MANAGEMENT-ZUSAMMENFASSUNG

CISO-Erkenntnisse zur Schließung der Lücken in der Cybersicherheitsbereitschaft

2024 Hybrid Cloud Security Survey

Die heutige Bedrohungslandschaft ist gewaltig und verändert sich ständig. Obwohl im Jahr 2024 globale Ausgaben für Informationssicherheit in Höhe von 215 Milliarden US-Dollar erwartet werden, verlieren die Unternehmen das Wettrüsten gegen Bedrohungsakteure. Mehr als die Hälfte (54 Prozent) der Sicherheits- und IT-Führungskräfte geben an, dass sie stark darin sind, Bedrohungen innerhalb ihrer Hybrid-Cloud-Infrastruktur zu identifizieren. Aber trotzdem passiert es immer wieder, dass Datensicherheitsverletzungen nicht erkannt werden.

In den letzten 12 Monaten war mehr als **1 von 3** Unternehmen **(37 Prozent)** nicht in der Lage, eine Sicherheitsverletzung mit den vorhandenen Sicherheitstools zu entdecken. Im Jahr 2023 waren dies noch **31 Prozent**. Hybrid-Cloud-Umgebungen mit unaufhörlich wachsender Komplexität steigern Cyberrisiken, indem sie Angriffsoberflächen vergrößern und das Erreichen von Sichtbarkeit erschweren. Die Gefahren werden weiter zunehmen, wenn Hybrid-Cloud-Infrastrukturen weiterentwickelt, skaliert und angepasst werden, um KI-Bereitstellungen zu ermöglichen. **Unternehmen stehen heute an einem Wendepunkt der IT-Sicherheit. Wie sollen CISOs am besten vorgehen, um die Lücken in der Cybersicherheitsbereitschaft zu schließen?**

Wir befragten über 1.000 Sicherheits- und IT-Experten in Australien, Frankreich, Deutschland, Singapur, Großbritannien und den USA als Basis für unseren „2024 Hybrid Cloud Security Report: Lücken der Sicherheitsbereitschaft schließen“. Den vollständigen Report finden Sie hier. Die vorliegende Management-Zusammenfassung fokussiert sich auf die Erkenntnisse von mehr 230 CISOs auf der ganzen Welt, um die Themen und Prioritäten zu verstehen, mit denen diese kritische Position konfrontiert wird. Die Ergebnisse zeigen:

Regulierungen erhöhen den Druck

Die Cybersicherheit ist ins Visier der Gesetzgeber gerückt, daher entwickelt sich die Rolle des CISO weiter und umfasst heute auch Compliance und sogar rechtliche Risiken. Zudem richten Unternehmensvorstände weltweit ihre Aufmerksamkeit vermehrt auf die Cybersicherheit, sodass CISOs dringend erforderliche Unterstützung erhalten. Aber verstehen Vorstandsetagen wirklich, was CISOs für erfolgreiche Cybersicherheit benötigen?

CISOs sind sich der Lücken in der Sichtbarkeit sehr bewusst

Heute fühlt sich fast die Hälfte **(46 Prozent)** der CISOs nicht ausreichend vorbereitet, um Bedrohungen in Hybrid-Cloud-Infrastrukturen zu erkennen. Die Befragten zeigten sich besonders besorgt über verschlüsselten und East-West -Datenverkehr, der es Bedrohungsakteuren ermöglicht, sich in Unternehmensinfrastrukturen zu verbergen und unentdeckt zu bleiben. Daher sind **7 von 10** Befragten der Ansicht, dass sie mit den vorhandenen Sicherheitstools keine Sicherheitsverletzungen identifizieren können.

Tooling-Strategien gehören zu den Hauptsorgen

Die Tool-Konsolidierung beherrscht weiterhin die Prioritäten von Unternehmen. Wenn es um die Identifikation und Behebung von Sichtbarkeitslücken geht, platzieren befragte CISOs die Tool-Optimierung sowie die Investition in neue Tools als **#1 bzw. #2** der wichtigsten Sorgen.

Deep Observability definiert: Die Fähigkeit, effizient aus dem Netzwerk abgeleitete Informationen an Cloud-, Sicherheits- und Observability-Tools zu liefern. Das reduziert blind spots und senkt die Kosten für Sicherheitswerkzeuge, sodass Unternehmen ihre Hybrid-Cloud-Infrastrukturen besser schützen und verwalten können.

Zero Trust ist zum Must-have geworden

Unternehmen sind sich der Bedeutung von Zero Trust schon seit langem bewusst, jetzt aber sind verpflichtende Zero-Trust-Mandate für viele Organisationen weltweit von einem vagen Gespenst zur Realität geworden. Die USA sind hier der Vorreiter. CISOs müssen sich nun mit der praktischen Umsetzung befassen, wobei **44 Prozent** der Befragten angeben, dass „der Druck des Vorstandes, Zero Trust zu erreichen“, zu ihren drei Hauptsorgen gehört.

Einbindung des Vorstands

Vor dem Hintergrund häufiger Schlagzeilen im Zusammenhang mit Cyberangriffen haben branchenführende Unternehmen wie auch staatliche Stellen deutlich gemacht, dass Cyberrisken zu den Geschäftsrisiken gehören. Von DORA in der EU bis zu den neuen Offenlegungsvorschriften der SEC: Vorschriften zu Risikoverantwortlichkeit und Bedrohungserkennung nehmen stärker als je zuvor Unternehmensführungen in die Pflicht. Und das scheint zu funktionieren – **85 Prozent** der CISOs berichten, dass Cloud-Sicherheit jetzt auf Vorstandsebene zu den

Was sind Ihre Hauptsorgen?

DIE TOP-FIVE-ANTWORTEN DER CISOS

1. **Druck von der Vorstandsebene, Zero-Trust-Architekturen umzusetzen, ohne über die nötigen Ressourcen und Fähigkeiten zu verfügen.**
2. **Zu viele schlecht integrierte Tools führen zu Datensicherheitsvorfällen.**
3. **Neue Cybersicherheitsgesetzgebungen und Compliance-Vorschriften, die fokussierter sind und deutlichere Konsequenzen beinhalten.**
4. **Schutz des exponentiellen Wachstums von IoT/OT-Geräten.**
5. **Ausnutzung von blind spots, deren Existenz unbekannt ist.**

Als moderner CISO wissen Sie, dass sich Ihre Rolle weiterentwickelt. Sie müssen das Unternehmen gegen negative Einwirkungen isolieren, insbesondere auch hinsichtlich rechtlicher und Compliance-Risiken. Wenn wir über Risiken sprechen, gehören dazu akzeptable und inakzeptable Risiken. Gesetzgeber weisen den Unternehmensführungen heute die rechtliche Verantwortung für akzeptierte Risiken zu, sodass die Risikobereitschaft klarer definiert wird. Die folgenlose Akzeptanz von Risiken gehört der Vergangenheit an.

CHAIM MAZAL
Chief Security Officer, Gigamon

Prioritäten gehört. Unternehmensführungen arbeiten mit CISOs zusammen, um Cybersicherheitsrisiken der Unternehmen zu identifizieren und zu managen. Oberflächlich betrachtet scheinen dies gute Neuigkeiten für CISOs zu sein, denn laut **6 von 10** CISOs besteht die wichtigste Unterstützung für ihre Arbeit darin, dass Cyberrisiken zu den Prioritäten auf Vorstandsebene gehören.

Doch mit der erhöhten Aufmerksamkeit steigt auch der Druck. Auf die Frage nach ihren Hauptsorgen nannte fast die Hälfte der CISOs **(44 Prozent)** den „Druck des Vorstandes, Zero Trust zu erreichen“. Dieser Druck wird von CISOs sehr stark empfunden, während dies nur von **29 Prozent** der gesamten Befragten weltweit bestätigt wird.

Die Umfrageergebnisse verdeutlichen ein anhaltendes Dilemma für CISOs: Vorstände müssen Cyberrisiken verstehen und priorisieren, aber Vorschriften und Regulierungen werden die größten Herausforderungen nicht allein lösen. Moderne CISOs sind zunehmend damit betraut, neben technischen Anforderungen auch rechtliche und geschäftliche Risiken zu adressieren – aber sie verfügen schlicht nicht über die Ressourcen, um Unternehmen auf die nächste Generation der Cyberbedrohungen vorzubereiten und vor dieser zu schützen. Ohne technische Unterstützung besteht daher die Gefahr, dass der Vorstandsdruck einfach nur den Stress für CISOs erhöht, ohne die Security Posture zu verbessern.

Risiken verstehen

Unter den befragten CISOs zeigte sich ein allgemeiner Mangel an Vertrauen in die Fähigkeiten ihrer Organisationen, Bedrohungen zu erkennen. Knapp die Hälfte **(46 Prozent)** fühlt sich nur einigermaßen oder überhaupt nicht darauf vorbereitet, Bedrohungen in Hybrid-Cloud-Infrastrukturen zu erkennen. **48 Prozent** haben ähnliche Bedenken, wenn es um die schnelle Reaktion auf unautorisierte Zugriffe in der Hybrid Cloud geht. Obwohl dies schon kein optimistisches Bild der Lage ist, weisen die Zahlen auf ein trotzdem noch übergroßes Vertrauen hin: Nur 1 von 5 **(20 Prozent)** der CISOs gibt an, mit den vorhanden Sicherheitstools fähig zu sein, Sicherheitsverletzungen in Echtzeit zu erkennen und Schäden einzudämmen. Da sich die Cloud-

Migration weiter beschleunigt – und KI-Bereitstellungen noch mehr Cloud-Investitionen versprechen – gehört verbesserte Sichtbarkeit zu den Top-Prioritäten von CISOs, denn anders ist kein echtes Vertrauen in die Fähigkeit zur Bedrohungserkennung möglich.

Die Erkennung und Verhinderung von Angriffen ist nicht das einzige Element der Sicherheitsbereitschaft, das derzeit im Rampenlicht steht. Wenn Unternehmen das Ausmaß von Sicherheitsverletzungen nicht schnell genug verstehen und offenlegen, drohen Konsequenzen. Das ist ein häufiger Schwachpunkt von Unternehmen. Mehr als die Hälfte **(53 Prozent)** der CISOs gibt an, innerhalb der letzten zwölf Monate eine Sicherheitsverletzung erst bemerkt zu haben, als Mitarbeiter nicht auf Anwendungen zugreifen konnten. Zudem gibt **1 von 3** Befragten an, dass die Ursache (Root Cause) der Sicherheitsverletzung nicht ermittelt werden konnte. Mangelhafte Nachforschungen und Analysen nach einem Sicherheitsvorfall können schwerwiegende Folgen haben: **39 Prozent** der CISOs wurden erst durch eine Erpresserforderung auf einen ernsthaften Sicherheitsvorfall aufmerksam, während **36 Prozent** den Angriff erst entdeckten, als Unternehmensdaten im Dark Web auftauchten.

Die große Anzahl von Angriffen unter dem Radar der Sicherheitsteams zeigt, dass Bedrohungsakteure die blind spots der Unternehmen kennen und ausnutzen. Jüngste Schlagzeilen unterstützen diese Annahme, denn Geheimdienste warnen vor einem Anstieg sogenannter Living-off-The-Land-Angriffe, die von fremden Nationen unterstützt werden. Bei dieser Art von Angriffen verstecken sich Bedrohungsakteure für ausgedehnte Zeitperioden in einem kompromittierten Netzwerk und bewegen sich seitlich (lateral), um wertvolle Informationen zu sammeln und den potenziellen Schaden folgender Angriffe zu maximieren.

Schlechte Sichtbarkeit des East-West Datenverkehrs und das übermäßige Vertrauen in Log-basierte Sicherheitsüberwachung spielt den Angreifern in die Hände. Logs sind veränderbare Aufzeichnungen, die manipuliert werden können, um die Entdeckung zu verhindern. In ähnlicher Weise missbrauchen Cyberkriminelle zunehmend verschlüsselten Datenverkehr, der von Unternehmen als Sicherheitsmaßnahme eingesetzt wird. Malware, Ausbreitung und Datenabfluss werden quasi in verschlüsseltem Datenverkehr maskiert. Um diese Taktiken auszuhebeln, müssen CISOs das implizite Vertrauen im Netzwerk konsequent beenden und die vollständige Sichtbarkeit von verschlüsseltem und East-West -Datenverkehr herstellen. Derzeit berichten **7 von 10** CISOs, dass sie Schwierigkeiten haben, Einblick in verschlüsselten Datenverkehr zu erhalten. Trotzdem glauben **8 von 10** CISOs, dass verschlüsselter Datenverkehr sicher ist. Bis Unternehmen die Risiken, die durch diesen blind spots entstehen, mit ausreichenden Ressourcen adressieren, können und sollten sie kein Vertrauen in ihre übergreifende Security Posture haben.

Wie konnten Sie eine Datensicherheitsverletzung identifizieren?

56 % **Unser Team entdeckte die Bedrohung mithilfe von Sicherheits- und Observability-Tools.**

53 % **Anwender konnten nicht auf Applikationen und digitale Ressourcen zugreifen.**

43 % **Anwender meldeten verlangsamte Performance von Applikationen.**

39 % **Wir erhielten eine Erpresserforderung von den Angreifern.**

36 % **Daten unseres Unternehmens tauchten im Dark Web auf.**

Befragte konnten mehrere Antwortoptionen wählen.

Chancen und Risiken von KI managen

Vorhandene Tool-Sets reichen offensichtlich nicht aus, aber CISOs scheinen sich nicht einig zu sein, wie es weitergehen soll. **4 von 5** Befragten sagen, dass ihre Teams vom Tool Sprawl, also der ausufernden Vermehrung von Sicherheitswerkzeugen, überfordert sind. Die Überholung und Modernisierung der eingesetzten Tools hat für CISOs in den nächste zwölf Monaten hohe Priorität, da sie ein entscheidender Schritt zur Eliminierung blind spots ist. Fast zwei Drittel der CISOs nennen Tool-Konsolidierung und -Optimierung als ihre Top-Priorität **(62 Prozent)**, dicht gefolgt von Investitionen in zusätzliche Tools **(54 Prozent)**. Die Gesamtzahl der weltweit Befragten verbindet große Hoffnungen mit Sicherheitsautomatisierung und KI, 54 Prozent nennen diesen Punkt an erster Stelle. Im Vergleich dazu sind CISOs skeptischer und platzieren KI mit **46 Prozent** an vierter Stelle.

Obwohl KI von Gartner zum wichtigsten Cybersicherheitstrend des Jahres 2024 gekürt wurde, konzentrieren sich die tatsächlich Sicherheitsverantwortlichen darauf, die Grundlagen zu stärken: Beseitigung blind spots, Optimierung des Tooling und Vorbereitung auf kommende Vorschriften. Darüber hinaus haben CISOs auch KI-generierte Bedrohungen auf dem Radar, wobei **83 Prozent** davon ausgehen, das KI zu einem Anstieg der globalen Ransomware-Bedrohung führen wird. Der KI-Aufbruch bedeutet für Unternehmen gleichermaßen Chancen und Risiken. Bei der Bewertung des Potenzials für die Risikominderung bestehen deutliche Unterschiede zwischen CISOs und ihren C-Level-Kollegen. Vielleicht sind sich CISOs einfach bewusst, dass sie sowohl eine kritische Rolle bei der sicheren KI-Bereitstellung haben als auch KI-gestützte Angriffe abwehren müssen.

Dies weist auf einen allgemeinen Trend hin: Die Rolle des CISO verbreitert sich und umfasst mehr als nur Cybersicherheit, so zum Beispiel KI-Strategien, physische Sicherheit und generelle IT-Technologieentscheidungen. Aber obwohl sich die Rolle immer weiter ausdehnt, verfügen CISOs aktuell nicht über ausreichende Tools und Unterstützung, um ihre Organisationen vollständig zu schützen.

Die Bereitschaftslücke schließen

Die Unzufriedenheit der CISOs mit den vorhandenen Tool-Sets wird gespiegelt von den Vorstandsetagen, die in der Regel auf Konsolidierung und Plattformangebote pochen, um IT-Ausgaben zu reduzieren. Da aber sowohl die Konsolidierung als auch die Investition in neue Tools auf den Prioritätenlisten der Unternehmen stehen, können weder Rip & Replace-Strategien (Herausreißen & Ersetzen) noch die totale Konsolidierung über einen einzigen Hersteller der richtige Weg sein.

Stattdessen sollten sich Unternehmen darauf konzentrieren, dass vorhandene Tools effizient arbeiten und gut integriert sind, um so blind spots der Sicherheit zu beseitigen. Das erfordert Deep Observability, die Highfidelity-Daten und Netzwerktelemetrie nutzt, um über MELT-Daten (Metrics, Events, Logs und Traces) hinauszugehen. CISOs sind sich dieser Zusammenhänge wohl bewusst: **83 Prozent** stimmen zu, dass Deep Observability ein grundlegendes Element der Cloud-Sicherheit ist.

Wenn Deep Observability erreicht wird, sind CISOs und ihre Unternehmen auf die IT-Strategien der Zukunft vorbereitet. Erfolgreiche KI-Bereitstellungen müssen mit akkuraten und vertrauenswürdigen Daten gefüttert werden. **65 Prozent** der CISOs haben bereits erkannt, dass die Sichtbarkeit aller Daten oberste Priorität hat für sichere und erfolgreiche KI-Investitionen. Die Komplexität von Hybrid-Cloud-Infrastrukturen wird weiter zunehmen, während Unternehmen neue Technologien einsetzen und den Betrieb skalieren. Proaktive CISOs sollten daher Infrastrukturtechnologien einsetzen, die Netzwerk-Telemetrie effizient an das bestehende Tool-Set liefern und Sicherheitsteams in Echtzeit auf dem Laufenden halten, sodass die Deep Observability der Hybrid-Cloud-Infrastruktur jederzeit gewährleistet ist.

85 Prozent der CISOs stimmen zu, dass Deep Observability der Hybrid-Cloud-Infrastruktur entscheidend ist für den Übergang zu einem proaktiven Denkansatz und der Verhinderung von Angriffen.

Über Gigamon

Gigamon® bietet eine Deep Observability Pipeline, die effizient netzwerkbasierte Informationen 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.

Jetzt vollständigen Report herunterladen und Erkenntnisse aus Ihrer Region entdecken: gigamon.com/umfragecloud-sicherheit

Gigamon®

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

06.24_01