Cyberrisiken in der Lieferkette

Verständnis von Cyberrisiken und Schutzstrategien in Lieferketten

17. November 2025

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Inhalt

Wichtige Erkenntnisse

“

Cyberrisiken in der Lieferkette haben sich zu einer der grössten Herausforderungen für Unternehmen im digitalen Zeitalter entwickelt und erfordern umfassende Strategien, die der komplexen, vernetzten Natur moderner Geschäftsbeziehungen gerecht werden.

Tom Schmidt
Partner, Cybersecurity Leader FSO Schweiz

Art und Umfang von Cyberrisiken in der Lieferkette

Globale Reichweite und Komplexität

Cybersicherheit in Lieferketten

Die Cybersicherheit in der Lieferkette schützt alle Komponenten und Beziehungen im erweiterten Netzwerk eines Unternehmens und mindert die Risiken durch Cyberbedrohungen.

Komplexität der globalen Lieferkette

Moderne Lieferketten sind global, mehrstufig und stark auf digitale Technologien angewiesen, was die Anfälligkeit für Cyberkriminelle erhöht.

Neu auftretende Cyberrisiken

Cyberrisiken in der Lieferkette erstrecken sich auf OT-Systeme, IoT-Geräte und kritische Infrastrukturen und erfordern ein umfassendes Risikoverständnis.

Auswirkungen von COVID-19 und rascher digitaler Transformation

Schwachstellen in Lieferketten

Die Pandemie hat kritische Schwachstellen in den globalen Lieferketten aufgedeckt, die sich auf die Abläufe und die Widerstandsfähigkeit verschiedener Branchen auswirken.

Schnelle digitale Transformation

Unternehmen führten schnell neue Technologien und Remote-Arbeitsregelungen ein, oft ohne ausreichende Sicherheitsüberlegungen.

Erweiterte Cyberbedrohungen

Die Verlagerung hin zur Digitalisierung schuf eine grössere Angriffsfläche und erhöhte die Möglichkeiten für Cyberkriminelle, Schwachstellen auszunutzen.

Aktuelle Bedrohungslandschaft und Angriffsvektoren

Zunehmende Häufigkeit und Raffinesse von Angriffen

Zunehmende Angriffe auf die Lieferkette

Die Angriffe auf die Lieferkette haben in den letzten Jahren deutlich zugenommen, was die wachsende Bedrohungslandschaft für Unternehmen zeigt.

Bedrohungen durch Nationalstaaten

Nationalstaatliche Akteure werden als wesentliche Bedrohung angesehen, die es mit ausgeklügelten Taktiken auf Hardware-Lieferketten abgesehen haben.

Komplexe mehrstufige Angriffe

APT-Gruppen (Advanced Persistent Threat) führen komplexe, mehrstufige Angriffe durch, die über lange Zeiträume unentdeckt bleiben und ernsthafte Risiken darstellen können.

Bedrohungsakteure	Angriffsvektoren	Mögliche Auswirkungen
Nationalstaaten, Cyberkriminelle, Insider-Bedrohungen	Kompromittierte Hardware/Software, gefälschte Komponenten, IoT, Cloud-Dienste, KI-gesteuerte Angriffe, Schwachstellen bei Anbietern und Lieferanten	Betriebsstörungen, Datenschutzverletzungen, finanzielle Verluste, Reputations-/ Marktverluste

Ransomware und Schwachstellen von Drittanbietern

Verbreitung von Ransomware

Ransomware-Angriffe werden immer häufiger, insbesondere bei Managed Service Providern, die mehrere Unternehmen gleichzeitig betreffen.

Schwachstellen von Drittanbietern

Schwachstellen von Drittanbietern stellen erhebliche Cyberrisiken dar, oft mit nur einem begrenzten Einblick in die Sicherheitspraktiken der Anbieter.

Ausnutzung menschlicher Schwächen

Cyberkriminelle nutzen häufig menschliche Schwächen aus und zielen durch Phishing und Social Engineering auf Mitarbeiter kleinerer Lieferanten ab.

Angriffe auf die Software-Lieferkette

Angriffe, die auf die Softwareentwicklung abzielen, ermöglichen das Einfügen von bösartigem Code in legitime Anwendungen, was weitreichende Risiken darstellt.

Regulatorische Rahmenbedingungen und Industriestandards

Die NIS2-Richtlinie der Europäischen Union und der Digital Operational Resilience Act

Erkennen von Cyberrisiken

Das zunehmende Bewusstsein für Cyberrisiken in der Lieferkette hat die Schaffung robuster regulatorischer Rahmenbedingungen (z. B. NIS2 und DORA) veranlasst.

NIS2 Cybersicherheit in der Lieferkette

Die NIS2-Richtlinie betont die Cybersicherheit in der Lieferkette als kritische Komponente des gesamten Cybersicherheits-risikomanagements.

DORA Cybersicherheit in der Lieferkette

Die Anforderungen von DORA an das Cyber-Risikomanagement in der Lieferkette sollen sicherstellen, dass Finanzinstitute nicht nur Risiken innerhalb ihrer eigenen Organisation managen, sondern auch robuste Kontrollen und Aufsicht auf ihr gesamtes digitales Lieferketten-Ökosystem ausweiten.

NIST-Richtlinien und ISO-Normen

NIST Cyber Supply Chain Hilfestellung

NISTIR 8276 zeigt Best Practices für das Management von Cybersicherheitsrisiken in Lieferketten auf, die für Unternehmen jeder Grösse anwendbar sind.

Integration von Cybersicherheit in das Risikomanagement

Die NIST-Sonderveröffentlichung 800-161 (Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations) enthält Richtlinien für die Integration des Risikomanagements in der Cybersicherheits-Lieferkette in die allgemeinen organisatorischen Risikoaktivitäten.

Normen ISO/IEC 27036-3:2023

ISO/IEC 27036-3:2023 bietet spezifische Leitlinien für die Sicherung von Lieferketten und geht dabei auf einzigartige Risiken bei Hardware und Software ein.

Regulierung der FINMA

FINMA Outsourcing-Rundschreiben 18/3

Bei der Auslagerung sicherheitsrelevanter Funktionen (insbesondere in der Informationstechnologie) müssen das Unternehmen und der Dienstleister vertraglich Sicherheitsanforderungen vereinbaren. Das Unternehmen muss die Einhaltung dieser Anforderungen überwachen.

FINMA Rundschreiben 23/1 Operationelle Risiken und Resilienz

Anforderungen an das Cyber-Risikomanagement entlang der fünf Funktionen des NIST Cybersecurity Framework: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Das NIST Cybersecurity Framework bietet einen umfassenden Ansatz für das Management von Cyberrisiken in der Lieferkette, indem es Cybersecurity Supply Chain Risk Management (C-SCRM) in die Governance- und Risikomanagementpraktiken von Unternehmen integriert.

Risikobewertung und Managementstrategien

Wichtige Praktiken

Systematisches Risikomanagement

Ein systematischer Ansatz zur Identifizierung, Bewertung und Priorisierung von Risiken im gesamten Lieferanten-Ökosystem ist für ein effektives Cybersecurity Supply Chain Risk Management (C-SCRM) unerlässlich.

Wichtige Praktiken des NIST-Frameworks

Das NIST-Rahmenwerk (NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management) beschreibt acht wichtige Praktiken, die für die Erstellung eines effektiven Programms für das Risikomanagement in der Cyber-Lieferkette entscheidend sind.

Cybersicherheit in der Lieferkette

- **Integration:** Anforderungen an die Cybersicherheit in Verträgen
- **Sicherer SDLC:** Softwareintegrität vom Code bis zur Bereitstellung
- **Vulnerability Management:** Regelmässige Tests und Behebung von Schwachstellen
- **Incident Response:** Koordination über alle Parteien hinweg

Kontinuierliche Überwachung

Kontinuierliche Überwachung

Eine kontinuierliche Überwachung ist unerlässlich, um sich an die sich entwickelnde Bedrohungslandschaft anzupassen und die Sicherheitslage der Lieferanten regelmässig zu bewerten.

Recht auf Audit

Regelmässige Durchführung von Sicherheitsaudits beim Drittanbieter / Lieferanten – entweder durch die eigene interne Revisionsabteilung oder mit Unterstützung externer Parteien.

Zertifizierungen

Vertrauen auf international anerkannte Zertifizierungen wie ISO 27001. Wichtig ist, den zugrundeliegenden Geltungsbereich und die Erklärung zur Anwendbarkeit des Zertifikats zu verstehen.

ISAE 3000 / SOC 2 Berichte

Vertrauen auf international anerkannte Berichte wie ISAE 3000 oder SOC 2. Die Berichte sollten sich mit der operativen Wirksamkeit der Kontrollen befassen (hinreichende Sicherheit).

Incident Response Fähigkeiten

Verfahren für Vorfälle in der Lieferkette

Die Entwicklung spezifischer Incident-Response-Verfahren für Supply-Chain-Szenarien ist entscheidend, um die Auswirkungen von Angriffen zu minimieren.

Kommunikationsverfahren

Die Festlegung klarer Kommunikationsverfahren mit den Beteiligten bei Vorfällen verbessert die Transparenz und Koordination.

Notfallpläne

Die Pflege von Notfallplänen für Lieferantenausfälle umfasst die Identifizierung alternativer Lieferanten für kritische Komponenten und Dienstleistungen.

Präventive Massnahmen und Best Practices

Lieferantenauswahl und vertraglicher Schutz

Beurteilung von Lieferanten

Führen Sie vor dem Onboarding von Lieferanten gründliche Bewertungen durch, um die Verpflichtung potenzieller Anbieter gegenüber Best Practices für die Cybersicherheit zu beurteilen.

Vertraglicher Schutz

Legen Sie grundlegende Sicherheitserwartungen durch vertragliche Vereinbarungen fest, einschliesslich Cybersicherheitsanforderungen und Verantwortlichkeiten.

Laufende Compliance-Überprüfung

Fügen Sie in den Verträgen Bestimmungen für Sicherheitskontrollen, Benachrichtigungen über Vorfälle und Audits hinzu, um die Einhaltung der Vorschriften in der gesamten Lieferkette sicherzustellen.

Zero-Trust-Architektur, SBOM-Implementierung und Quellcode-Scanning

Zero-Trust-Prinzipien

Die Zero-Trust-Architektur erhöht die Sicherheit der Lieferkette, indem sie eine kontinuierliche Überprüfung von Benutzern und Geräten erfordert.

Dieser Ansatz schränkt den Zugriff auf notwendige Funktionen ein und reduziert so die potenziellen Auswirkungen von Sicherheitsverletzungen.

Software-Stückliste (SBOM)

Die Implementierung von SBOMs hilft Unternehmen, Risiken in der Software-Lieferkette zu managen, indem alle Komponenten und Abhängigkeiten identifiziert werden.

Quellcode Security Analyzer

Quellcode Security Analyzer untersuchen den Quellcode, um Schwachstellen zu erkennen und zu melden, die zu Sicherheitslücken führen können.

EY | Building a better working world

EY schafft neue Werte für seine Mandanten, die Gesellschaft und den Planeten insgesamt. Damit leistet EY einen wichtigen Beitrag für eine bessere Welt und stärkt dabei das Vertrauen in die Kapitalmärkte.

Mithilfe von Daten, KI und modernsten Technologien unterstützen die Teams von EY ihre Mandanten dabei, die Zukunft mit Zuversicht zu gestalten und Antworten auf die drängendsten Fragen von heute und morgen zu finden.

Die Teams von EY decken ein breites Portfolio an Dienstleistungen ab, das die Bereiche Assurance, Consulting, Tax and Law und Strategy and Transactions umfasst. Fundierte Branchenkenntnisse, ein global vernetztes, multidisziplinäres Netzwerk und vielfältige Ökosystem-Partner ermöglichen es den Teams von EY, ihre Mandanten in mehr als 150 Ländern und Gebieten mit ihren Dienstleistungen zu unterstützen.

Sie geben alles, um die Zukunft mit Zuversicht zu gestalten.

ED MMYY

ey.com/ch