationen außerdem die Verantwortung für Betriebssysteme, Middleware, die Prävention von Datenverlusten, die Verschlüsselung und das Firewalling der genutzten Plattformen sowie für Anwendungen und laufende Prozesse übernehmen.

Zusammengefasst bedeutet das für Sie: Bei der Migration aus einem traditionellen On-Premise-Kontext sollte die Cloud-Sicherheit oberste Priorität genießen. Alle Vorteile von Cloud Computing (wie Skalierbarkeit, geringere Nutzungskosten und maximale Flexibilität) werden angesichts des enormen Schadens, den eine erfolgreiche Cloud-Cyberattacke anrichtet, zunichte gemacht. Die gute Nachricht: Es gibt spezielle Tools, Systeme und Anbieter, die bei der Sicherung der Cloud helfen.

Wählen Sie Ihr Cloud-Security Tool Service- und Modell-basiert

Der Markt für Cybersicherheit wächst; zahlreiche Anbieter von Cloud-Sicherheitslösungen drängen in den hart umkämpften Sektor. Jeder neue Ansatz trägt zum Anstieg von Buzzwords bei und macht die Situation aus Sicht einer Organisation noch komplexer. Daher müssen sich Unternehmen vor der Auswahl eines Anbieters und Tools für Cloud-Sicherheit zunächst einen Überblick über den Anbietermarkt ver-schaffen. Im Folgenden möchten wir die verfügbaren Lösungen strukturiert und übersicht¬lich darstellen.



CASB
Cloud Security Access Broker (Cloud Firewall)

CWPP
Cloud Workload Protection Platform

CSPM
Cloud Security Posture Management

CNAPP
Cloud-Native Application Protection Platform (Kombinationslösung)

CASB: Cloud Access Security Broker

Ein CASB-Tool fungiert als Schnittstelle zwischen Verbrauchern und Anbietern von Cloud-Services und stellt sicher, dass die Richtlinien für Cloud-Sicherheit beim Zugriff auf Ressourcen befolgt werden. Wir betrachten CASB-Tools als grundlegende Tools zum Management von Sicherheit in der Cloud, allerdings mit einem stärkeren Fokus auf SaaS-Sicherheit. Sie können die Cloud-Nutzung granular überwachen und kontrollieren, sensible Daten schützen, vor Verlust bewahren und Schutz gegen Bedrohungen wie Malware bieten.

CWPP: Cloud Workload Protection Platform

CWPP ist eine Lösung zum Schutz von Server-Workloads in einer Public-Cloud-Infrastruktur. CWPP schützt in erster Linie durch Workload-Schutz vor Angriffen auf die Serviceverfügbarkeit, adressiert jedoch nicht die grundlegenderen Sicherheitsbedürfnisse. Dennoch ermöglicht CWPP die Erkennung von Schwachstellen sowie eine adäquate Reaktion bei Zwischenfällen im Zusammenhang mit Cloud-basierten Workloads.

CSPM: Cloud Security Posture Management

CSPM ist ein Tool, das sich primär auf die kontinuierliche Beurteilung und Überwachung der Compliance konzentriert, um Cloud-Sicherheitsrisiken zu steuern. Beim Management von Sicherheit in der Cloud durch höhere Sichtbarkeit, Richtlinienmanagement und priorisierte Warnmeldungen können CSPM-Tools einen wesentlichen Beitrag leisten. Die Hauptvorteile: mögliche Multicloud-Sichtbarkeit, maßgeschneiderte Sicherheitsrichtlinienkompetenzen, die Erstellung von Compliance-Berichten in Echtzeit sowie eine grundlegende Warnfunktion.

CNAPP: Cloud Native Application Protection Platform

CNAPP kombiniert die Kernfunktionen von CSPM- und CWPP-Lösungen. Der Haupt¬vorteil von CNAPP besteht darin, dass diese Lösung den kompletten Bedarf an Cloud-Anwendungssicherheit abdeckt und nicht nur ein Toolset verschiedener Lösungen ist.

Starten Sie Ihre Cloud-Sicherheits-Journey mit adäquaten CSPM-Richtlinien

Organisationen müssen verschiedene Kompetenzen entwickeln, um ihre Pläne für Cloud-Sicherheit auf den Weg zu bringen. Sieben grundlegende Kompetenzen sind erforderlich, um die wichtigsten Sicherheitsfunktionen in einer Cloud-Umgebung zu nutzen und Schutz vor den gängigsten Angriffsvektoren zu bieten.

Grundlegende Kompetenzen	Beschreibung	CSPM	CASB	CWPP	CNAPP[1]
Governance	Definition von Nutzergenehmigungen, Zugang, Sicherheitskontrollen und Leitlinien	✓			✓
Monitoring	Überwachung von Anwendungen, der Infrastruktur und des Netzwerks in Echtzeit	✓	✓	✓	✓
Protokollierung	Protokollierung aller Ereignisse, von Nutzeraktivitäten, Anwendungen oder Services in der Cloud	✓	✓		✓
Scanning	Identifizierung von Schwachpunkten und Lecks durch gezielte Scans	✓	✓	✓	✓
Warnungen	Warnung bei Richtlinienverstößen in Echtzeit	✓			✓
Auditing	Filterung, Speicherung und Verschlüsselung von Protokollen für Prüfzwecke	✓			✓
Compliance	Definition von Sicherheitsleitlinien für die Einhaltung der regulatorischen Vorgaben	✓	✓		✓

1. CNAPP: Deckt alle Funktionen ab, allerdings nur mit Fokus auf Schutz von Cloud-Native-Anwendungen

Die Übersicht zeigt, dass **CSPM-Tools sämtliche Basiskompetenzen abdecken**, während andere Optionen spezifischere Kompetenzen mitbringen

Kunden sollten zunächst auf CSPM setzen und darauf aufbauend weitere Cloud-Sicherheits-Tools aufnehmen

Von den vier oben genannten Lösungen stellt eine CSPM-Lösung aus unserer Sicht den besten Ausgangspunkt dar, um die Cloud-Sicherheitsfunktionen einer Organisation vollständig neu zu definieren. Ein CSPM bietet ein besonders umfassendes Spektrum an Grundlagenkompetenzen. Wir empfehlen Organisationen, bei der Entwicklung ihrer Cloud-Sicherheitsfunktion den Fokus auf die Basiskompetenzen zu setzen und im ersten Schritt eine CSPM-Lösung einzuführen. Anschließend können sie ihre Cloud-Sicherheitskompetenzen ausweiten – mit Hilfe eines Multipurpose-Anbieters, der mittel- bis langfristig sowohl CSPM- als auch CASB-Fähigkeiten und -Kapazitäten bereitstellen kann.

Allerdings entbindet eine CSPM-Lösung Organisationen nicht von der Pflicht, ihre Cloud-Sicherheit selbstständig zu steuern und zu konfigurieren. Cloud-Sicherheit auf Richtlinienebene ist und bleibt die Zuständigkeit der Organisation. Die Organisation muss je nach Risikoappetit, Risiken und Sicherheitszielen adäquate Sicherheitsrichtlinien entwickeln und durchsetzen. Eine angemessene Definition und Steuerung der Richtlinien ist essenziell, um die umfassenden Basiskompetenzen einer CSPM-Lösung zu nutzen. Generell sollten die geltenden Richtlinien für eine CSPM-Lösung auf der Basis von drei Kernelementen entwickelt und definiert werden:

Kompetenzen von CSPM-Anbietern

Bei der Umsetzung und Durchsetzung der Richtlinien müssen die Serviceumfänge von CSPM-Tools berücksichtigt werden, da sie durch die technischen Fähigkeiten eingeschränkt sein könnten.

Existierende Sicherheitsrichtlinien

On-Premise-Sicherheitsricht-linien sollten als Referenzpunkt für Entscheidungen zur Cloud-Sicherheit dienen, allerdings angepasst an Cloud-spezifische Risiken, Bedrohungen und technische Nuancen.

Input von Cloud-Teams/-Anbietern

Die Mitglieder von Cloud-Teams (z.B. Operations, Engineering) verfügen über Erfahrungswerte und können Einblicke in Risiken und Bedrohungen in der Cloud-Umgebung von Klienten geben. Die Anbieter können auf Basis gängiger Praktiken in der Branche Empfehlungen zu Richtlinien abgeben.

Wählen Sie Ihr passendes CSPM-Tool basierend auf 5 Kriterien

Selbst wenn der Markt nur auf CSPM-Anbieter eingegrenzt wird, kommen mehrere Kandidaten in Frage. Anbieter wie Zscaler, Orca und Trend Micro haben in den vergangenen Jahren ein breites Kompetenzspektrum mit unterschiedlichen Schwer-punkten entwickelt. Wir sehen eine Reihe von Kriterien, die Organisationen dabei helfen können, einen passenden Anbieter zu identifizieren bzw. ungeeignete Anbieter auszuschließen:

1. Wichtigste technische Kompetenzen

Für eine maximale Risikominderung sollte der Anbieter die wichtigsten technischen Kompetenzen abdecken: die Überwachung anormalen Verhaltens und Compliance-Reporting.

2. Kompatibilität mit der existierenden Infrastruktur

Um sämtliche Optionen und Kompetenzen in der IT-Umgebung auszuschöpfen, ist die Kompatibilität mit der vorhandenen und geplanten Cloud- und Sicherheitsinfrastruktur einer Organisation von Bedeutung. Zudem sollte das CSPM-Tool in die bestehenden SIEM-/XDR-Tools integriert werden können, um Logdaten-Quellen und Über-wachungskompetenzen zu ergänzen.

3. Komplexität der Implementierung und Abläufe

Der Anbieter sollte in der Lage sein, die CSPM-Lösung selbstständig zu implementieren. Gleichzeitig sollte die Organisation die Lösung unabhängig betreiben können, ohne auf zu viel Unterstützung durch den Anbieter angewiesen zu sein. Auch ein Abgleich der erforderlichen Implementierungsdauer mit der Sicherheits-Roadmap der Organisation sollte erfolgen.

4. CSPM Assessment Fähigkeiten

Die Organisation sollte die Fähigkeiten eingesetzter CSPM-Anbieter laufend evaluieren – während der geplanten Assessments sowie ereignisbasiert auf Abruf. Wichtig dabei ist der Verbleib der Daten innerhalb der Organisation.

5. Möglichkeit eines kurzfristigen Anbieterwechsels

Auf Grund der unterschiedlichen Kompetenzen der Anbieter CSPM-Markt sollte eine Organisation die Flexibilität beibehalten, jederzeit zu einem fortschrittlicheren Anbieter wechseln zu können.

Wir empfehlen Organisationen dringend, die verfügbaren Anbieter im Vorfeld anhand dieser Kriterien zu filtern, um den Auswahlprozess des passenden Anbieters möglichst effizient, also mit begrenztem Ressourcenbedarf und Zeitaufwand, zu gestalten. Organisationen haben trotzdem immer noch die Qual der Wahl. Eine Ausschreibung mit einem Vergleich einzelner Anbieter in einem sich rasch entwickelnden Markt kann extrem aufwendig und ermüdend sein. CyberCompare unterstützt Sie gerne bei der Spezifizierung Ihrer Anforderungen, bei Budgetüberlegungen, beim Einholen von Angeboten (falls gewünscht auch anonym) sowie bei deren Vergleich und bietet so eine solide Entscheidungsgrundlage. Wir freuen uns auf Ihre Anfrage.

Die wichtigsten Erkenntnisse

Bei der Migration in eine Cloud stellt die Cloud-Sicherheit einen der wichtigsten Aspekte dar. Alle Vorteile von Cloud Computing wie Skalierbarkeit, geringere Nutzungskosten und maximale Flexibilität werden angesichts des enormen Schadens, den eine erfolgreiche Cloud-Cyberattacke anrichtet, zunichte gemacht.

Abhängig von ihrer jeweiligen Situation bei der Migration in die Cloud ist es für Organisationen extrem wichtig, das richtige Tool und den richtigen (Service-) Anbieter zu wählen. Wir empfehlen als Ausgangspunkt die definierten grundlegenden Auswahlkriterien für CSPM-Tools und stehen jederzeit mit unserer Ausschreibungsexpertise und Marktkenntnis zu Ihrer Verfügung.

Kontaktieren Sie uns!

Zusammen stärken wir Ihre Cybersicherheit – vom transparenten Überblick über Ihr Risiko bis hin zur Auswahl passender Anbieter.

Individuell. Pragmatisch. Unabhängig.

Kontaktieren Sie das CyberCompare Management

Dr Jannis Stemmann (CEO)

Jannis.Stemmann@
de.bosch.com
Tel.: +49 711 811-44954

Philipp Pelkmann (CTO)

Philipp.Pelkmann@
de.bosch.com
Tel.: +49 711 811-15519

Simeon Mussler (COO)

Simeon.Mussler@
de.bosch.com
Tel: +49 711 811-19893

Verbände/Industriekooperationen von **Bosch CyberCompare**

Besuchen Sie unsere Website:
www.cybercompare.com