

KONTROLLEN SIND GUT, TRANSPARENZ IST BESSER

Das American Institute of Certified Public Accountants (AICPA) hat ein Rahmenwerk für die Berichterstattung über das Risikomanagement von Lieferketten präsentiert. Die System- und Organisationskontrollen für die Lieferkette (SOC for Supply Chain) sind für Unternehmen ein vertrauensbildendes Instrument.

Komplexität gestiegen. Herstellung und Vertrieb von Produkten und Dienstleistungen sind komplexer und vernetzter denn je, u. a. aufgrund des Internet of Things (IoT) und der Digitalisierung. Neue Technologien und Organisationsformen verbinden erzeugende, zuliefernde und handelnde Unternehmen enger mit Geschäftspartnern und Kundinnen.

Die Pandemie hat verdeutlicht, dass die Anfälligkeit der vernetzten und globalisierten Lieferketten seit Jahren – von der Öffentlichkeit fast unbemerkt – gestiegen ist. Dieser Trend wächst mit der Digitalisierung. Zu den Schlüsselrisiken gehören die Verfügbarkeit von Rohstoffen, Halbfabrikaten und Produkten oder die Abhängigkeit von Monopolanbietenden, aber vermehrt auch Datenschutzverletzungen und Angriffe aus dem Cyberspace. Zum einen ist das Risiko von Produkten mit IoT-Konnektivität hoch. Zum anderen hat die Pandemie einen Digitalisierungsschub ausgelöst und bietet Cyberkriminellen neue Angriffsflächen. Daher wird der Ruf nach mehr Transparenz in der Lieferkette lauter.

Branchenübergreifender Standard. Dem Bedürfnis nachkommend hat das AICPA im März 2020 ein Rahmenwerk vorgestellt mit Kriterien für die freiwillige Berichterstattung über System- und Organisationskontrollen für die Lieferkette in einem SOC-Bericht. Die Kriterien sind branchenunabhängig anwendbar und geben der Offenlegung des Risikomanagements von Lieferketten einen institutionalisierten, prüfbareren Rahmen. Wie bei anderen SOC-Berichten müssen Unternehmen die Lieferkette, ihre Systeme und Betriebsprozesse beschreiben. Grundlage der Beschreibung ist ein Kriterienkatalog (DC 300). Der Bericht enthält zudem einen aus-

föhrlichen Nachweis der Implementierung und Wirksamkeit interner Kontrollen nach den AICPA Trust Services Criteria (TSP), um die mit Sicherheit, Verfügbarkeit, Integrität, Vertraulichkeit oder Datenschutz verbundenen Risiken zu minimieren. Die TSP-Kriterien entsprechen denen einer SOC-2-Prüfung.

Vorteile. Mithilfe des SOC-Berichts für die Lieferkette können Unternehmen, deren Kundschaft sowie Wirtschaftsprüfer nachweisen, dass Instrumente und interne Kontrollen etabliert sind, mit denen sich zentrale Lieferkettenrisiken identifizieren, bewerten, adressieren und minimieren lassen.

Das Modell der «einmaligen Bewertung zur mehrfachen Berichterstattung» hilft, die Anzahl unabhängiger Anfragen von bestehender oder potenzieller Kundschaft zu reduzieren und Mehrfachprüfungen durch Nutzer mit denselben Lieferantinnen zu vermeiden. Die Prüfung eines SOC-Berichts für die Lieferkette gehört zu den komplexesten und aufwendigsten. Doch ist ein solcher Bericht ein wichtiges Kommunikationstool, um Gewissheit zu vermitteln, dass Produkte und Informationen innerhalb der Lieferkette sicher und verfügbar sind. So schafft ein Unternehmen maximale Transparenz über seine ganze Wertschöpfung hinweg und stärkt das Vertrauen seiner Kunden und Geschäftspartnerinnen in sich und seine Marke.

Ausblick. Risiken in der Lieferkette werden seit der Pandemie stärker wahrgenommen. Noch fordern schweizweit nur wenige Kundinnen von ihren Lieferbetrieben einen SOC-Bericht für die Lieferkette und von ihren Wirtschaftsprüfern dessen unabhängige Prüfung. Die SOC-Berichterstattung über Lieferketten ermöglicht weitsichtigen Unternehmen einen risikobasierten Fahrplan, um Risiko- und Qualitätsmanagement sowie Compliance-Prozesse weiterzuentwickeln und die wesentlichen Risiken in der Wertschöpfung noch gezielter anzugehen. ■



RALF HOFSTETTER,
DIRECTOR, TRUST &
TRANSPARENCY SOLUTIONS
LEADER, CISA, CISSP,
ISO 27001 LEAD AUDITOR,
PWC SCHWEIZ



CRISTIAN MANGANIELLO,
MBA ROCHESTER-BERN,
EIDG. DIPL. WIRTSCHAFTS-
INFORMATIKER, PARTNER
RISK AND COMPLIANCE
MANAGEMENT SERVICES,
PWC SCHWEIZ