Sicherheit in der Lieferkette – Risiken und Maßnahmen

Für Unternehmen, ganz gleich welcher Branche, hat die Sicherheit der Lieferkette hohe Priorität, denn Störungen diesbezüglich können schnell den gesamten Geschäftsbetrieb gefährden. Kommt es zu Schwachstellen oder Ausfällen innerhalb der Lieferkette, drohen unnötige Kosten, ineffiziente Lieferpläne und Reputationsschäden. Darüber hinaus kann die Lieferung von Produkten, die manipuliert oder nicht autorisiert wurden, für Schäden beim Kunden sorgen und entsprechende Klagen mit sich bringen.

FÜR DIE KONTINUITÄT des Geschäftsbetriebs ist es daher äußerst wichtig, dass Unternehmen mögliche Risiken frühzeitig erkennen – und dass diese Risiken dann effektiv gemanagt sowie angemessene Maßnahmen ergriffen werden.

Lieferkettensicherheit als Teil des Supply Chain Managements

Die Sicherheit der Lieferkette ist ein bedeutender Aspekt des Supply Chain Managements (SCM), das sich auf das Risikomanagement von externen Lieferanten, Anbietern, Logistik, Transport und weiteren Faktoren konzentriert. Hierbei müssen Lösungen gefunden werden, wie Firmen ihren Geschäftsbetrieb auch in Ausnahmesituationen aufrechterhalten können. Es gilt somit, Risiken zu identifizieren, zu analysieren und diese dann möglichst in den Griff zu bekommen. Der Aufbau eines solchen Managementsystems ist unverzichtbar, um Schwachstellen in der weltweiten Supply Chain zu lokalisieren und gezielt gegenzusteuern. Zudem können Security-Managementlösungen helfen, Lieferketten vor physischen und Cyberbedrohungen zu schützen. Eine krisensichere Supply Chain sollte somit oberste Priorität haben, um denkbare Risiken von Betriebsunterbrechungen zu minimieren.

Physische Risiken und Cyberbedrohungen

Lange Zeit konzentrierte man sich bei der Sicherung der Lieferkette hauptsächlich auf die physische Sicherheit und Integrität, also um Risiken durch interne und externe Quellen wie Diebstahl, Sabotage oder etwa durch Natureinflüsse. Heute spielen Cyberbedrohungen bei den Sicherheitsrisiken für die Lieferkette eine zunehmend wichtige Rolle. Diese Bedrohungen beziehen sich auf Schwachstellen in den IT- und Software-Systemen – und hier die Risiken zu minimieren ist ungleich schwieriger. Seit einigen Jahren nehmen Hacker-Angriffe auf Lieferketten zu. Schuld daran ist nicht nur die sich verstärkende Digitalisierung in der Coronakrise – auch anhaltendeSorglosigkeit, unzureichende Sicherheitsarchitektur und fehlende Investitionsbereitschaft seitens der Unternehmen machen es Angreifern leicht. Hacker wissen um die Fragilität der globalisierten Wertschöpfungsketten und verschieben ihren Aktionsradius deshalb zunehmend in diesen Bereich.

Risiko Fremdsoftware

In vielen Unternehmen kommt innerhalb ihrer Lieferkette Software zum Einsatz, die von externen Firmen entwickelt wurde. Zudem können und sollten Unternehmen nicht davon ausgehen, dass die von ihnen verwendete Software unbedingt sicher ist. Eine weitere Gefahr: Weil zwischen Unternehmen, Lieferanten und Wiederverkäufern eine enge Zusammenarbeit oftmals unabdingbar ist, sind in diesen Fällen Computernetzwerke miteinander verwoben und sensible Daten werden gemeinsam genutzt. Diese Situation kann zur Folge haben, dass ein Einbruch in das Datennetzwerk einer Firma gleichermaßen viele Unternehmen betrifft. Das führt wiederum dazu, dass Hacker nicht die gewünschte Firma direkt angreifen, sondern lieber die schwächste Stelle innerhalb der Lieferkette als Zugang nutzen, um ihre Ziele zu erreichen. Kriminelle können durch sogenannte Ransomware großen Schaden anrichten und sie haben nach erfolgreichem Angriff oft ohne großen Aufwand die Möglichkeit, danach die sogenannten Infektionen weiterzuverbreiten.

Vorgehen gegen Lieferkettenrisiken

Es gibt unterschiedliche Vorgehensweisen, um Lieferkettenrisiken zu minimieren; hundertprozentiger Schutz ist jedoch nicht realisierbar. Aber mit den richtigen Maßnahmen kann eine Sicherheitsstufe erreicht werden, die einen reibungslosen Ablauf ermöglicht und im Falle eines Störfalles eine schnelle Erholung begünstigt. Da sich Lieferketten für jedes Unternehmen

anders definieren und viele verschiedene Organisationen daran beteiligt sein können, gibt es keine Patentlösung für Richtlinien oder Best Practices. Es existiert somit kein allgemeingültiges Regelwerk an Maßnahmen, das jede Situation abdeckt. Im Folgenden sind einige erfolgsversprechenden Faktoren aufgeführt.

Erfolgsfaktor: Schutz vor physischen Risiken

Häufig gehen Unternehmen gegen diese Gefahr vor, indem sie die Abhängigkeiten in ihren Lieferketten zu reduzieren versuchen. Sendungen werden nachverfolgt und behördliche Papiere überprüft. Darüber hinaus können Lieferanten verpflichtet werden, ihre Lieferungen nach bestimmten Qualitätsrichtlinien zu sichern. Wer zudem mehrere Lieferanten beauftragt, stellt damit seine lückenlose Versorgung mit Waren sicher. Zudem können externe Inspektoren vor Ort in Lagerhäusern oder Produktionsanlagen Mengen- und Qualitätsprüfungen durchführen. Sendungen zu protokollieren, zu bewachen oder auch vor und nach dem Versand zu kontrollieren hilft, Manipulationen oder Diebstahl zu vermeiden.

Erfolgsfaktor: Defense in depth

Eine umfassende Security-Strategie für die Lieferkette erfordert in der Regel einen Defense-in-depth-Ansatz. Unter „Defense in depth" versteht man den koordinierten Einsatz mehrerer Sicherheitsmaßnahmen zum Schutz der Integrität von Informationen. Dabei werden alle Aspekte der Unternehmenssicherheit abgedeckt – bei Bedarf bewusst redundant. Darüber hinaus müssen alle Regularien wie Zollbestimmungen, Datenschutz-Grundverordnung (DSGVO) oder auch das IT-Sicherheitsgesetz berücksichtigt werden.

Erfolgsfaktor: IT-Sicherheitsprophylaxe

Für Unternehmen gibt es durchaus schon zu überschaubaren Kosten Schutzmaßnahmen vor IT-Risiken. Dazu zählen eine ausgereifte Cyberhygiene ebenso wie ein solides Risikomanagement. Viele Gefahren können bereits durch einfach zu etablierende und erprobte Praktiken abgewehrt werden. Gegen die gängigsten Phishing-Attacken helfen beispielsweise regelmäßige Updates, Anti-Ransomware-Toolkits und Mitarbeiterschulungen. Eine Multi-Faktor-Authentifizierung für sensible IT-Bereiche ist ebenfalls unbedingt empfehlenswert. Auch vorab erprobte Krisen- und Reaktionspläne können im Fall eines Ausfalls die Folgekosten beträchtlich mindern.

Erfolgsfaktor: Lieferantenaudits

Professionelle Lieferantenaudits können bei der nachhaltigen Auswahl, bei der Bewertung und Entwicklung neuer oder bestehender Lieferanten helfen. Es gilt, die aktuellen Leistungen des Lieferanten zu ermitteln und diese regelmäßig mit dem zwischen beiden Seiten vertraglich vereinbarten Soll-Zustand zu vergleichen. Unternehmen erhalten dadurch einen umfassenden Eindruck über die Leistungen ihrer Zulieferer und deren Subunternehmer nach vordefinierten Kriterien. Dabei geht es beispielsweise um Compliance-Richtlinien, Menschenrechte, Arbeitsbedingungen oder Umweltaspekte. Im Zuge des Lieferantenaudits definiert das Unternehmen somit wichtige Qualitätsziele; zudem werden dadurch die Lieferantenleistungen auch international vergleichbar. Dies schafft eine belastbare Entscheidungsgrundlage für oder auch gegen eine neue bzw. erneute Auftragsvergabe.

Erfolgsfaktor: ISO 28000

Das ISO 28000-Zertifikat ist ein internationaler Standard. Die Norm bietet einen Best-Practice-Rahmen zur Verringerung der Risiken für Menschen und Fracht innerhalb der Lieferkette. Sie hilft zudem dabei, potenzielle Sicherheitsrisiken im Logistikbereich zu managen und zu mindern, und zielt auf Bedrohungen wie Terrorismus, Betrug und Piraterie ab. Durch die verbesserte Transparenz der Lieferkette und die Verringerung von Lieferketten-Unterbrechungen kann die ISO 28000 Unternehmen dabei unterstützen, Auswirkungen von Sicherheitsvorfällen zu mindern.

Die Norm wurde im Jahr 2007 von der International Organization for Standardization (ISO) herausgegeben; es war der erste internationale Managementsystemstandard für Lieferkettensicherheit. Die internationale Norm hierfür wird derzeit überarbeitet, die neue Version soll Anfang 2022 veröffentlicht werden. Sie wird den Standard an andere ISO-Managementsystemnormen angleichen sowie die Klarheit und Konsistenz erhöhen. Unternehmen, die bereits nach ISO 28000:2007 zertifiziert sind, sollten bei der Umstellung auf ISO 28000:2022 keine Probleme haben.

Erfolgsfaktor: Transparenz

Unternehmen, die auf mehr Transparenz in ihrer gesamten Lieferkette setzen, sind gut aufgestellt für die wachsenden Herausforderungen der kommenden Jahre in puncto Qualitätssicherung. Ganz gleich ob sich diese aus unvorhergesehenen Krisensituationen, steigenden Erwartungen von Kundenseite und Unternehmen oder aus gesetzlichen Anforderungen ergeben. Transparenz gilt heute ganz klar als einer der zentralen Erfolgsfaktoren im modernen Lieferantenmanagement.

Neues Lieferkettengesetz

Am 11. Juni 2021 wurde das „Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten" verabschiedet. Es schafft einen rechtlichen Rahmen, um den Schutz der Umwelt, Menschen- und Kinderrechte entlang globaler Lieferketten zu verbessern. Zudem verpflichtet es Unternehmen ab einer bestimmten Größe dazu, ihrer Verantwortung in der Lieferkette besser nachzukommen. Bei Nichteinhaltung der neuen Vorgaben zu sozialen und ökologischen Mindeststandards innerhalb der Lieferkette drohen Imageverlust, Umsatzeinbußen, Bußgelder und der Ausschluss von Vergabeverfahren des Bundes. Durch das neue Gesetz gewinnen Transparenz und Risikomanagement entlang der gesamten Lieferkette weiter an Bedeutung.

Fazit

Es gibt heute für Unternehmen vielfältige Möglichkeiten, die Sicherheit ihrer Lieferkette zu optimieren und zu schützen. Ob physische Bedrohungen oder Cyber-Risiken: An einem transparenten Security-Management führt kein Weg vorbei. Und ganz gleich welche Maßnahmen zur Verbesserung der Lieferkettensicherheit ergriffen werden, sollten keine zu großen Kompromisse gemacht werden und sich in jedem Fall für qualitativ hochwertige Lösungen entschieden werden. Das reicht von den IT-Sicherheitsmaßnahmen bis zu den Lieferantenaudits. Für Unternehmen, die hier am falschen Ende sparen, kann es im Ernstfall richtig teuer werden – oder sogar deren Existenz kosten.

bedürfnis nach individuelleren Langzeitangeboten nach. Auch die pflegenden Angehörigen sollen entlastet und gestärkt werden, unter anderem durch eine Dynamisierung des Pflegegeldes und den Ausbau haushaltsnaher Dienstleistungen.

Ebenfalls ein Teil der Langzeitpflege ist der stationäre Sektor, also die Pflege im Heim. Dort ist es über die Jahre zu einer Kostenexplosion der Eigenanteile gekommen, die viele Menschen in die Altersarmut treibt. Der Gesetzgeber beabsichtigt nun, für Planbarkeit zu sorgen. Allerdings bleibt abzuwarten, ob es dann allein um die Pflegekosten oder auch um die gleichzeitig gestiegenen Investitions- und Wohnkosten geht.

Der Mensch als Kunde der Pflege im Krankenhaus taucht im KV nicht auf. Das entspricht einer traditionellen Sicht zur Stellung der klinischen Pflege, die bei allen Fortschrittsversprechen, die das Regierungspapier parat hält, doch an einigen Stellen durchschimmert und klinische Versorgung schlicht durch die Brille der Medizin betrachtet.

Rat und Resistenz

Es bleibt zu hoffen, dass es nicht auch der Pflegequalität so geht. Denn ihr sind keine Vorhaben oder Ideen im KV gewidmet und sie spielt nur mittelbar eine Rolle. Aber es ist wünschenswert, wenn das, was die Koalition auf Seite 80 in den KV geschrieben hat, der Leitsatz für alle Neuerungen und Änderungen in den Sozialgesetzbüchern wäre, dort steht (Zitat): „Wir sorgen für eine bedarfsgerechte Gesundheitsversorgung und eine menschliche und qualitativ hochwertige Medizin und Pflege."

Wichtige Voraussetzungen für die Qualitätssicherung sind Transparenz und Kunden-Empowerment. Dafür wollen die Koalitionäre zum einen die Patient:innenrechte stärken und deren Vertretung in der Selbstverwaltung des Gesundheitswesens ein stärkeres Gewicht geben. Beim Einstieg und am Anfang der Pflegebedürftigkeit stehen Klient:innen und ihre Angehörigen aber vor einer völlig unübersichtlichen Beratungslandschaft. In Bezug auf die Beratung zur Pflege bleibt der KV jedoch seltsam stumm.

Rot, gelb, grün oder pandemiegrau

Zugegeben, die Regierung ruft im KV einige der dringenden Herausforderungen in der Pflege auf und beschäftigt sich ausdrücklich auch mit den Folgen der Pandemie. An vielen Stellen wird aber bereits sichtbar, dass es sich um ein Kompromisspapier handelt. Besonders gute Vorschläge aus einigen Wahlprogrammen, die für sich genommen große Fortschritte bedeutet hätten, sind offenbar in einer koalitionären Zurückhaltung untergegangen und bei den Verhandlungen geschluckt worden.

European Foundation for Quality Management

Auch 2021: EFQM zeichnet DGQ als Partnerorganisation aus

DIE DGQ FREUT SICH ÜBER diese erneute Ehrung: Nach 2020 hat die European Foundation for Quality Management (EFQM) die DGQ auch für 2021 zur Outstanding Certified Training Organisation ernannt. Damit würdigt die EFQM das Engagement und die Leistung der DGQ als eine Organisation, die Weiterbildungen und Beratung in diesem Bereich anbietet.

Das EFQM Modell ist international anerkannt und dient der Analyse von Organisationen, zur Organisationsentwicklung sowie zur Organisationsbewertung. Kein anderes Modell seiner Art wird in so viele Sprachen übersetzt und weltweit eingesetzt.

Neues EFQM Modell 2020

2020 hat die EFQM eine grundlegend überarbeitete Version des EFQM Modell veröffentlicht, das Organisationen noch besser dabei unterstützt, sich an Krisensituationen anzupassen. Es trifft detaillierte Annahmen, wie Organisationen unter den aktuellen Bedingungen erfolgreich handeln können. Dazu berücksichtigt das Modell zwei Konzepte, die unverzichtbar sind: Die Auseinandersetzung mit dem Ecosystem einer Organisation und die 17 Nachhaltigkeitsziele der Vereinten Nationen.

Die DGQ verbindet eine langjährige Partnerschaft mit der EFQM. Sie bietet verschiedene Trainings und umfassende Beratung zur Organisationsentwicklung mit dem EFQM Modell an. Sie erweitert ihr Spektrum in diesem Bereich kontinuierlich durch E-Trainings.

https://shop.dgq.de/themen/e-learning