ISC2 Supply Chain Risk Survey: 70 Prozent der Befragten sind sehr besorgt über Cybersicherheit

Eine neue Umfrage von ISC2 bestätigt, dass Organisationen jeder Größe und jeder Branche mit mangelnder Transparenz in ihrem weitreichenden Netzwerk von Drittanbietern und Partnern zu kämpfen haben.

Aufgrund der zunehmenden Bedeutung der Cybersicherheit in der Lieferkette führte ISC2 eine weltweite Umfrage unter 1.062 Cybersicherheitsfachleuten durch. Ziel war es, den aktuellen Stand dieses drängenden Themas und der Auswirkungen auf die Cybersicherheit einzuschätzen.

Sicherheitsbedenken für die Lieferkette

In der Umfrage gaben 70 Prozent an, dass ihre Organisationen sehr oder extrem besorgt über Cybersicherheitsrisiken in ihren Lieferketten sind. Organisationen, die einen Cybersicherheitsvorfall von einem Drittanbieter oder Lieferanten bereits erlebt haben, melden deutlich häufiger hohe Besorgnisgrade (75 Prozent).

Die Ergebnisse zeigen zudem, dass 28 Prozent der Befragten in den letzten zwei Jahren einen Cybersicherheitsvorfall, der von einem Drittanbieter ausging, erlebt haben. Allerdings führen nicht alle Vorfälle bei Dritten zu direkten Auswirkungen auf das eigene Unternehmen. 47 Prozent der Teilnehmer gaben an, dass ihre Organisationen nicht direkt betroffen waren, als ihre Lieferanten einen Cybersicherheitsvorfall hatten.

Herausforderungen bei der Lieferkettensicherheit

Auf die Frage nach den größten Herausforderungen bei der Sicherheit gegen Cyberbedrohungen in der Lieferkette, dominierten der Mangel an Transparenz oder Kontrolle der Lieferanten. Viele Befragte sind zudem über die Komplexität ihrer Lieferketten besorgt und weisen darauf hin, dass sie weder die Lieferanten ihrer Lieferanten noch alle möglichen Einstiegspunkte kennen.

Zudem bestätigten die Befragten, dass Bedrohungen für die Lieferkette nicht zwangsläufig nur von außen kommen. 29 Prozent stufen Insider-Bedrohungen durch externe Dienstleister als disruptiv für ihre Organisationen ein.

Risikominimierung für die Lieferkette

Eine der größten Herausforderungen, denen Unternehmen mit ihren Lieferketten gegenüberstehen, ist der Mangel an Informationen über das inhärente Risiko, das ein Zulieferer oder eine Kette von Lieferanten darstellt. Um dieses Risiko zu mindern, führt eine Vielzahl an Organisationen (70 Prozent) regelmäßig Risikobewertungen durch, etwa zum Zeitpunkt der Vertragsverlängerung oder jährlich. Darüber hinaus prüfen 49 Prozent der Organisationen ihre Zulieferer genau während der Erstbewertung oder Einarbeitung, 26 Prozent bei Vorfällen und 25 Prozent, wenn Überwachungstools sie auf eine Bedrohung aufmerksam machen.

Aktives Risikomanagement der Lieferkette

Die befragten Organisationen verfolgen unterschiedliche Ansätze beim Risikomanagement der Lieferkette. 54 Prozent geben an, dass ihre Organisation ein dediziertes Programm für das Risikomanagement verfolgt. Dieser Prozentsatz steigt bei Großunternehmen auf 70 Prozent deutlich an. Viele Organisationen verfolgen das Risikomanagement der Lieferkette jedoch weniger formell oder überraschenderweise gar nicht. Rund 20 Prozent verlassen sich auf Verträge beziehungsweise Service-Level-Vereinbarungen (SLAs), und 16 Prozent behandeln die Risiken von Fall zu Fall. Darüber hinaus haben 10 Prozent kein formelles Programm oder keinen dedizierten Ansatz für das Management Lieferkettenrisiken – 8 Prozent dieser Befragten entwickeln allerdings derzeit ein solches.

5 Empfehlungen für mehr Sicherheit in der Lieferkette

Es liegt in der Verantwortung der Cybersicherheit, den Schutz der Lieferkette zu priorisieren. Zu den fünf wichtigsten Ratschlägen für Organisationen und Cybersicherheitsfachkräfte gehören:

- Risikobewertungen durch Dritte: Da die Software-Lieferkette für Organisationen immer wichtiger wird, sind Risikobewertungen durch Dritte gängige Praxis, um potenzielle Sicherheitsprobleme zu identifizieren. Diese Bewertungen beinhalten häufig Schwachstellenscans und Prüfungen auf Fehlkonfigurationen.
- Risikomanagement kritischer Infrastruktur: Angriffe auf kritische Infrastrukturen (CI) können erhebliche Auswirkungen auf die öffentliche Sicherheit haben – mit Folgeeffekten auf weitere CI-Sektoren, da die Lieferketten eng verflochten sind. Die Priorisierung der Sicherheit der CI-Lieferkette durch formelle Einarbeitungen und laufende Bewertungen ist unerlässlich.
- Zero-Trust-Architektur: Sicherheit bedeutet nicht nur den Perimeter zu bewachen; es geht darum, Sicherheitsprotokolle an jeder Flanke zu haben. Ein Zero-Trust-

Ansatz bietet eine ständige Gewissheit, dass jede Person dort ist, wo sie sein soll, und nur auf das zugreifen kann, was sie benötigt und wofür sie befugt ist – von On-Premise bis zur Cloud.

- Lieferantenvertragsprüfungen: Die Überprüfung und Bewertung von Lieferantenverträgen ist eine wichtige Aufgabe für Cybersicherheitsteams und Budgetinhaber. Als wichtiger Stresstest für die Lieferkette bietet dies die Möglichkeit, Schwächen und sich ändernde Bedürfnisse zu identifizieren und anzugehen. Ein guter Vertrag mit klaren Lieferergebnissen und Erwartungen ist – neben Menschen und Technologie – Teil einer Cybersicherheitsstrategie.
- Entwicklung von Cybersicherheitskompetenzen: Fachkräfte für Cybersicherheits-Governance, Risiken und Compliance (GRC), die Rahmenwerke nutzen, um Sicherheit und Datenschutz in organisatorische Ziele zu integrieren, können auf professionelle Zertifizierungen wie ISC2s CGRC zurückgreifen. Damit ist es allen Stakeholdern in der Organisation möglich, fundierte Entscheidungen für Datensicherheit, Compliance, Lieferkettenrisikomanagement und mehr zu treffen.

Über die Umfrage:
Die Online-Umfrage wurde unter 1.062 Befragten durchgeführt, die in einer Position mit Cybersicherheitsverantwortung arbeiten. Die Befragten arbeiteten in Organisationen unterschiedlicher Größe: klein (1–499 Mitarbeiter), mittlere (500–2.499 Mitarbeiter), große (2.500–4.999 Mitarbeiter) und Unternehmen (5.000+ Mitarbeiter). Die Daten wurden vom 12. bis 28. August 2025 erhoben.

Die kompletten Ergebnisse der ISC2 Supply Chain Risk Survey stehen unter diesem Link zum Download bereit.

Über ISC2
ISC2 ist die weltweit führende Nonprofit-Organisation für Cybersecurity-Experten. Mit über 265.000 zertifizierten Mitgliedern und Partnern setzen wir uns in einer immer stärker vernetzten Gesellschaft für eine sichere Cyberwelt ein. Unsere renommierten Zertifizierungen – darunter die branchenführende CISSP®-Zertifizierung – dienen Fachkräften als Nachweis ihrer Kenntnisse, Fähigkeiten und Kompetenzen in jeder Phase ihrer Karriere.
ISC2 setzt Cybersecurity auf die politische und gesellschaftliche Agenda. Wir fördern die Relevanz, Vielfalt und Dynamik der Cybersecurity-Branche durch engagierte Fürsprache, fundiertes Fachwissen und die Schulung und Zertifizierung von Fachkräften.
Mit unserer gemeinnützigen Stiftung, dem Center for Cyber Safety and Education, vereinfachen wir den Zugang zu diesem Berufszweig für angehende Nachwuchskräfte.

Erfahren Sie mehr über ISC2 und werden Sie Teil unserer Mission. Vergrößern Sie ihr Netzwerk und folgen Sie uns auf X, Facebook und LinkedIn.

Pressekontakt:

ISC2
Kiri O'Leary, Corporate Communications Professional
koleary@isc2.org

TC Communications
Arno Lücht, +49 157 52443749
Thilo Christ, +49 171 6220610
Alexandra Schmidt, +49 170 3871064
ISC2@tc-communications.de