Praxistipps

- **Führen Sie Inventar über Ihre Drittanbieter:** Vielen Organisationen fehlt der Überblick über ihre Drittanbieter. Inventar zu führen, ist jedoch mehr, als eine Liste aller Anbieter zu erstellen. Dazu gehört auch das Scannen von Web-Datenverkehr, Workstations und Gateways auf Schatten-IT, die Überprüfung von Rechnungen und Kreditkartentransaktionen sowie Selbstauskünfte der Geschäftsbereiche im Rahmen der Business-Continuity- und DR-Planung. Um verborgene Abhängigkeiten zu erkennen und Risiken zu beheben, sind regelmäßige Updates des Inventars unerlässlich.

- **Klassifizieren Sie Drittanbieter nach ihrem Risikolevel:** Entwickeln Sie ein Risikomodell, um die möglichen Bedrohungen der einzelnen Zulieferer zu bewerten. Wenden Sie je nach Risikolevel Nachverfolgungen, vertragliche Verpflichtungen und Kontrollmaßnahmen an und stellen Sie sicher, dass diese vom Supplier Management Team umgesetzt werden.

- **Optimieren Sie Ihre Risiko-Assessments:** Ergänzen Sie traditionelle Fragebögen durch Vor-Ort-Prüfungen, Penetrationstests und Perimeter-Scans, um technische Risiken präziser zu bewerten. Beachten Sie auch menschliche Faktoren, wie die Security Awareness und Sicherheitskultur Ihrer Drittanbieter.

- **Isolieren Sie Kollaborationsbereiche:** Halten Sie Kollaborationsbereiche von Ihren kritischen Systemen getrennt. So können Sie die Auswirkungen eines Angriffs auf die Systeme Ihres Zulieferers für Ihre Organisation minimieren.

- **Diversifizieren Sie Ihre Lieferkette:** Machen Sie sich nicht zu abhängig von einem einzelnen Drittanbieter. Stellen Sie sicher, dass Sie bei Bedarf die nötige operationale Flexibilität haben, um schnell auf Alternativen umzulenken und bei einem Angriff auf wichtige Partner Ihr eigenes Risiko zu reduzieren.

> Vor dem Kauf von Software müssen wir sicherstellen, dass bei ihrer Entwicklung Sicherheitsaspekte beachtet wurden. Dazu fordere ich Berichte und Informationen zu Sicherheitskriterien an und überprüfe, dass die Entwicklungsmethoden sicher sind.

Lars Kukuk
CISO der Bundesagentur für Arbeit