Cybersecurity-Strategie für Lieferketten

Internationale Lieferketten sind fragil – je länger die Kette ist, desto anfälliger ist sie für negative Einflüsse von außen. Insbesondere Cyber-Angriffe haben das Potenzial, die Lieferkette empfindlich zu stören: Indem Cyber-Kriminelle Unternehmen angreifen, beeinträchtigen sie alle folgenden Glieder der Lieferkette. Ihr Ziel ist dabei häufig, wertvolle Daten zu entwenden. Allerdings kann auch eine gezielte Störung des Betriebsablaufs gewollt sein. Insbesondere staatliche Akteure werden in Zukunft verstärkt dazu übergehen, Lieferketten zu stören, um beispielsweise Versorgungsengpässe zu schaffen. Eine Cybersecurity-Strategie für Lieferketten ist entsprechend von großer Bedeutung.

Lieferkettengesetz: Jeder Teil der Lieferkette muss geschützt sein
Das Lieferkettengesetz verpflichtet Unternehmen dazu, die Sicherheit ihrer Lieferketten im Detail zu überwachen und zu verbessern. Daher ist es zunächst einmal wichtig, dass Unternehmen enge Beziehungen zu ihren Lieferanten aufbauen und sich regelmäßig über mögliche Sicherheitsbedrohungen austauschen. Eine wirksame Cybersecurity-Strategie für Lieferketten beinhaltet darüber hinaus die Identifikation von Schwachstellen in den Lieferkettenprozessen und -systemen und die Implementierung von Maßnahmen zur Verbesserung der Sicherheit – konkret der Investition in IT-Infrastrukturen. Dazu gehören zum Beispiel die Einführung von Zugangskontrollen und Authentifizierungsverfahren, die Verwendung von Verschlüsselungstechnologien und die regelmäßige Durchführung von Sicherheitsüberprüfungen.

Ein weiterer relevanter Aspekt zum Schutz vor Supply-Chain-Angriffen ist der Mensch selbst: Cyberkriminelle versuchen vor allem, über Mitarbeitende, egal ob im eigenen Unternehmen oder bei Partnerunternehmen, bei Lieferanten etc., in IT-Infrastrukturen zu gelangen. Am Anfang steht häufig eine täuschend echt aussehende Phishing-Mail, bei der selbst Cyber-Security-Profis erst spät Verdacht schöpfen würden. Kommt der oder die Mitarbeitende den Anweisungen in der Mail nach, haben die Angreifer:innen ihr Ziel erreicht und kompromittieren das Netzwerk. Die Folgen sind dramatisch und reichen von Störungen im Betriebsablauf, über Umsatzeinbußen bis hin zu Reputationsverlust. Bis der Schaden behoben ist, kann viel Zeit verstreichen – Zeit, in denen Dienstleistungen und Produkte für nachfolgende Unternehmen der Lieferketten nicht zur Verfügung stehen. Um sicher zu bleiben sollten Organisationen deshalb die Sensibilität ihrer Mitarbeitenden gegenüber Cyberbedrohungen aufrecht erhalten, indem sie regelmäßig E-Learnings zu den Themen Cyber-Sicherheit anbieten.