HYBRID-CLOUD-SICHERHEIT:

Wahrnehmung gegen Realität

Eine globale Umfrage unter mehr als 1.000 IT- und Sicherheitsverantwortlichen zeigt, dass die Wahrnehmung der Hybrid-Cloud-Sicherheit und Transparenz nicht mit der Realität übereinstimmt. Außerdem bereiten neue Gesetzgebungen CISOs Sorgen. Dies zeigt, dass Deep Observability wichtiger ist als je zuvor.

WAHRNEHMUNG vs. REALITÄT

94% der weltweit befragten Unternehmen gaben an, **dass ihre Sicherheitswerkzeuge und -prozesse vollständige Sichtbarkeit und tiefe Einblicke** in ihre IT-Infrastruktur bieten.

50% sind zuversichtlich oder sehr **zuversichtlich, dass ihre gesamten** IT-Infrastrukturen ausreichend gesichert sind – von On-Premises bis Cloud

96% der Befragten sind der Meinung, **dass Cloudsicherheit von der Sichtbarkeit aller Daten im Transit abhängt.**

97% sind ihrer Ansicht nach fähig, **bei der Erkennung und Behebungvon Schwachstellen innerhalb ihrer IT-Organisation** zusammenzuarbeiten.

NUR 30% **haben Einblick in verschlüsselte Daten.** Ein Drittel der CISOs weiß nicht sicher, wo sensible Daten gespeichert sind und wie sie geschützt werden.

NUR 10% **haben in den letzten** 18 Monaten keinen Datenschutzvorfall verzeichnet.

MEHR ALS 30% **der Datenschutzverstöße wurden von Sicherheits-** und Monitoring-Werkzeugen nicht entdeckt.

ÜBER 16% **aller Unternehmen praktizieren keine kollektive Verantwortung.** SecOps trägt die Sicherheitsverantwortung oft allein.

Es herrscht eine gewisse Naivität in Bezug auf die Gefahren von Sichtbarkeitslücken

Trotz des Vertrauens in die vollständige Sichtbarkeit geben IT- und Sicherheitsteams eine Reihe von bekannten Transparenzlücken in ihren IT-Infrastrukturen zu.

Aber erkennen sie diese als Bedrohungen?

26%
Mehr als ein Viertel (26%) der weltweit Befragten ist besorgt, dass sie nicht über die nötigen Werkzeuge bzw. ausreichende Sichtbarkeit für den Unternehmensschutz verfügen.

52%
haben keinen Einblick in lateralen (Ost-West) Datenverkehr.

35%
verfügen nur über begrenzte Sichtbarkeit des Container-Datenverkehrs.

Unerwartete blinde Flecken

und deren Ausnutzung wurden von Befragten **(56%)** als wichtigste Sorge genannt.

Gesetzgebung

ist ein zentraler Stressfaktor **(34%)**, wobei der EU Cyber Resilience Act weltweit die meisten Kopfschmerzen verursacht.

Angriffskomplexität

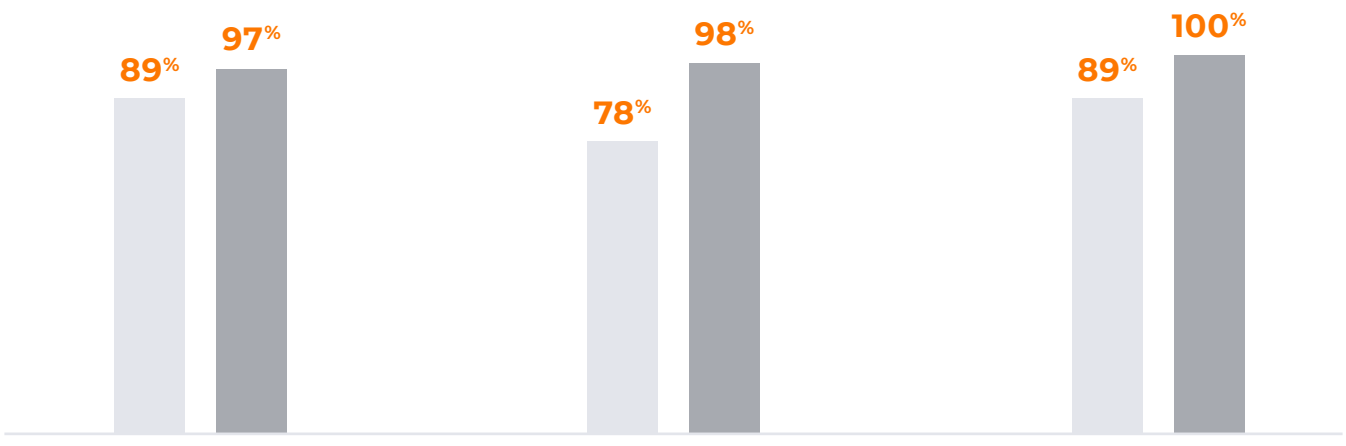
ist eine größere Sorge **(32%)** für CISOs als unzureichende Cyberinvestitionen **(14%)**.

Blinde Flecken und Gesetze bereiten CISOs Sorgen

Der erwartete Fachkräftemangel und der Investitionsbedarf tauchen 2023 kaum auf dem Radar der IT- und Sicherheitsverantwortlichen auf. **ONur 19% geben an, dass eine wirksame Sicherheitsschulung der Mitarbeiter ein entscheidender Faktor** ist, um Vertrauen in die Sicherheit der IT-Infrastruktur zu gewinnen.

DEEP OBSERVABILITY: Wachsende Bedeutung für Cloudsicherheit und Zero Trust

Deep Observability gewinnt bei IT- und Sicherheitsverantwortlichen zwischen 2022 und 2023 weiter an Bedeutung



Deep Observability ist ein wichtiges Element der Cloud-Sicherheit.

Deep Observability wird durch den Vorstand als Priorität zur besseren Sicherung der Hybrid Cloud diskutiert.

Deep Observability ist eng mit Zero Trust verbunden.

Entdecken Sie die Erkenntnisse aus Ihrer Region im vollständigen Report: gigamon.com/umfrage-cloud-sicherheit

Datensammlung: 19. April bis 2. Mai 2023
Befragte: 1.020 CIOs/CISOs/CTOs und andere Netzwerk- und Cloud-Experten
Regionen: USA, Großbritannien, Frankreich, Deutschland, Singapur, Australien

Gigamon®

Weltweiter Hauptsitz 3300 Olcott Street, Santa Clara, CA 95054 USA +1 (408) 831-4000 | gigamon.com
© 2023 Gigamon. Alle Rechte vorbehalten. Gigamon und Gigamon-Logos sind Marken von Gigamon in den Vereinigten Staaten und/oder anderen Ländern. Gigamon-Marken finden Sie unter gigamon.com/legal-trademarks. Alle anderen Marken sind die Marken der jeweiligen Eigentümer. Gigamon behält sich das Recht vor, diese Veröffentlichung ohne vorherige Ankündigung zu ändern, zu modifizieren, zu übertragen oder anderweitig zu überarbeiten.