Sicherer Datenaustausch in Wertschöpfungs-netzwerken

Autor: Ralf Keuper

Juni 2024

EINLEITUNG

Wenn es um den Datenaustausch mit Dritten geht, ist die Zurückhaltung in den KMUs noch stark ausgeprägt. Die Sorge ist groß, dass sensible Daten in die falschen Hände geraten oder zweckentfremdet werden könnten.

Aktuell werden die Risiken daher als zu hoch einschätzt. Dabei ist es gar nicht mal so sehr die Frage, ob die Daten sicher von A nach B übertragen werden können. Hier ist das Vertrauen in die Verschlüsselungstechnologien durchaus vorhanden. Schwerer wiegt dagegen, wenn sich sensible Maschinen-, Prozess-, Qualitäts- und Energiedaten außerhalb der eigenen Kontrolle bei Dritten befinden. Stand heute kann nicht ausgeschlossen werden, dass Dritte auf irgendeine Weise in der Lage sind, die Anwendungsfälle zu rekonstruieren.

Andererseits erfordert die Zusammenarbeit in Wertschöpfungsnetzwerken ein Mindestmaß an der Bereitstellung sensibler Daten. Abgesehen davon setzt die Entwicklung datenbasierter Geschäftsmodelle in vielen Fällen eine bestimmte Menge an Daten für das Training von KI-Modellen voraus. Die meisten KMUs verfügen jedoch nicht über die dazu nötige Datenbasis. Damit besteht die Gefahr, dass die KMUs bei der Digitalisierung ihrer Geschäftsmodelle von den großen Unternehmen abgehängt werden, die über die nötigen technischen, personellen und organisatorischen Kapazitäten verfügen. Ein Weg könnte der Zusammenschluss mehrerer KMUs zu einer Datenkooperation oder Datengenossenschaft sein.

Mittlerweile stehen einige Verfahren und Technologien zur Verfügung, die sich jedoch noch im Anfangsstadium befinden. Am bekanntesten dürfte hierzulande GAIA-X sein, die europäische Dateninfrastruktur, welche die Datensouveränität der Unternehmen sicherstellen soll. Deren primäres Ziel ist es, die Abhängigkeit der europäischen Wirtschaft von den sog. Hyperscalern, wie Amazon, Microsoft und Google, zu verringern. Gemeinsame Datenräume auf Basis von GAIA-X

könnten KMUs neben dem sicheren Austausch der Daten auch den Zugang zu großen Datenpools verschaffen.

Auf dem Gebiet neuer Technologien sind Confidential Computing, Multi Party Computation, Federated Learning und der Einsatz synthetischer Daten zum gegenwärtigen Zeitpunkt vielversprechend. Der Vorteil dieser Lösungen besteht darin, dass keine realen Daten übertragen oder für Auswertungszwecke verwendet werden.

Unter den kommerziellen Anwendungen stechen derzeit die Industrie Clouds der Hyperscaler hervor.

Die KMUs stehen vor der schwierigen Frage, auf welche Lösung und welchen Trend sie setzen sollen, was angesichts der Vielzahl der zur Wahl stehenden Optionen kaum zu bewältigen ist.

Der vorliegende Report dient dem Zweck, den aktuellen Stand an verfügbaren Lösungen für den sicheren Datenaustausch in WS-Netzwerken zu veranschaulichen, um dadurch vor allem KMUs einen ersten bzw. besseren Überblick über die Thematik zu verschaffen.