Enterprise Strategy Group™ by TechTarget

WHITEPAPER

Steigerung des Unternehmens-wachstum durch mehr Sicherheit in Hybrid- und Multicloud-Umgebungen

Effizientes Sicherheitsmanagement als Beitrag zur digitalen Transformation

Von Melinda Marks, Practice Director, Cybersecurity
Enterprise Strategy Group

Oktober 2023

Inhalt

Einleitung

Heutzutage sind Unternehmen gezwungen, sich digital zu transformieren, denn nur so können sie ihre Produktivität optimieren und sich einen Wettbewerbsvorteil verschaffen. Zu diesem Zweck lagern sie zunehmend Anwendungen in Cloud-Dienste aus. Dadurch können sie die Softwareentwicklung beschleunigen, ohne sich um die Bereitstellung von Servern oder Hardware kümmern zu müssen. Außerdem müssen sie Remote-Arbeit unterstützen, um ihrer Belegschaft und ständig wachsenden Teams größtmögliche Flexibilität zu bieten. Auf ihrem Weg zur digitalen Transformation sehen sich Unternehmen dabei mit einer zunehmenden IT-Komplexität konfrontiert, da sie verteilte Anwendungen in Hybrid- und Multicloud-Umgebungen einsetzen und eine verteilte Belegschaft unterstützen müssen.

Daraus ergeben sich neue Anforderungen an die Sicherheit, denn sie muss skalierbar sein, damit Anwendungen in verschiedenen Umgebungen unterstützt werden können und das Unternehmenswachstum uneingeschränkt möglich ist. Die Sicherheit von Anwendungen und BenutzerInnen in verschiedenen Umgebungen, die jeweils ihre eigenen Plattformarchitekturen, Funktionen und Kapazitäten aufweisen, muss gewährleistet sein. Sicherheitsteams müssen außerdem flexibel skalieren können, um veränderten Geschäftsanforderungen gerecht zu werden, beispielsweise durch organisches Wachstum und Übernahmen.

Sie stehen jedoch vor zahlreichen Herausforderungen bei der Umstellung ihrer Security-Strategien, die erforderlich ist, damit sie mit der zunehmenden Nutzung von Cloud-Diensten und der Cloud-nativen Entwicklung Schritt halten können. Der Grund dafür sind Probleme mit der Transparenz, die sich aus dem kurzlebigen Charakter von Cloud-Ressourcen und einer Infrastruktur ergeben, die schnell nach oben oder unten skaliert werden kann. Außerdem ist es schwierig, mit der gestiegenen Produktivität von Entwicklern Schritt zu halten und Bedrohungen zu verhindern, wenn sich Zugriffe und Berechtigungen ausbreiten.

Viele Unternehmen versuchen zwar, diese Herausforderungen durch den Einsatz mehrerer Sicherheitslösungen oder -plattformen zu bewältigen, sehen sich aber häufig mit Sicherheitsvorfällen konfrontiert, die auf allgemeine Probleme wie Fehlkonfigurationen oder übermäßigen Zugriff zurückzuführen sind. Auch blinde Flecken und Lücken zwischen den Tools erschweren die Transparenz. Selbst wenn ihre Tools sie auf Sicherheitslücken hinweisen, gelingt es den Sicherheitsteams zudem oft nicht, kritische Probleme rechtzeitig zu priorisieren und zu beheben, um ihre Anwendungen vor Angriffen zu schützen. Mit der zunehmenden Verbreitung von Ressourcen und Anwendungen in Cloud-Umgebungen werden diese Herausforderungen noch zahlreicher.

Sicherheitsteams benötigen eine wirksame Strategie, um Anwendungen in verschiedenen Umgebungen zu schützen und dabei eine umfassende Transparenz und einen Zugriffsschutz zu gewährleisten, der die Mobilität der Workloads abdeckt. Dieser Beitrag befasst sich mit den wichtigsten Elementen für einen effektiven Ansatz zur Anwendungssicherheit. Dieser muss flexibel genug sein, um dem schnellen Unternehmenswachstum und dessen Anforderungen an Hybrid- und Multicloud-Umgebungen gerecht zu werden.

Unternehmen sollten ein flexibles Konzept anstreben, das Sicherheitsteams unabhängig von ihren Kenntnissen darin unterstützt, eine vollständige Transparenz der Ressourcen für eine effiziente Behebung von Schwachstellen und einen Zero-Trust-Ansatz zu gewährleisten. Denn nur so können Anwendungen in allen Umgebungen vor Angriffen geschützt werden. Dieses Konzept sollte die schnelle Erkennung von Sicherheitsproblemen sowie kontextbezogene Einblicke und Threat-Intelligence umfassen, um Maßnahmen zu priorisieren, die den größten Einfluss auf die Risikominimierung haben. Zudem sollte es vereinfachte, zentralisierte Möglichkeiten für die Aufstellung von Richtlinien zum Schutz von Ressourcen bieten.

Mit einem Ansatz, der die Anwendungen und den Zugriff über ihre vernetzten, dynamischen Multicloud- und Hybrid-Umgebungen hinweg abdeckt, können Sicherheitsteams ihre Ressourcen und Abläufe optimieren, um Risiken effektiv zu überwachen und schnell auf Bedrohungen zu reagieren. Dies ermöglicht den Sicherheitsteam eine effiziente Skalierung zur Unterstützung der schnellen Entwicklung und des Geschäftswachstums.

Sicherheitsrelevante Herausforderungen im Zusammenhang mit der digitalen Transformation

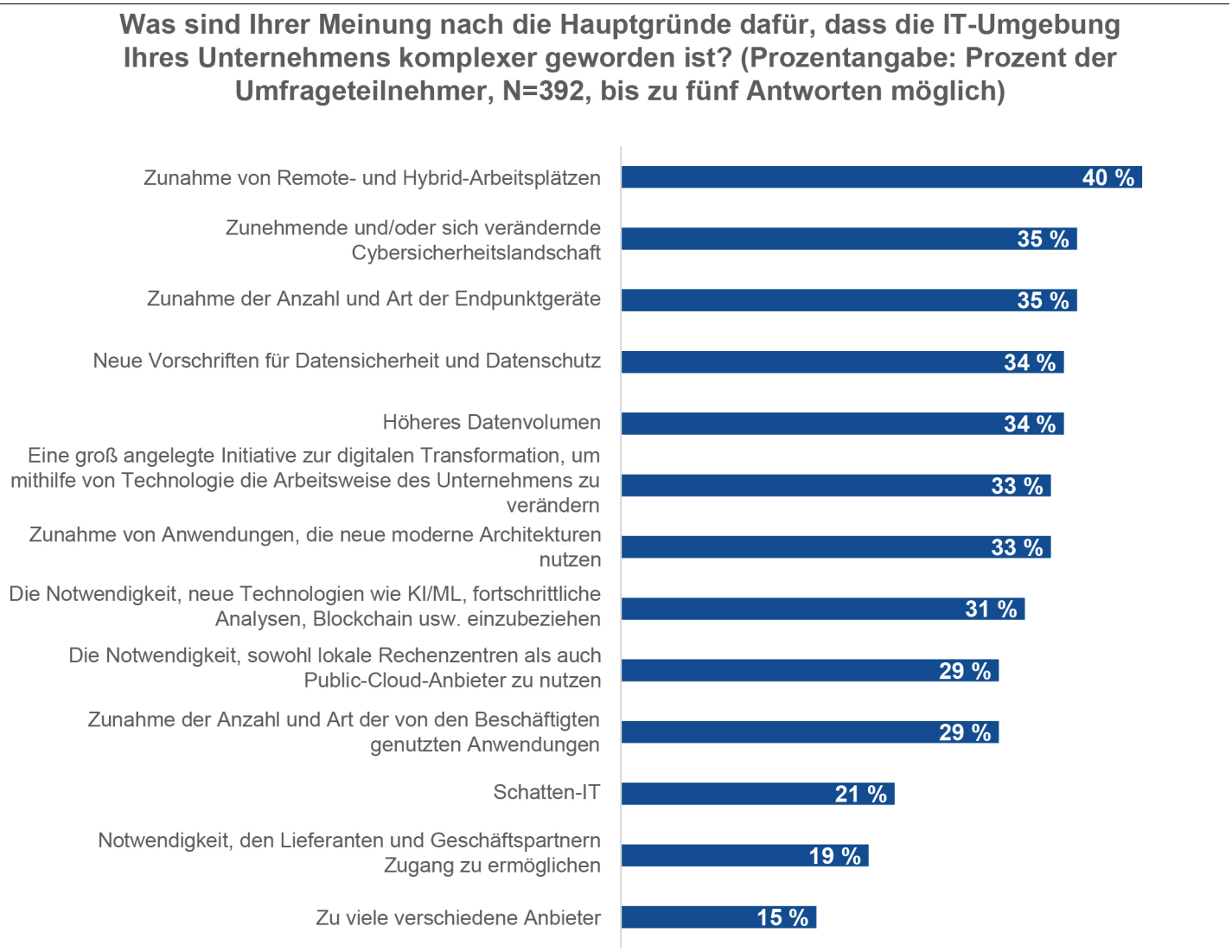
Eine Studie der Enterprise Strategy Group von TechTarget zeigt, dass ein „perfekter Sturm“ der jüngsten Entwicklungen die Sicherheitsteams vor besondere Herausforderungen stellt. Dazu gehören die zunehmende Komplexität von IT-Umgebungen, die Verbreitung von Cloud-nativen Anwendungen aufgrund der gestiegenen Produktivität von EntwicklerInnen und Transparenzlücken über mehrere Public Clouds hinweg. All dies birgt die Gefahr verschiedenster Sicherheitsvorfälle. Sicherheitsteams benötigen eine effektive Strategie, um diese Herausforderungen zu meistern und das Unternehmenswachstum zu ermöglichen. Gleichzeitig müssen sie dafür sorgen, dass ihre Anwendungen sicher und in verschiedenen Umgebungen geschützt sind, ohne dass hierfür spezielle Fähigkeiten erforderlich sind.

Komplexere IT

Wenn Unternehmen die digitale Transformation nutzen, um ihre Produktivität zu steigern und sich einen Wettbewerbsvorteil zu verschaffen, ist dies auch mit Komplexität und neuen Anforderungen an die IT und Sicherheit verbunden. Laut einer Studie der Enterprise Strategy Group sind mehr als die Hälfte (53 %) der Unternehmen der Meinung, dass ihre IT-Umgebung komplexer oder wesentlich komplexer ist als noch vor zwei Jahren.[1] Als Hauptgrund für die zusätzliche Komplexität nennen diese Unternehmen die Zunahme von Remote- und Hybrid-Arbeit (40 %). Weitere wichtige Gründe für die zunehmende Komplexität sind die sich stetig verändernde Cybersicherheitslandschaft (35 %), die Zunahme der Anzahl und Arten von Endgeräten (35 %), neue Datensicherheits- und Datenschutzbestimmungen (34 %) und ein höheres Datenvolumen (34 %). Weiter unten auf der Liste nannten 29 % der Befragten die Notwendigkeit, sowohl lokale Rechenzentren als auch Public-Cloud-Provider nutzen zu müssen (siehe Abbildung 1).

[1] Studie der Enterprise Strategy Group, *2023 Technology Spending Intentions Survey*, November 2022.

Abbildung 1. Gründe für die IT-Komplexität



Quelle: Enterprise Strategy Group, eine Abteilung von TechTarget, Inc.

Unternehmen können wirksame Wege finden, um Wachstum und Skalierung zu unterstützen, auch wenn diese verschiedenen Bereiche mit zusätzlicher Komplexität verbunden sind.

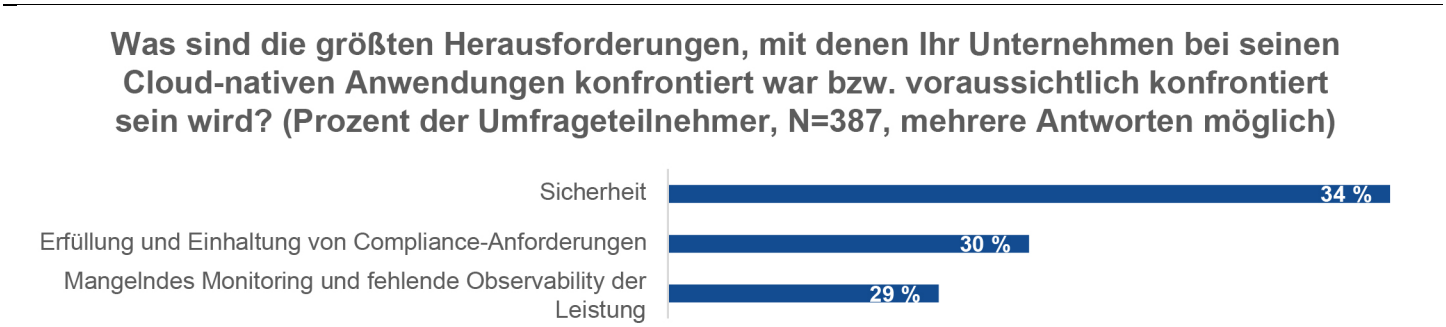
Zunehmende Verlagerung von Anwendungen in Cloud-Umgebungen

Unternehmen nutzen auch zunehmend die Public-Cloud-Infrastruktur, um durch Cloud-native Entwicklung die Produktivität und Innovationskraft zu steigern. Sie müssen sich nicht um die zugrunde liegende Infrastruktur oder die Wartung kümmern, sondern können von Skaleneffekten durch Pay-as-you-go-Modelle von Cloud Service Providern (CSPs) profitieren.

Die Studie der Enterprise Strategy Group zur Modernisierung der Anwendungsinfrastruktur zeigt, dass 88 % der befragten Unternehmen Produktionsworkloads auf Public-Cloud-Infrastrukturen/-Plattformen ausführen und Unternehmen ihre Produktionsworkloads zunehmend in die Cloud verlagern.[2] Sie zeigt auch, dass Unternehmen, die ihre Anwendungen in die Cloud verlagert haben, von vielen Vorteilen profitieren, darunter mehr Flexibilität, niedrigere Infrastrukturkosten und eine schnellere Bereitstellung.

Die Einführung der Cloud erleichtert zudem DevOps, wodurch die EntwicklerInnen mit einem Shift-Left-Ansatz ihre eigene Infrastruktur bereitstellen können, anstatt auf die Bereitstellung von Servern durch IT- oder Betriebsteams zu warten. EntwicklerInnen können effizienter arbeiten und profitieren von einer schnelleren Wertschöpfung als bei der herkömmlichen Anwendungsentwicklung. Im Zuge der höheren Produktivität bei der Softwareentwicklung entstehen jedoch auch Sicherheits- und Compliance-Herausforderungen bei Cloud-nativen Anwendungen.

Abbildung 2: Die drei größten Herausforderungen, denen Unternehmen mit Cloud-nativen Anwendungen gegenüberstehen



Quelle: Enterprise Strategy Group, eine Abteilung von TechTarget, Inc.

Unternehmen benötigen eine effektive Methode zur Eindämmung von Sicherheitsrisiken, damit sie den geschäftlichen Anforderungen gerecht werden können, die sich aus der Umstellung auf die Cloud-native-Entwicklung ergeben, und um ein höheres Volumen und eine höhere Geschwindigkeit bei den Releases zu erreichen. Sicherheitsteams, die ihre Effizienz zur Unterstützung von Skalierung und Wachstum optimieren, anstatt die Einführung neuerer Technologien zur Steigerung von Produktivität und Innovation zu behindern, spielen eine wichtige Rolle dabei, das Unternehmen zu besseren Ergebnissen zu führen.

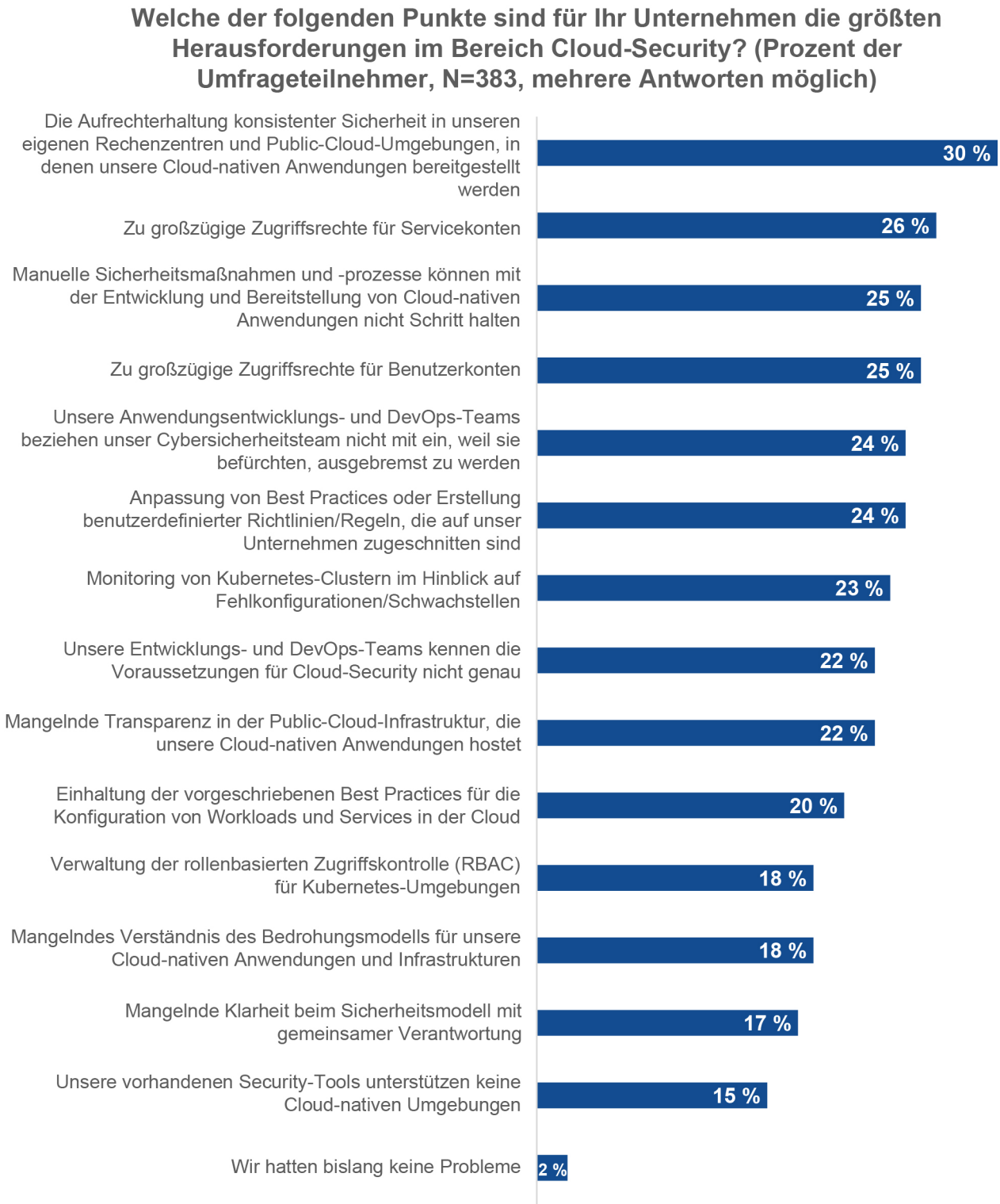
[2] Quelle: Enterprise Strategy Group Research Report, *Cloud-native Applications*, Mai 2022.

Management des Sicherheitsstatus in Multicloud-Umgebungen

Die Förderung des Wachstums mit Cloud-Umgebungen erfordert auch Sicherheitsteams, die Multicloud-Umgebungen unterstützen. Untersuchungen der Enterprise Strategy Group zum Management des Cloud-Sicherheitsstatus zeigen, dass die meisten Unternehmen (94 %) mehrere Service-Provider für die Cloud-Infrastruktur nutzen. Dabei setzt die Mehrheit (69 %) auf drei oder mehr Anbieter.[3] Obwohl die Mehrheit der Unternehmen (68 %) angab, über zuverlässige Lösungen für das Management des Sicherheitsstatus in der Cloud zu verfügen, berichteten sie auch über eine Reihe von Problemen. Dies betrifft vor allem die Transparenz und Kontrolle, die sie für ein effektives Risikomanagement in verschiedenen Umgebungen und Teams benötigen, einschließlich des Erreichens einer einheitlichen Sicherheit in ihrem Rechenzentrum und in ihren Cloud-Umgebungen (30 %). Weitere Herausforderungen sind zu großzügige Berechtigungen für Service- und Benutzerkonten (25 % bzw. 26 %), manuelle Sicherheitsmaßnahmen und Prozesse, die nicht mit der Geschwindigkeit der Bereitstellung Cloud-nativer Anwendungen Schritt halten (25 %), mangelnde Beteiligung an und mangelnde Kontrolle über Entwicklungsprozesse (24 %), mangelnder Einblick in die Public-Cloud-Infrastruktur (22 %) und unzureichendes Verständnis von Cloud-nativen Bedrohungen (18 %, siehe Abbildung 3).[4]

[3] Quelle: Studie der Enterprise Strategy Group, *Cloud Entitlements and Posture Management Trends*, April 2023.
[4] ebd.

Abbildung 3: Größte Herausforderungen der Unternehmen im Bereich Cloud-Security



Quelle: Enterprise Strategy Group, eine Abteilung von TechTarget, Inc.

Unternehmen benötigen einen effektiven Ansatz, der diese Herausforderungen angeht. Nur so können sie ihre Anwendungen in allen Umgebungen schützen. Dies erfordert eine Möglichkeit, die Anwendungen unabhängig von ihrem Standort sichtbar und kontrollierbar zu machen und sie so zu betrachten, als befänden sie sich in einer vernetzten, dynamischen Umgebung und nicht in getrennten Umgebungen. Die Zusammenführung von Informationen aus Multicloud- und Hybrid-Umgebungen erhöht die Effizienz von Sicherheitsverfahren, mit denen sich Risiken eindämmen lassen und schnell auf Bedrohungen reagiert werden kann. Nur so ist Sicherheit skalierbar, um das Unternehmenswachstum mit zunehmender Cloud-Präsenz zu unterstützen.

Ein breites Spektrum an Sicherheitsvorfällen

Obwohl Unternehmen in der Regel über mehrere Sicherheitslösungen verfügen, haben die meisten von ihnen Sicherheitsvorfälle im Zusammenhang mit ihren Cloud-nativen Anwendungen oder ihrer Infrastruktur erlebt. Konkret berichteten 94 % der teilnehmenden Unternehmen, dass sie in den letzten 12 Monaten Sicherheitsvorfälle mit Angriffen und/oder lateralen Bewegungen verzeichneten. Diese reichten von gestohlenen Anmeldeinformationen (29 %) über die Ausnutzung von Fehlkonfigurationen (29 %) bis hin zu Datenverlusten durch unsichere Nutzung von APIs (24 %) und Ransomware (16 %, siehe Abbildung 4).[5]

Dies geschah entweder, weil sich die Unternehmen ihrer Gefährdung nicht bewusst waren oder weil sie nicht in der Lage waren, Sicherheitsprobleme rechtzeitig zu beheben, um Vorfälle zu verhindern oder einzudämmen. Dies unterstreicht die Notwendigkeit von umgebungsübergreifender Transparenz sowie die Notwendigkeit eines plattformbasierten Ansatzes, um effiziente Sicherheitsverfahren zu fördern und Maßnahmen zu priorisieren, die den größten Einfluss auf die Risikoreduzierung haben.

[5] ebd.

Abbildung 4: Arten von Sicherheitsvorfällen mit Cloud-nativen Anwendungen und Infrastrukturen im vergangenen Jahr

Quelle: Enterprise Strategy Group, eine Abteilung von TechTarget, Inc.

Zu viele isolierte Tools und Daten

Eine weitere Herausforderung für Unternehmen ist die häufige Verwendung mehrerer, isolierter Tools in IT-, Netzwerk- und Sicherheitsteams, was die Sicherheitsverfahren verlangsamt. Während die herkömmliche Anwendungssicherheit mehrere Sicherheitsprodukte einsetzt, um die Abdeckung mit Tests und Monitoring zur Erkennung von Sicherheitsproblemen zu gewährleisten, ist es für Cloud-native Anwendungen und die zunehmende Geschwindigkeit der Entwicklungszyklen nicht sinnvoll, immer wieder mehrere separate Tools hinzuzufügen, die Warnmeldungen generieren, ohne den Kontext zu kennen. Dies erschwert die Ermittlung, wie die erforderlichen Maßnahmen zu priorisieren sind.

33 % gaben an, dass die Zusammenführung der Ergebnisse mehrerer Sicherheitsprodukte eine große Herausforderung darstellt

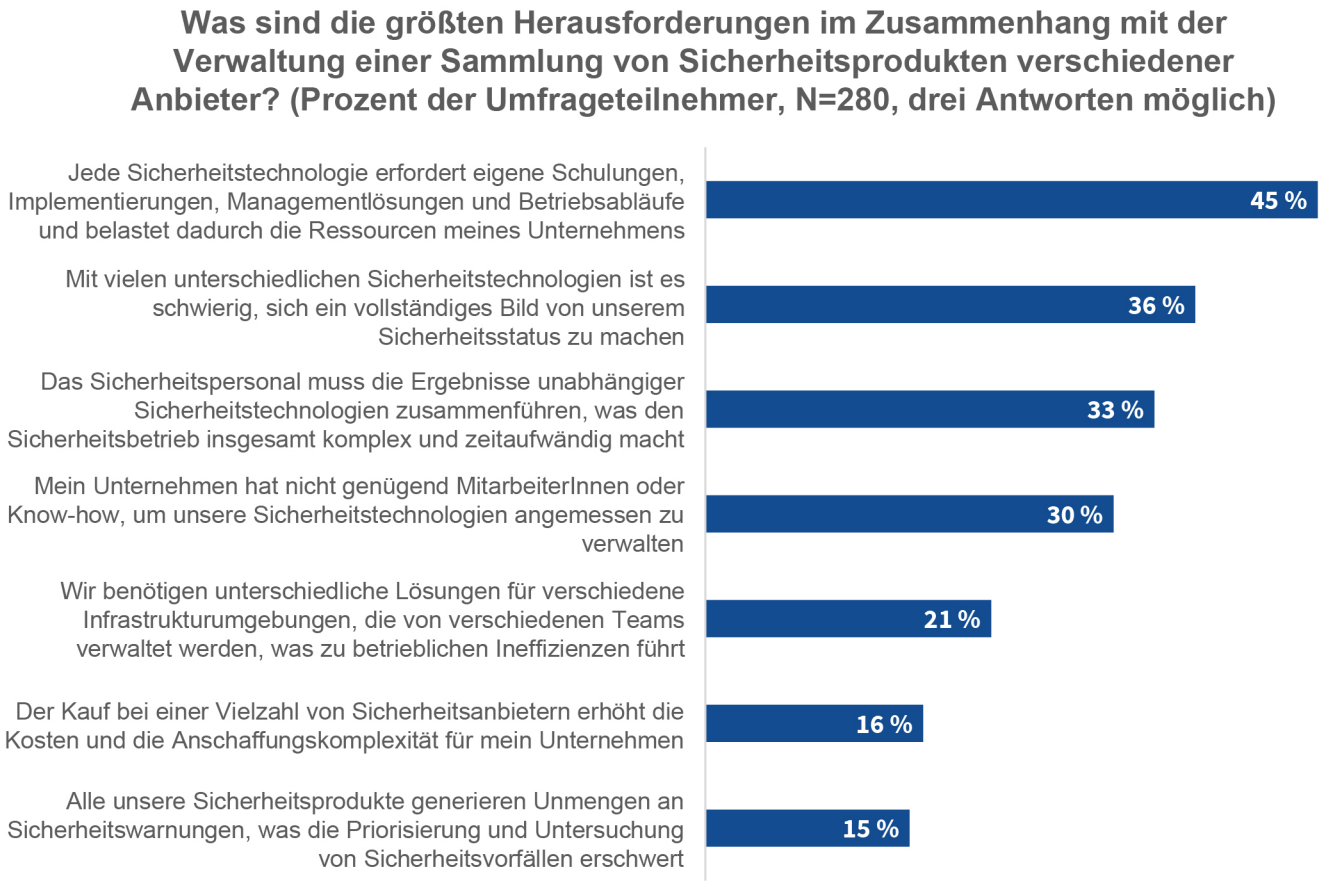
Wenn das Sicherheitspersonal Daten aus mehreren unabhängigen Sicherheits-technologien zusammenstellen muss, werden die Sicherheitsverfahren insgesamt zu komplex und zeitaufwändig.

Entwickler und Sicherheitsteams können mit den vielen Warnungen von mehreren Produkten nicht Schritt halten. Außerdem wurden die einzelnen Tools oft in verschiedenen Sprachen entwickelt und es ist schwierig, ihre Ergebnisse im Hinblick auf den Kontext zu analysieren, der erforderlich ist, um Prioritäten hinsichtlich der zu beachtenden Punkte zu setzen. Darüber hinaus kann jedes Tool Warnungen oder falsch-positive Meldungen generieren, durch die kostbare Zeit verschwendet wird.

Die Studie der Enterprise Strategy Group zeigt, dass die Verwaltung mehrerer Tools Herausforderungen für CybersicherheitsmitarbeiterInnen darstellt. Dies betrifft insbesondere den Schulungs- und Zeitbedarf für die Bereitstellung und Verwaltung der einzelnen Tools. Dieser Punkt wurde von 45 % der Befragten genannt. Außerdem gaben die Unternehmen an, dass es schwierig ist, sich mit den einzelnen Tools ein vollständiges Bild vom Sicherheitsstatus zu machen (36 %) und dass die Zusammenführung der Ergebnisse der einzelnen Tools mehr Arbeit für die Sicherheitsverantwortlichen bedeutet (33 %, siehe Abbildung 5).[6]

[6] Quelle: Vollständige Ergebnisse der Enterprise Strategy Group-Umfrage, *ESG/ISSA Cybersecurity Process and Technology Survey*, Juni 2022.

Abbildung 5: Herausforderungen bei der Verwaltung mehrerer Sicherheitsprodukte



Quelle: Enterprise Strategy Group, eine Abteilung von TechTarget, Inc.

Aus diesem Grund setzen Unternehmen auf Produkte und Services, die CSP-übergreifend funktionieren, um die benötigten Daten zu sammeln und ganzheitlich darzustellen. Dies hilft Sicherheitsteams dabei, Sicherheitsrisiken effektiver zu verwalten, einschließlich effizientem Schwachstellenmanagement, Angriffsflächenmanagement und Angriffspfadanalysen, um ein besseres Verständnis von Sicherheitslücken zu erlangen.

Eine einheitliche Plattform für Hybrid- und Multicloud-Umgebungen bietet Folgendes:

- Zugriff nach dem Prinzip der geringsten Rechte mit zentralisierten Kontrollen, die laterale Bewegungen stoppen
- Umfassende Einblicke in die Ressourcenerkennung und das Angriffspfadmanagement für alle Anwendungen, Workloads und Ressourcen.
- Hochgradig zuverlässige Einblicke, Maßnahmen und Prioritäten für SecOps-Teams mit Bereitstellung des Sicherheitsstatus aus einer zentralen Informationsquelle

Übermäßig bereitgestellter Netzwerkzugriff

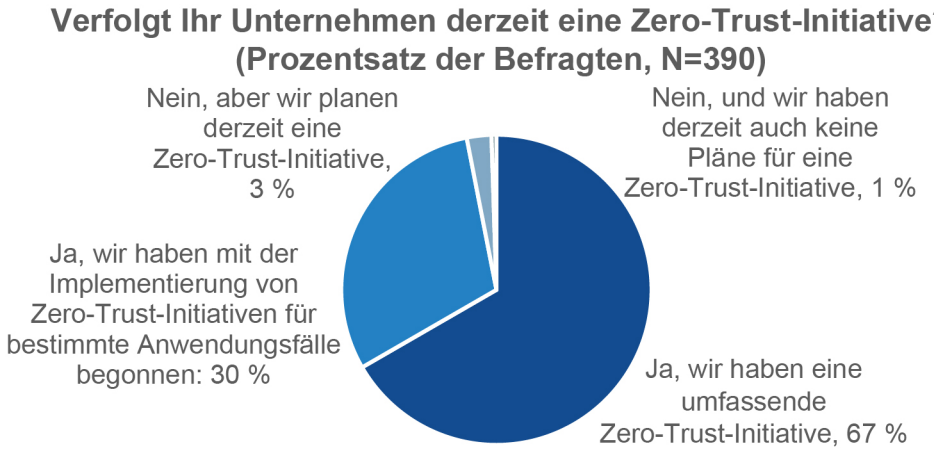
Auch das Management von Identitäten und sicherem Zugang spielt eine wichtige Rolle bei der Effektivität von Sicherheitsprogrammen. Der Grund dafür ist, dass die Cloud-native Entwicklung es Unternehmen und ihren EntwicklerInnen erleichtert, ihre Anwendungen in der Cloud bereitzustellen und sie für Kunden, MitarbeiterInnen und Partner zur Verfügung zu stellen. Nach der Bereitstellung in der Cloud sind die Anwendungen für die vorgesehenen BenutzerInnen verfügbar, aber der Zugriff muss ordnungsgemäß verwaltet werden, um Risiken und Gefahren für die Unternehmens- und Kundendaten zu minimieren. Mit anderen Worten: In der Cloud gibt es keinen Perimeter zum Schutz von Workloads; Identität und Zugriff bilden den Perimeter.

Ein Blick auf die bereits erwähnten Herausforderungen und Vorfälle im Zusammenhang mit Cloud-nativer Sicherheit zeigt, dass viele davon mit Identitäts- und Zugriffsproblemen zusammenhängen. Das liegt daran, dass der Zugang oft übermäßig bereitgestellt wird, um eine schnelle Entwicklung zu ermöglichen. Wenn der Zugang jedoch nicht ordnungsgemäß verwaltet wird, vergrößert sich die Angriffsfläche und das Risiko für ein Unternehmen, da Anwendungen offen für Angriffe bleiben oder es Angreifern leicht gemacht wird, sich nach dem Eindringen in ein System seitlich zu bewegen.

Die Implementierung eines Zero Trust Network Access(ZTNA)-Ansatzes trägt zum Schutz von Anwendungen bei, indem sichergestellt wird, dass jede Zugriffsanfrage überprüft wird, bevor Verbindungen hergestellt werden. Dadurch können Sicherheitsteams die Wahrscheinlichkeit und die Auswirkungen eines Vorfalls minimieren. Wenn also ein Workload oder eine Anwendung Opfer eines Angriffs wurde, würde eine Zero-Trust-Umgebung den Zugriff auf oder die Ausgabe von Daten verhindern. Untersuchungen der Enterprise Strategy Group zeigen, dass die überwiegende Mehrheit der Unternehmen (97 %) entweder bereits Zero-Trust-Initiativen durchgeführt hat oder dabei ist, diese zu implementieren, um ihre Workloads in verschiedenen Umgebungen besser schützen zu können.[7]

[7] Quelle: Vollständigen Ergebnisse der Enterprise Strategy Group-Umfrage, *2023 SASE Series: SSE Leads the Way Toward SASE*, August 2023.

Abbildung 6: Prozentsatz der Unternehmen, die Zero-Trust-Initiativen einführen



Quelle: Enterprise Strategy Group, eine Abteilung von TechTarget, Inc.

Unternehmen stehen jedoch vor Herausforderungen bei der Implementierung des Zugriffs mit geringsten Rechten für ihre Anwendungen in Multicloud- und Hybrid-Umgebungen. Dazu gehören die Erleichterung der Zusammenarbeit zwischen IT-, Betriebs- und Sicherheitsteams, die Bereitstellung eines sicheren Zugriffs von einer Reihe von Geräten aus, die Verwaltung der Kosten, die Gewährleistung der Datensicherheit, die Aufrechterhaltung der Leistung und die Bereitstellung einer umfassenden Transparenz und Berichterstattung.

Daher sollten Unternehmen nach einer Lösung suchen, die sowohl Hybrid- als auch Multicloud-Umgebungen abdeckt und einen Zero-Trust-Ansatz integriert. Eine solche Lösung würde Unternehmen helfen, Risiken zu mindern und gleichzeitig die Betriebseffizienz zu optimieren. IT-, Netzwerk- und Sicherheitsteams könnten ihre Anwendungen in verschiedenen Umgebungen schützen.

Neu: Cisco Cloud Protection Suite

Die Cisco Cloud Protection Suite bietet einen modernen Ansatz für Anwendungssicherheit mit End-to-End-Security für Hybrid- und Multicloud-Anwendungsumgebungen. Von Bare-Metal-Umgebungen bis hin zu nativen Cloud-Umgebungen: Die Cloud Protection Suite ermöglicht Kunden ganzheitliche Anwendungssicherheit und schützt Workloads umgebungsübergreifend – vor Ort und in der Cloud.

Cisco Cloud Protection bietet Folgendes:

- **Umfassende Hybrid- und Multicloud-Sicherheit:** Mit der Cisco Cloud Protection Suite können User Sicherheitsrisiken umgebungsübergreifend effizient und effektiv verwalten.
- **Umfassende Transparenz sämtlicher Ressourcen:** Ein klarer Überblick über jedes Netzwerk, jede Anwendung und jede Cloud-Ressource ermöglicht es Unternehmen, ihren Sicherheitsstatus zu überprüfen und die Risiken für das Unternehmen zu priorisieren.
- **Umgebungsübergreifende Konsistenz:** Die Suite von Cisco vereinfacht die Anwendung von Security-Frameworks, Kontrollen und Compliance-Richtlinien zur Risikominimierung und zur Umsetzung von Best Practices der Branche.
- **Optimierte Effizienz bei Korrekturmaßnahmen:** Die Suite von Cisco nutzt eine auf Datenwissenschaft basierende Risikobewertung zur Priorisierung von Schwachstellen, die ein echtes Risiko in der gesamten Hybrid-Umgebung darstellen.

- **Anwendungsschutz:** Die Suite schützt den Datenverkehr über das Netzwerk, die Clouds und die VPCs hinweg und ermöglicht eine konsistente und genaue Makro- und Mikrosegmentierung in verschiedenen Umgebungen.
- **Zugriff nach dem Prinzip der geringsten Rechte mit einem Zero-Trust-Ansatz:** Cisco Cloud Protection nutzt ZTNA, um Workloads vor Ort und in der Cloud zu schützen, die Angriffsfläche zu reduzieren und seitliche Bewegungen zu verhindern.

Die Cisco Cloud Protection Suite zum Management der Anwendungssicherheit in Cloud-Umgebungen bietet Kunden folgende Vorteile:

- Weniger Betriebsaufwand und Optimierung von Ressourcen
- Eindämmung von Sicherheitsrisiken mit einer Priorisierung der Schwachstellen nach Risiko
- Einfachere Erfüllung von Compliance-Vorschriften
- Schnellere Reaktion auf Bedrohungen mit umfassender Transparenz
- Umsetzung der digitalen Transformation zur Unterstützung des Unternehmenswachstums

Fazit

Heutzutage verlagern immer mehr Unternehmen ihre Workloads in die Cloud, um die Produktivität zu optimieren. Dies stellt Sicherheitsteams vor einige Herausforderungen, wenn es darum geht, ihre Anwendungen in verschiedensten Umgebungen zu schützen und mit dem Unternehmenswachstum Schritt zu halten. Die Komplexität der Unterstützung von Anwendungen in Hybrid- und Multicloud-Umgebungen bei gleichzeitiger Möglichkeit der Cloud-Migration oder sogar der Rückführung erfordert einen einheitlichen, flexiblen Ansatz.

Die Cisco Cloud Protection Suite bietet Sicherheitsteams eine effektive Möglichkeit, die Anwendungssicherheit über mehrere Clouds und Rechenzentren hinweg zu verwalten. Durch umfassende Transparenz und eine Zugriffskontrolle mit geringsten Rechten wird eine ganzheitliche und effektive Methode zum Schutz von Ressourcen und Anwendungen in der gesamten Umgebung bereitgestellt. Die Lösung bietet ein einheitliches Risikomanagement mit Automatisierung, umgebungsübergreifender Konsistenz und konsolidierten Security-Tools. Außerdem werden manuelle Aufgaben reduziert, um die Effizienz der IT-, Netzwerk- und Sicherheitsteam zu optimieren.

Mit der Cisco Cloud Protection Suite sind Sicherheitsteams besser gerüstet, um das Unternehmenswachstum und die digitale Transformation zu unterstützen, einschließlich der Skalierung von Entwicklungsteams, der Einführung neuer Technologien sowie Fusionen und Übernahmen, die Unternehmen wettbewerbsfähig halten.

Informationen zur Enterprise Strategy Group
Die Enterprise Strategy Group von TechTarget bietet fokussierte und aussagekräftige Marktinformationen, nachfrageseitige Forschung, Analystenberatungsservices, GTM-Strategieleitfäden, Lösungsvalidierungen und benutzerdefinierte Inhalte zur Unterstützung des Kaufs und Verkaufs von Enterprise-Technologien.

contact@esg-global.com
www.esg-global.com