Gigamon®

CISO-Erkenntnisse

MANAGEMENT-ZUSAMMENFASSUNG

Risiko-Rekalibrierung im Zeitalter der KI

Einleitung

CISOs stehen unter wachsendem Druck. Hybrid-Cloud-Umgebungen werden immer verteilter, dynamischer und schwieriger zu schützen. Künstliche Intelligenz (KI) treibt die digitale Transformation voran und verursacht eine noch nie dagewesene Komplexität. Das überfordert die Fähigkeiten konventioneller Security- und Management-Werkzeuge. Intern müssen sich CISOs mit unklaren Befugnissen hinsichtlich Budgets und Strategien arrangieren – werden aber dennoch zur Verantwortung gezogen, sobald etwas schief geht. Infolgedessen geben **97 Prozent** der CISOs an, dass sie bei der Schutz und Management ihrer Hybrid-Cloud-Infrastruktur Kompromisse eingehen.

Die gemachten Kompromisse reichen von lückenhafter Sichtbarkeit bis hin zu Datenqualität und Tool-Integration. CISOs wissen aber genau, dass sie es sich nicht leisten können, diese grundlegenden Elemente zu verlieren. Die Warnzeichen waren bereits im Jahr 2024 deutlich zu erkennen. Jetzt, im Jahr 2025, steht noch mehr auf dem Spiel. Die Zahl der Sicherheitsverletzungen steigt, KI-Bedrohungen entwickeln sich rasant weiter und die schiere Datenmenge bringt herkömmliche Sicherheitswerkzeuge an ihre Grenzen. Traditionelle Bedrohungsmodelle reichen nicht mehr aus. Die CISOs von heute müssen Risiken in Echtzeit rekalibrieren, auf neue Schwachstellen reagieren und an der Schnittstelle von Sichtbarkeit, Kontrolle und Geschäftsstrategie die Führung übernehmen.

Ein neuer Weg zeichnet sich ab. CISOs vertrauen in wachsendem Maße auf Deep Observability, um die nötige Klarheit für schnelle, selbstbewusste und präzise Aktionen zu erhalten. Dieser Report untersucht, wie sich Sicherheitsverantwortliche heute anpassen und was sie tun müssen, um den Entwicklungen auch zukünftig einen Schritt voraus zu sein. Für unseren 2025 Hybrid Cloud Security Report „Risiko-Rekalibrierung im Zeitalter der KI“ haben wir über 1.000 Security- und IT-Experten in Australien, Frankreich, Deutschland, Singapur, Großbritannien und den USA befragt. Den vollständigen Report finden Sie hier. In der vorliegenden Zusammenfassung präsentieren wir die wichtigsten Erkenntnisse von 211 CISOs weltweit, um kritische Herausforderungen, Kompromisse und Prioritäten aufzudecken, von denen die Rolle des CISO in der modernen KI-getriebenen Hybrid-Cloud-Landschaft bestimmt wird.

In diesen kritischen Bereichen müssen Kompromisse gemacht werden:

Herstellung umfassender Sichtbarkeit der gesamten IT-Infrastruktur On-Premises und in der Cloud, inklusive lateralem East-West-Datenverkehr.

Verwendung von Netzwerk- und Anwendungsmetadaten, um die Effektivität von Sicherheitswerkzeugen zu verbessern.

Integration sich ergänzender Sicherheitswerkzeuge On-Premises sowie in Public und Private Clouds, inklusive virtualisierter und Container-Umgebungen.

Verfügbarkeit sauberer, akkurater und qualitativ hochwertiger Daten, um die Bereitstellung neuer Workloads (inklusive KI) zu unterstützen.

Umsetzung von Zero-Trust-Frameworks und -Architekturen.

DEEP OBSERVABILITY DEFINIERT

Die Fähigkeit zur effizienten Bereitstellung von Telemetrie aus dem Netzwerk (Pakete, Datenströme, Metadaten) für Cloud-, Security- und Observability-Werkzeuge, die MELT-Daten (Metrik-, Event-, Log- und Trace-Daten) verwenden. Diese leistungsstarke Kombination ermöglicht die Deep Observability, die Unternehmen benötigen, um Blind Spots zu beseitigen, den Netzwerkverkehr zu optimieren und die Kosten und Komplexität zu reduzieren, die ansonsten mit Schutz und Management von Hybrid-Cloud-Infrastrukturen verbunden sind.

Die Cloud-Wahrnehmung verändert sich

CISOs bilden die Speerspitze einer veränderten Wahrnehmung von Cloud-Risiken und ihrem Management. Was einst als akzeptabler Kompromiss für mehr Agilität galt, wird nun als wachsende Belastung neu bewertet, insbesondere da die Einführung von KI neue Komplexitätsebenen mit sich bringt.

Im Jahr 2024 stimmten nur **29 Prozent** der CISOs der Aussage zu, dass das Cyberrisiko durch die schnelle Cloud-Migration ansteigt. Jetzt, im Jahr 2025, sagen **75 Prozent** der CISOs, dass die öffentliche Cloud ein größeres Sicherheitsrisiko darstellt als jede andere Umgebung.

Dies führt zu einer Neubewertung der Cloud-Strategien auf breiter Front. Fast drei Viertel (**73 Prozent**) der CISOs erwägen die Rückführung von Daten aus der Public in die Private Cloud. Das deutet darauf hin, dass sie die Kontrolle über sensible Workloads zurückgewinnen wollen. Ein Drittel (**33 Prozent**) nennt Public-Cloud-Sicherheit und KI-Governance als wichtigste Herausforderungen und mehr als die Hälfte (**54 Prozent**) zögert aufgrund von Sicherheitsbedenken, KI in Public-Cloud-Umgebungen einzusetzen.

CISOs betrachten die Public Cloud nicht länger als Standard, sondern als eine Entscheidung, die eine genaue Prüfung, eine solide Strategie und wirksame Sicherheitsvorkehrungen voraussetzt. Dieser Wandel spiegelt eine umfassende Risiko-Rekalibrierung im Zeitalter der KI wider. Sichtbarkeit und Governance sind nicht mehr verhandelbar. Da hybride Cloud-Umgebungen immer komplexer werden, treffen CISOs bewusstere Entscheidungen über die Speicherung kritischer Daten und KI-Anwendungen. Dabei steht nicht mehr nur Performance im Fokus, sondern kontrollierbare Sicherheit, der CISOs vertrauen können.

Datenqualität ist die wahre Währung der Cybersicherheit

CISOs befanden sich schon einmal an diesem Punkt. Laut unserer Umfrage geben CISOs an, durchschnittlich 15 Sicherheitstools in ihren Umgebungen einzusetzen. Aber sie haben gelernt, dass die Anzahl der Werkzeuge nicht dem Sicherheitsniveau entspricht. Integration ist die eigentliche Herausforderung: Granulare und qualitativ hochwertige Daten müssen über verschiedene Tools hinweg zusammengeführt werden, um ein vollständiges Gesamtbild zu erhalten. In den komplexen Hybrid-Cloud-Umgebungen von heute können CISOs so mithilfe von Deep Observability den KI-Datenverkehr schützen, Systeme effektiv überwachen und den Wert bestehender Investitionen maximieren.

CISO-PERSPEKTIVE

86 Prozent der CISOs stimmen zu, dass Daten auf Paketebene sowie Metadaten für eine verbesserte Security Posture und schnellere Bedrohungserkennung von entscheidender Bedeutung sind.

Werkzeug-Integration ist eine Herausforderung, mit der viele noch zu kämpfen haben. Für **1 von 3** CISOs (**32 Prozent**) bilden zu viele schlecht integrierte Tools das größte und am häufigsten genannte Hindernis für effektive Cybersicherheit. Die KI-getriebene Datenexplosion verstärkt den Druck zusätzlich: **40 Prozent** der CISOs geben an, dass sich die Menge der Netzwerkdaten, die von Tools erfasst und überwacht werden muss, in den letzten zwei Jahren mehr als verdoppelt hat. In diesem Zusammenhang wird die Qualität der Daten zu einem kritischen Unterscheidungsmerkmal.

Es gibt aber auch Anzeichen für Fortschritt. Letztes Jahr gaben **7 von 10** CISOs an, dass ihre vorhandenen Tools nicht fähig sind, Sicherheitsverstöße effektiv zu erkennen. In diesem Jahr ist diese Zahl auf **1 von 2** CISOs (**52 Prozent**) gesunken. Dies deutet darauf hin, dass die Optimierung vorhandener Tools – durch höhere Datenqualität und engere Integration – allmählich zu Ergebnissen führt. Auch wenn es nach wie vor Herausforderungen gibt, ist also ein positiver Trend zu beobachten: CISOs konzentrieren sich auf die Erreichung vollständiger Sichtbarkeit, anstatt immer weiter zusätzliche Werkzeuge hinzuzufügen. Im Zeitalter der KI wird Kontrolle von CISOs durch vertrauenswürdige integrierte Daten neu definiert – dadurch gewinnen sie mehr Vertrauen in ihre Fähigkeit, sich gegen die sich ständig wandelnden Bedrohungen zu verteidigen.

Kritische Erfolgsfaktoren für CISOs

Aufgrund der durch KI zunehmenden Komplexität und den steigenden Erwartungen an CISOs kann der Erfolg nicht allein durch technische Expertise erreicht werden. Stattdessen ist der CISO-Erfolg abhängig von einer Mischung aus Strategie, operativer Klarheit und Einflussnahme.

Sichere KI-Bereitstellung anführen

KI ist keine Zukunftsmusik mehr, sondern unmittelbare Realität, CISOs stehen unter dem Druck, KI hier und heute zu schützen und zu managen – oftmals, ohne über eine verlässliche Sichtbarkeit der Infrastruktur oder klare Governance Frameworks zu verfügen. Im Jahr 2024 waren **59 Prozent** der Befragten der Meinung, dass mehr KI-spezifische Schulungen hilfreich wären. Im Jahr 2025 werden jetzt praktische Lösungen gefordert, weil die KI-Implementierung in vollem Gange ist.

Angesichts dieses Wandels konzentrieren sich CISOs darauf, die Grundlagen für eine sichere KI-Bereitstellung zu schaffen. Für fast die Hälfte (**46 Prozent**) ist Deep Observability dabei eine der obersten Sicherheitsprioritäten, wenn es um KI geht.

CISO-PERSPEKTIVE

85 Prozent sind der Ansicht, dass Deep Observability nicht nur ein nützliches, sondern ein grundlegendes Element der Hybrid-Cloud-Sicherheit ist.

Weitere **45 Prozent** setzen KI-Tools aktiv ein, um ihre eigene interne Sicherheitsfunktionalität zu verbessern. Auch Monitoring klettert auf der Agenda nach oben: **39 Prozent** konzentrieren sich auf die Verbesserung der Datengenauigkeit durch eine genauere Überwachung von KI-Anwendungen. Zudem implementiert **jeder dritte** CISO (**34 Prozent**) Leitplanken für große Sprachmodelle (LLMs) wie DeepSeek, um die Gefährdung durch aufkommende Risiken zu mindern.

KI-Implementierungen sind nicht mehr nur eine theoretische Angelegenheit - CISOs müssen die Umsetzung bewerkstelligen. Der Erfolg hängt jetzt von praktischen Frameworks ab, die Sichtbarkeit und Kontrolle gewährleisten, um hybride Cloud-Infrastrukturen besser zu sichern und zu verwalten.

Sichtbarkeit als Differentiator

Weil KI das Wachstum der Komplexität beschleunigt, wird Sichtbarkeit zu einem zentralen Erfolgsfaktor für CISOs. Erst die Fähigkeit, die Gesamtheit der Data-in-Motion zu überwachen, verwandelt fragmentierte Signale in verwertbare Informationen. Dies gilt insbesondere für lateralen East-West-Datenverkehr in hybriden Umgebungen. Die Prioritäten werden immer deutlicher: In diesem Jahr geben **83 Prozent** der CISOs an, dass effektive Cloud-Sicherheit von der Sichtbarkeit der Data-in-Motion abhängt. Dennoch hat fast die Hälfte (**48 Prozent**) nach eigener Auffassung immer noch keinen umfassenden Einblick in die eigene Hybrid-Cloud-Infrastruktur. Wiederum gilt dies insbesondere für den lateralen East-West-Datenverkehr. Infolgedessen gehören Bedrohungsüberwachung und Sichtbarkeit in Echtzeit für **57 Prozent** der CISOs zu den wichtigsten Themen im kommenden Jahr.

Sichtbarkeit ist mehr als eine technische Notwendigkeit. In einer Landschaft, die durch Rauschen und Fragmentierung geradezu überwältigt wird, wirkt das Erreichen eines Zustands von Klarheit transformativ: Reaktive Sicherheit wird zu proaktiver Verteidigung, sodass Organisationen in der Lage sind, Bedrohungen zu erkennen und zu neutralisieren, bevor es zu einer Eskalation kommt.

Das Potenzial der CISO/Vorstand-Partnerschaft erschließen

Obwohl die Erwartungen an CISOs beständig wachsen, haben diese hinsichtlich Cybersicherheitsstrategien, Entscheidungsfindung und Finanzierung weiterhin mit unklaren Befugnissen zu kämpfen. Der Widerspruch ist eklatant. Während **52 Prozent** der CISOs glauben, dass sie die Kontrolle über das Cybersicherheitsbudget haben, sind nur **8 Prozent** ihrer C-Suite-Kollegen derselben Meinung. Diese Diskrepanz ist nicht allein auf mangelnde Kommunikation zurückzuführen. Vielmehr handelt es sich um ein strukturelles Problem: CISOs tragen die

Die von KI ausgehenden Risiken sind eindeutig. Es ist wichtig, dass CISOs in der Offensive bleiben und diese Bedrohungen genauso angehen, wie es Bedrohungsakteure tun. Die Stärkung der Cybersicherheit erfordert Deep Observability der gesamten Data-in-Motion, um zu verstehen, wo sich Sicherheitslücken befinden. Nur so können CISOs ihre Hybrid-Cloud-Infrastrukturen vor Bedrohungsakteuren schützen, die permanent nach einer perfekten Gelegenheit zum Angriff suchen.

CHAIM MAZAL
Chief Security Officer, Gigamon

Verantwortung für Sicherheitsergebnisse, haben aber keine Möglichkeit, die Entscheidungen zu beeinflussen, von denen die Ergebnisse abhängen.

Da die Cybersicherheit auf den Vorstandsetagen zusehends an Bedeutung gewinnt, tritt der Widerspruch zwischen Wahrnehmung und Verantwortung deutlicher hervor. Die IT-Budgets liegen immer noch größtenteils bei den CIOs und CTOs. Das beschränkt die Möglichkeiten der CISOs, Programme voranzutreiben, für deren Sicherheit sie verantwortlich sind. Doch der Druck wird immer größer. Infolgedessen sind **81 Prozent** der CISOs der Meinung, dass Cybersicherheit bald gleichauf mit finanziellen oder rechtlichen Risiken betrachtet wird – und das CISOs schlussendlich die Verantwortung tragen müssen.

Die Überbrückung dieser Kluft beginnt mit einer gemeinsamen Ausrichtung innerhalb des Führungsteams. Für **1 von 3** CISOs (**35 Prozent**) ist es wichtig, dass auf Vorstandsebene ein Bewusstsein für die Risiken und Vorteile von KI existiert. Obwohl **86 Prozent** der Befragten sagen, dass Deep Observability mittlerweile Teil der Vorstandsgespräche über Cybersicherheit ist (im Jahr 2024 waren es noch **76 Prozent**), garantiert die Diskussion noch nicht die Implementierung.

KI wird die Cybersicherheit auf der Unternehmensagenda weiter nach oben treiben, deshalb benötigen CISOs mehr als nur einen Platz am Tisch. Wenn sie für die Minderung von Geschäftsrisiken verantwortlich sein sollen, erfordert dies die Befugnis zur Gestaltung des Risikomanagements. Dieser Wandel beginnt mit einer Neudefinition der eigenen Rolle als strategischer Partner auf Vorstandsebene.

Über Gigamon

Gigamon® bietet eine Deep Observability Pipeline, die effizient netzwerkbasierte Telemetrie an Cloud-, Sicherheits- und Observability-Tools liefert. Das reduziert Blind Spots und senkt die Kosten für Sicherheitswerkzeuge, sodass Unternehmen ihre Hybrid-Cloud-Infrastrukturen besser schützen und verwalten können. Gigamon hat mehr als 4.000 Kunden weltweit, darunter über 80 Prozent der Fortune 100 Unternehmen, 9 der 10 größten Mobilfunkanbieter und mehrere Hundert Regierungen und Bildungseinrichtungen. Für weitere Informationen besuchen Sie bitte: gigamon.com/de

Gigamon®

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

05.25_01