EXECUTIVE SUMMARY

2023 Hybrid-Cloud-Sicherheit

Wahrnehmung gegen Realität

Für die 72 Prozent aller Organisationen, die bereits auf hybride Cloud-Infrastrukturen setzen, ist die richtige Sicherheit immer noch eine Herausforderung. Viele der traditionellen Sicherheitswerkzeuge wurden noch für On-Premises-Umgebungen konzipiert. Moderne digitale Infrastrukturen lassen sich damit nicht ausreichend überwachen und schützen.

Um die Wahrheit über den Stand der Hybrid-Cloud-Sicherheit herauszufinden, haben wir die Meinungen und Erkenntnisse von mehr als 1.000 Sicherheitsverantwortlichen aus sechs globalen Schlüsselmärkten (USA, Großbritannien, Frankreich, Deutschland, Australien und Singapur) analysiert. Das Ergebnis? Zwischen der Wahrnehmung der Sicherheitslage und der rauen Realität klafft eine erhebliche Lücke. Lesen Sie hier den vollständigen Report, oder erfahren Sie unten mehr über die wichtigsten Erkenntnisse.

Der Stand der Hybrid-Cloud-Sicherheit

Die gute Nachricht ist, dass 96 Prozent der Befragten die Cloud-Sicherheit als übergreifende Aufgabe für alle Beteiligten betrachten. Fast alle (**99 Prozent**) der IT- und Sicherheitsverantwortlichen, mit denen wir in EMEA, APAC und den USA gesprochen haben, sind zudem überzeugt, dass CloudOps und SecOps in ihren Unternehmen gemeinsame Ziele verfolgen.

Aber es gibt noch viel zu tun. Die Erkennung von Schwachstellen und die Einleitung von Reaktionen ist bei **99 Prozent** der Befragten nach wie vor auf das SecOps-Team beschränkt. Es fehlt eine Security-first-Kultur. Viele sind außerdem besorgt über Wissenslücken in Bezug auf den richtigen Schutz der Cloud, wobei mehr als die Hälfte (**52 Prozent**) der Befragten behauptet, dass Vorstände das Modell der gemeinsamen Verantwortung noch nicht verstehen.

Daher ist es kaum verwunderlich, dass **93 Prozent** der weltweiten IT- und Sicherheitsverantwortlichen eine Zunahme von Cloud-Sicherheitsangriffen in den nächsten 12 Monaten vorhersagen. Dabei ist insbesondere zu bedenken, dass **90 Prozent** seit Anfang 2022 bereits Opfer eines erfolgreichen Cyberangriffs geworden sind.

Wachsende Sichtbarkeitslücken: Wahrnehmung gegen Realität

31 Prozent der IT- und Sicherheitsverantwortlichen erkannten eine Sicherheitsverletzung erst durch:

- Verlangsamte Performance von Applikationen (**18 Prozent**), wahrscheinlich aufgrund von DoS oder laufender Daten-Exfiltration
- Verlust des Anwenderzugriffs auf Applikationen oder digitale Ressourcen (**9 Prozent**)
- Veröffentlichung proprietärer Unternehmensinformationen im Dark Web (**4 Prozent**)

Im Ergebnis wurden Sicherheitsverstöße zu spät identifiziert, wobei fast ein Drittel der Vorfälle von den bestehenden Monitoring- und Sicherheitswerkzeugen nicht erkannt werden konnte. Angesichts dieser drastischen Ergebnisse ist es keine Überraschung, dass die Besorgnis über blinde Flecken zunimmt.

Ein weiteres beunruhigendes Ergebnis ist, dass 1 von 3 CISOs nicht weiß, wo die sensibelsten Daten gespeichert sind und wie sie gesichert werden. Offenbar gibt es eine Reihe kritischer Sichtbarkeitslücken, die durch eine Fehleinschätzung des Ausmaßes blinder Flecken noch verstärkt werden: **70 Prozent** geben an, dass verschlüsselter Datenverkehr ungehindert über ihre hybride Cloud läuft. Weitere **35 Prozent** haben nach eigener Einschätzung nur begrenzten Einblick in Container. So entstehen erhebliche Geschäftsrisiken, weil der verschlüsselte Datenverkehr nicht ausreichend analysiert werden kann. Eingehende, ausgehende und laterale Datenbewegungen lassen sich mit den vorhandenen Werkzeugen nicht auf Malware-Bedrohungen untersuchen.

Hier besteht eine Diskrepanz zwischen Wahrnehmung und Realität. **50 Prozent** der IT- und Sicherheitsverantwortlichen sind nach eigener Aussage entweder zuversichtlich oder sehr zuversichtlich, dass sie über ausreichende Sicherheit von On-Premises bis Cloud verfügen. In Wahrheit existieren aber viele blinde Flecken der Cloud-Sicherheit in Unternehmen rund um die Welt.

Weiterhin verhaltene Umsetzung von Zero Trust

Außerdem haben wir im dritten Jahr in Folge mit IT- und Sicherheitsverantwortlichen über Zero Trust gesprochen. Dabei konnten wir eine Reihe von Veränderungen in der Wahrnehmung des Security Frameworks feststellen.

Definition von Deep Observability:
Erweiterung der Leistungsfähigkeit herkömmlicher Monitoring- und Sicherheitswerkzeuge durch sofort verwertbare und aus dem Netzwerk gewonnene Informationen und Erkenntnisse. Deep Observability beseitigt blinde Flecken und ermöglicht es Teams, Kosten zu senken, Komplexität zu reduzieren und Sicherheits- wie auch Compliance-Risiken in der Cloud proaktiv zu minimieren.

Zero Trust bleibt ein zentrales Diskussionsthema in der Branche. **80 Prozent** der CISOs waren der Meinung, dass Zero Trust im Jahr 2022 ein großer Trend sein würde. Für das Jahr 2023 und darüber hinaus steigt die Zahl auf **96 Prozent** der CISOs. Weitere Ergebnisse weisen in dieselbe Richtung: **87 Prozent** der Befragten sagten, dass Zero Trust im Jahr 2023 auf Vorstandsebene mit Priorität diskutiert wird. Das ist ein Anstieg von **29 Prozent** gegenüber 2022.

Doch mit der zunehmenden Diskussion über das Security Framework wächst auch die Skepsis hinsichtlich der Realität der Implementierung. Viele sind noch unsicher, wie Zero Trust designt und bereitgestellt werden soll. Dies unterstreicht ein wachsender Trend zur Skepsis in EMEA: Im Jahr 2021 waren **77 Prozent** der IT- und Sicherheitsverantwortlichen der Ansicht, dass Zero Trust möglich und machbar ist. Diese Zahl ist im Jahr 2022 auf **53 Prozent** gefallen und liegt im Jahr 2023 bei weniger als der Hälfte (44 Prozent). Diese Skepsis ist wahrscheinlich darauf zurückzuführen, dass nur **34 Prozent** der Unternehmen bereits über die nötige Sichtbarkeit für Zero Trust verfügen.

Die Power von Deep Observability

IT- und Sicherheitsverantwortliche sind sich bewusst, dass Sichtbarkeit ein wesentlicher Bestandteil von Zero Trust ist. Tatsächlich haben wir herausgefunden, dass **89 Prozent** der Befragten im Jahr 2022 eine mittlere bis starke Verbindung von Sichtbarkeit und Deep Observability sahen. Im Jahr 2023 sind jetzt **100 Prozent** von einer starken Verbindung überzeugt. Wichtig ist auch das wachsende Bewusstsein für Deep Observability als Lösung zum Schutz der Hybrid Cloud. Nach Vorlage der Definition von Deep Observability stimmten **89 Prozent** der globalen IT- und Sicherheitsverantwortlichen im Jahr 2022 zu, dass Deep Observability ein wichtiges Element der Cloud-Sicherheit ist. Diese Zahl ist nun auf **97 Prozent** geklettert. Um **20 Prozent** gegenüber dem Vorjahr ist zudem die Zahl der Befragten gestiegen, die angeben, dass Deep Observability mit Priorität auf Vorstandsebene diskutiert wird.

Die Hybrid Cloud ist ein komplexer Raum. Da aber die Mehrheit der Unternehmen Hybrid-Cloud-Infrastrukturen nutzt oder nutzen wird, ist es wichtig, dass IT- und Sicherheitsverantwortliche eine realistische Vorstellung von ihrer Security Posture haben. Das Rennen hat begonnen: Jetzt geht es darum, Sichtbarkeit für alle Daten im Transit zu gewährleisten, die Lücken zwischen Wahrnehmung und Realität zu schließen und gefährliche blinde Flecken in der Cloud zu beseitigen.

Über Gigamon

Gigamon bietet eine Pipeline für Deep Observability, die sofort verwertbare Informationen auf Netzwerkebene nutzt, um die Leistungsfähigkeit von Observability-Werkzeugen zu maximieren. Diese effektive Kombination ermöglicht es IT-Organisationen, Sicherheit und Compliance umfassend zu gewährleisten, die Ursachen von Leistungsengpässen schneller zu identifizieren und den Verwaltungsaufwand zu senken, der ansonsten durch das Management hybrider und Multi-Cloud-Infrastrukturen entsteht. Das Ergebnis: Moderne Unternehmen realisieren das volle Transformationspotenzial der Cloud. Gigamon unterstützt mehr als 4.000 Kunden weltweit, darunter über **80 Prozent** der Fortune-100-Unternehmen, 9 der 10 größten Mobilfunkanbieter und Hunderte von Behörden und Bildungseinrichtungen weltweit.

Download der vollständigen Studie, um die Erkenntnisse aus Ihrer Region zu erfahren gigamon.com/umfrage-cloud-sicherheit

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

09.23_01