Gigamon®

Stärkung der CISO-Rolle im Zeitalter von KI

CISO-ERKENNTNISSE

Hybrid Cloud Security Report 2026

Einleitung

KI verändert die Art und Weise, wie Unternehmen arbeiten, den Wettbewerb gestalten und Innovationen schaffen. Durch die schnelle Verbreitung von KI entstehen aber auch Risiken, die sich im selben Tempo vermehren. In vielen Fällen führt dies dazu, dass die Fähigkeit zur Messung, Überprüfung und Eindämmung von Risiken nicht mehr Schritt halten kann.

Für CISOs entsteht dadurch eine entscheidende Herausforderung. Als Verantwortliche für Sicherheit müssen sie Umgebungen schützen, die fragmentierter, dynamischer und schwieriger zu beobachten sind als je zuvor. Hybrid-Cloud-Architekturen, dezentrale KI-Nutzung und verschlüsselte Datenströme verändern die Entstehung und das Management von Risiken.

Dies ist kein rein technisches Problem, sondern eine Frage der Sicht- und Nachweisbarkeit.

Das Ausmaß dieser Herausforderung ist dabei eindeutig. In den letzten 12 Monaten meldeten **83 Prozent** der globalen Unternehmen Sicherheitsvorfälle im Zusammenhang mit KI. Dazu gehörten externe, KI-gestützte Angriffe (**41 Prozent**), interne Datenlecks (**30 Prozent**), die unerlaubte Nutzung von KI (**30 Prozent**) sowie direkte Angriffe auf KI- oder LLM-Systeme (**33 Prozent**).

Gleichzeitig verfügen viele CISOs nicht über die benötigte Sichtbarkeit, um souverän handeln zu können. **Fast die Hälfte** gibt an, dass die Aufdeckung von Sicherheitsvorfällen heute länger dauert. Zudem berichten **46 Prozent**, dass KI-getriebener Datenverkehr die Identifizierung und Untersuchung von Vorfällen erschwert.

CISOs werden für Risiken zur Verantwortung gezogen, die sie nicht vollständig überblicken und nicht vollständig nachweisen können. In dieser Umgebung wird Sichtbarkeit zu einer Voraussetzung für Handlungsfähigkeit. Sie verschafft CISOs die nötige Klarheit entschlossen zu handeln, die Nachweise für eine glaubwürdige Kommunikation und das Vertrauen, souverän zu führen.

Die vorliegende Analyse basiert auf den Erkenntnissen von 307 CISOs, die an der Umfrage zum **Hybrid Cloud Security Report 2026** teilgenommen haben. Es spiegeln sich hier die Erfahrungen und Perspektiven von Sicherheitsverantwortlichen wider, die weltweit in vorderster Reihe mit KI-getriebenen Risiken konfrontiert werden.

Rechenschaftspflicht ohne Nachweise

Die Verbreitung von KI und Hybrid-Cloud-Umgebungen hat die Art, wie sich Daten bewegen, grundlegend verändert. Anwendungen erstrecken sich mittlerweile über Umgebungen hinweg, Workloads werden permanent verlagert und der Datenverkehr wird standardmäßig verschlüsselt. Systeme interagieren miteinander auf Wegen, die mit traditionellen Ansätzen nur schwer nachvollzogen werden können.

Zu den **größten Herausforderungen** für CISOs gehören heute Sichtbarkeitslücken aufgrund von Cloud-Komplexität. CISOs können erkennen, dass sich Risiken im East-West-Datenverkehr, in hybriden Cloud-Umgebungen und innerhalb KI-gestützter Prozesse entwickeln. Außerdem wissen sie, dass Governance-Modelle, Datensicherheitskontrollen und KI-spezifische Kompetenzen nicht mit der rasanten Entwicklung dieser Umgebungen Schritt halten können.

Aber Bewusstsein ersetzt keinen Nachweis.

Ohne einen einheitlichen Überblick zu allen Daten in Bewegung (Data in Motion) können Sicherheitsteams nicht überprüfen, was in der Umgebung vor sich geht. Außerdem sind sie oftmals nicht in der Lage, Bedrohungen in verschlüsseltem oder lateralem Datenverkehr zuverlässig zu erkennen, den Ursprung einer Bedrohung (Root Cause) eindeutig zu ermitteln oder die erforderlichen Nachweise zu liefern, um Berichtswesen und Entscheidungsfindung umfassend zu unterstützen.

Dies führt zu einem strukturellen Ungleichgewicht. Von CISOs wird erwartet, kritische Fragen zu beantworten, ohne stets über die Daten zu verfügen, die für eine fundierte Antwort notwendig wären.

CISOs betrachten Herausforderungen anders und fokussieren sich auf strukturelle und operative Schwachstellen

CISO	HERAUSFORDERUNGEN	ALLE ANDEREN BEFRAGTEN
1	Sichtbarkeitslücken aufgrund von Cloud-Komplexität	2
2	Mangel an Cloud-Expertise	3
3	Fragmentierte Sicherheits-Tools	5
4	Wachsende Komplexität durch KI-Verbreitung	4
5	Zunahme KI-gestützter Angriffe	1

Wahrnehmungskluft erhöht Risiken

CISOs sind sich der bestehenden Einschränkungen bewusst, aber im restlichen Unternehmen ergibt sich oftmals ein anderes Bild. **Fast 40 Prozent** der Unternehmen geben an, dass sie auf einer integrierten Reifegradstufe der KI-Sicherheit operieren. **Sechzig Prozent** sind der Ansicht, dass ihre Data-Governance-Regelwerke solide und gut etabliert sind. Auf den ersten Blick lässt dies auf Zuversicht und Kontrolle schließen.

Die Daten zeichnen ein anderes Bild.

Der Anteil der Unternehmen, die einen Sicherheitsvorfall verzeichnen mussten, ist von **47 Prozent** im Jahr 2024[1] auf **65 Prozent** im Jahr 2026 gestiegen. Die Bedrohung durch Insider nimmt zu. Bei den meisten Vorfällen spielt mittlerweile KI eine Rolle. In hybriden Umgebungen bestehen weiterhin Sichtbarkeitslücken.

Diese Kluft zwischen Wahrnehmung und Realität wird immer größer.

Fast die Hälfte der befragten C-Level-Führungskräfte ist der Ansicht, dass die Ursache von Sicherheitsvorfällen innerhalb von 72 Stunden ermittelt werden kann. Dem stimmt nur **etwa ein Viertel** (27 Prozent) der CISOs zu. **Fast die Hälfte** gibt an, dass die Nachverfolgung tatsächlich bis zu sieben Tage dauern kann. CISOs berichten also von einer langsameren und komplexeren Realität: Weitere **23 Prozent** geben an, dass es bis zu 30 Tage dauern kann, die Ursache zu ermitteln oder den Betrieb wiederherzustellen. Nur **8 Prozent** der anderen Führungskräfte auf C-Level teilen diese Einschätzung.

CISOs, die direkt mit Incident-Daten arbeiten, wissen, wie viel Zeit und Aufwand es kostet, Aktivitäten systemübergreifend nachzuverfolgen. Andere Führungskräfte stützen sich häufig auf zusammengefasste Berichte, die nicht denselben Detailgrad aufweisen. Das führt zu einem optimistischeren Bild der Performance, als die Realität hergibt.

Diese Diskrepanz hat Konsequenzen. Wenn Unternehmen glauben, dass sie sich schneller und vollständiger erholen, als dies tatsächlich der Fall ist, verstärken sie eher bestehende Ansätze, anstatt Ursachen anzugehen.

Probleme bei der Sichtbarkeit verschärfen diese Situation noch. **Über ein Drittel** der CISOs nennt den East-West-Datenverkehr als den größten Risikobereich. Bei anderen C-Level-Führungskräften sinkt dieser Anteil auf **26 Prozent**. Das verdeutlicht die Kluft zwischen denjenigen, die am nächsten an den Daten sind, und denjenigen, die sich auf zusammengefasste Reports verlassen. Dieser Datenverkehr bleibt oft verschlüsselt und wird derzeit nur unzureichend überwacht. Hier können sich Angreifer dauerhaft einnisten und Insider-Bedrohungen weiter ausbreiten.

Das Gleiche gilt für KI. **Drei von vier** CISOs (76 Prozent) geben an, dass die eingeschränkte Sichtbarkeit von KI-getriebenem Datenverkehr ein großes Hindernis darstellt. KI verbreitet sich schnell und überholt die Fähigkeit der Unternehmen zur Datensicherung. Je stärker KI in die Betriebsabläufe integriert wird, desto mehr Unsicherheit entsteht, da die Interaktion mit Daten nicht beobachtet werden kann.

Größte Risiken für Sicherheitsverletzungen in der Infrastruktur

NACH RELEVANZ AUS SICHT DER CISOS SORTIERT

1. **Public Cloud**
2. **Lateraler (East-West) Datenverkehr**
3. **Private KI-/LLM-Umgebungen**
4. **Verschlüsselter Datenverkehr**
5. **Private Cloud/virtualisierte Workloads und SaaS-Data-Lakes**

Warum mehr Tools das Problem nicht lösen

In der Umfrage von 2025[2] nannte **fast die Hälfte** (46 Prozent) der CISOs Herausforderungen bei der Fragmentierung und Integration von Tools als größte Schwachpunkte. Als Reaktion darauf investieren Unternehmen weiterhin in Sicherheitstechnologien, um so wachsenden Bedrohungen zu begegnen. **9 von 10** CISOs (93 Prozent) geben an, im vergangenen Jahr neue Tools zur Verbesserung der Erkennung und Sichtbarkeit eingeführt zu haben. Dennoch sind die Sicherheitsvorfälle im Vergleich zum Vorjahr um **18 Prozent** gestiegen.

Hier spiegelt sich ein tieferliegendes Problem wider. Sicherheits-Tools sind auf die Qualität und Vollständigkeit der Daten angewiesen, die sie verarbeiten. Selbst fortschrittlichste Tools können daher keine zuverlässigen Ergebnisse liefern, wenn die Telemetrie über Umgebungen hinweg fragmentiert ist, keine Einblicke in verschlüsselten Datenverkehr möglich sind oder keine konsistenten Datenquellen zur Verfügung stehen.

Viele Unternehmen geraten in einen bekannten Kreislauf: Ein Vorfall deckt eine Sicherheitslücke auf. Es werden neue Tools eingeführt. Die Sichtbarkeit bleibt jedoch unvollständig. Bei zukünftigen Sicherheitsvorfällen treten dann dieselben Probleme auf.

Um diesen Kreislauf zu durchbrechen, muss der Fokus verlagert werden. Es geht nicht darum, weitere Tools hinzuzufügen. Stattdessen müssen die Sichtbarkeit und Integrität der Daten verbessert werden, die für die Werkzeuge grundlegend sind.

Der Druck auf CISOs wächst

Steigt das Risiko, steigt auch die Verantwortung – und sie verlagert sich stärker auf einzelne Personen.

Mehr als **jeder vierte CISO** befürchtet, nach einem schwerwiegenden Vorfall den Arbeitsplatz zu verlieren. Von Sicherheitsverantwortlichen wird in wachsendem Maße erwartet, erklären zu können, was passiert ist, wo die Ursachen liegen und wie sich ähnliche Vorfälle zukünftig verhindern lassen.

Auch der regulatorische Druck nimmt zu. In den USA haben die Offenlegungsvorschriften der SEC zur Cybersicherheit die Erwartungen an eine zeitnahe und präzise Berichterstattung erhöht. In Europa erweitert die NIS2-Richtlinie die Rechenschaftspflicht auf die Führungsgremien, einschließlich der CISOs. Ähnliche Trends zeichnen sich im gesamten asiatisch-pazifischen Raum ab, wo die Regelwerke den Schwerpunkt auf Sorgfaltspflichten und Verantwortung auf Vorstandsebene legen.

Cybersicherheit wird heute als eine Frage der Governance betrachtet, nicht mehr nur als rein technisches Thema.

CISOs stehen zudem vor einer Reihe von anhaltenden Herausforderungen. Dazu gehören die Absicherung von Daten in Public-Cloud-Umgebungen, das Schließen von KI-Kompetenzlücken, der Umgang mit nicht genehmigter KI-Nutzung, die Verbesserung der Sichtbarkeit von East-West-Datenverkehr sowie die Unterstützung überlasteter Teams.

Jede dieser Herausforderungen lässt sich auf ein übergreifendes Problem zurückführen: Unternehmen fehlt ein klares Verständnis davon, wie Daten fließen, wie KI eingesetzt wird und wo Risiken entstehen.

80 Prozent der CISOs geben an, dass unzureichende Governance im Zusammenhang mit nicht genehmigter KI-Nutzung heute die größte Herausforderung für die Datensicherheit darstellt. Um diesem Problem zu begegnen, setzen **41 Prozent** die Governance auf die Top-Position der Sicherheitsprioritäten.

Was echte CISO-Handlungsfähigkeit wirklich erfordert

Wenn CISOs in wachsendem Maße rechenschaftspflichtig sind, muss gewährleistet sein, dass sie dieser Anforderung auch gerecht werden können. Voraussetzung ist hier eine klare und verlässliche Sichtbarkeit der Datenbewegungen, KI-Nutzung und Risiko-Ursachen. Zudem müssen sie über die Befugnisse und Ressourcen verfügen, um auf Basis dieser Erkenntnisse handeln zu können.

CISOs nennen drei Faktoren, die für ihren Erfolg entscheidend sind:

- Zugriff auf präzise, netzwerkbasierte Telemetriedaten
- Umfassende Sichtbarkeit aller übertragenen Daten
- Ausreichende Ressourcen zur Skalierung von Teams und Betriebsabläufen

CISOs ergreifen bereits Maßnahmen. **Fast die Hälfte** (47 Prozent) plant, KI-gestützte Tools einzusetzen, um Teams und Workflows zu unterstützen. **43 Prozent** wollen die Governance stärken, um sicherzustellen, dass KI sicher und angemessen eingesetzt wird. Gleichzeitig priorisieren **45 Prozent** die Verbesserung der Sichtbarkeit KI-getriebener Datenflüsse in Hybrid-Cloud-Umgebungen.

Gemeinsam weisen diese Prioritäten auf eine Entwicklung hin zu echter Deep Observability.

Deep Observability vereint netzwerkbasierte Telemetriedaten – darunter Metadaten, Pakete und Datenströme – mit Metriken, Ereignissen, Logs und Trace-Daten (MELT). Dadurch entsteht eine einheitliche Sicht auf die Datenflüsse in Hybrid-Cloud-Umgebungen. Durch die Bereitstellung notwendiger Kontextinformationen können Verantwortliche verstehen, wie Systeme interagieren und Risiken entstehen. Außerdem sind CISOs in der Lage, Sicherheitsentscheidungen auf Geschäftsziele abzustimmen und die Geschwindigkeit, Genauigkeit und Glaubwürdigkeit der Risikoberichterstattung auf Führungsebene zu verbessern.

Mit diesem Grad an Sichtbarkeit können CISOs über einzelne, fragmentierte Erkenntnisse hinausgehen und ein umfassenderes Bild ihrer Umgebung gewinnen.

Bedrohungen lassen sich frühzeitiger und präziser erkennen. Aktivitäten können über verschiedene Systeme hinweg nachverfolgt werden, um die eigentlichen Ursachen von Vorfällen zu identifizieren. CISOs erhalten die Möglichkeit, die Wirksamkeit von Kontrollen zu bewerten und Sicherheitslücken aufzudecken, bevor sie zu Vorfällen führen. Darüber hinaus können sie ihre Berichte mit klaren, belastbaren Nachweisen untermauern.

Damit wandelt sich grundlegend, wie Sicherheitsarbeit funktioniert. Annahmen werden durch beobachtbare Daten ersetzt. Entscheidungen können auf einer Grundlage aus Fakten statt nur Vermutungen getroffen werden.

Zugleich gewinnt KI an Bedeutung. Bei unvollständiger Sichtbarkeit kann KI bestehende Lücken verstärken und trügerische Sicherheit erzeugen. Bei hoher Sichtbarkeit hingegen verbessert KI die Erkennung, beschleunigt Analysen und unterstützt fundierte Entscheidungen.

Somit werden CISOs durch mehr Klarheit gestärkt, befähigt und unterstützt.

Neudefinition der CISO-Rolle

Verbesserte Sichtbarkeit wirkt sich nicht nur positiv auf Betriebsabläufe aus. Sie verändert auch, wie CISOs führen.

Sieben von zehn CISOs geben an, dass mangelndes Verständnis auf Vorstandsebene ein großes Hindernis für die erfolgreiche Einführung von KI darstellt. Um diese Lücke zu schließen, bedarf es mehr als nur technisches Fachwissen. Es erfordert die Fähigkeit, Risiken so zu vermitteln, dass sie klar auf geschäftliche Prioritäten bezogen sind.

Wenn CISOs Zugang zu klaren, verlässlichen Daten haben, sind sie in der Lage, die Sicherheit auf die Geschäftsziele abzustimmen. Zudem bezeichnen CISOs eine verbesserte Berichterstattung als den wichtigsten Schritt zu einer gestärkten Abstimmung mit dem Vorstand, da sie dabei hilft, technische Risiken in klare geschäftliche Auswirkungen zu übersetzen. Durch die konkrete Darstellung von Risiken können CISOs den Wert von Sicherheitsinvestitionen aufzeigen und als strategische Berater Vertrauen aufbauen.

Da KI für die Arbeitsweise von Unternehmen immer mehr an Bedeutung gewinnt, ist dieser Wandel unerlässlich. Sicherheit muss in die allgemeine unternehmerische Entscheidungsfindung integriert werden und darf nicht als separate Funktion betrachtet werden.

Von Sichtbarkeit zu Vertrauen

Die Herausforderungen für CISOs entstehen nicht durch mangelnde Investitionen, sondern durch fehlende Klarheit.

Während KI die Entstehung von Risiken beschleunigt, weitet sich die Kluft zwischen Wahrnehmung und Realität. Gleichzeitig steigen die Anforderungen an Verantwortlichkeit. Ohne eine einheitliche Methode zur Beobachtung und Überprüfung der Vorgänge in Hybrid-Cloud-Umgebungen bleiben Unternehmen weiterhin gefährdet.

Fortschritte lassen sich nicht durch den Einsatz weiterer Tools erzielen, sondern durch das Erreichen von Deep Observability, sodass ein konsistenter und umfassender Blick auf alle Datenbewegungen in der Umgebung möglich wird.

Wie CISOs ihre Beziehung zum Vorstand stärken

1. **Verbesserung der Berichterstattung auf Vorstandsebene durch den Nachweis, dass Security klar auf die Geschäftsziele einzahlt.**
2. **Gewährleistung, dass Cybersicherheit ein zentraler Punkt auf der Risiko-Agenda des Vorstands ist.**
3. **Unterstützung der CISOs mit Blick auf ihre Verantwortung und Rechenschaftspflichten für die Security Posture.**
4. **Definition verbindlicher Kriterien für die Offenlegung und Rechenschaftspflicht im Falle eines Sicherheitsvorfalls.**
5. **Einführung regelmäßiger Meetings zwischen CISO und Vorstand zur gemeinsamen Diskussion von Risiken und Strategie.**

Wenn CISOs erkennen können, wie Daten fließen, Systeme interagieren und Risiken entstehen, profitieren sie nicht nur von verbesserter Sichtbarkeit. Sie gewinnen handfeste Beweise.

Diese Beweisbarkeit schafft Vertrauen in die eigenen Fähigkeiten. CISOs können nicht nur auf Risiken reagieren, sondern diese auch erklären und verhindern. Mit dieser Handlungsfähigkeit führen sie Unternehmen aktiv und erfüllen die Anforderungen einer KI-getriebenen Welt..

Über Gigamon

Gigamon schützt die Hybrid-Cloud-Netzwerke und Daten der komplexesten Unternehmen weltweit. Die KI-gestützte Gigamon Deep Observability Pipeline bietet vollständige Sichtbarkeit aller Daten in Bewegung, indem sie vertrauenswürdige, netzwerkbasierte Telemetriedaten direkt an Cloud-, Sicherheits- und Observability-Tools liefert. Mit KI-gestützten Erkenntnissen über Pakete, Datenströme und Anwendungsmetadaten können Unternehmen verborgene Bedrohungen in verschlüsseltem und lateralem Datenverkehr aufspüren, Engpässe bei der Netzwerk- und Anwendungsleistung auflösen und die Compliance überprüfen – und das bei gleichzeitiger Reduktion von Kosten und Komplexität. Mehr als 4.000 Kunden weltweit vertrauen auf Gigamon, darunter 83 Prozent der Fortune 100 Unternehmen sowie große Mobilfunkanbieter und Behörden auf allen Ebenen.

Erfahren Sie mehr auf **gigamon.com**.

Download des Reports unter gigamon.com/umfragecloud-sicherheit

1 Gigamon, 2024, Hybrid Cloud Security Report: Lücken der Sicherheitsbereitschaft schließen

2 Gigamon, 2025, Hybrid Cloud Security Report: Entwicklung der Hybrid Cloud Security im Zeitalter der KI

Gigamon®

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

05.26_01