Hermes-Barometer IT- und Datensicherheit
Sorge von Unternehmen vor Cyberangriffen auf Lieferketten nimmt zu

Mittwoch, 01.06.2022

Die Bedrohung für Lieferketten durch Cyberkriminalität ist in den vergangenen Jahren gestiegen. So setzen sich immer mehr Unternehmen verstärkt mit den möglichen Gefahren sowie Sicherheitsmaßnahmen auseinander. Insbesondere die Sicherheit der Daten von Kundinnen und Mitarbeitern stehen im Fokus. Dies zeigen die Ergebnisse des 16. Hermes-Barometers „IT- und Datensicherheit in der Supply Chain" von Hermes Germany, einer Umfrage unter 150 Logistikverantwortlichen deutscher Unternehmen.

13 Prozent der befragten Unternehmen waren tatsächlich schon von Störungen oder Ausfällen der Lieferkette durch IT-Sicherheitsvorfälle betroffen – und sogar die Hälfte der Verantwortlichen (51 Prozent) sehen in IT-Sicherheitsproblemen wie Hackerangriffen oder Computerviren die größte Bedrohung für die eigene Supply Chain – ein Plus von zehn Prozentpunkten im Vergleich zu 2017. „Die Digitalisierung gewinnt zunehmend an Bedeutung, um Lieferketten resilienter und auch leistungsfähiger zu gestalten. Gleichzeitig sind sich Entscheider auch zunehmend bewusst, dass sie sich einer wachsenden Bedrohungslage durch Cyberkriminalität stellen müssen", erläutert Moritz Gborglah, Division Manager und Digitalisierungsexperte bei Hermes Germany die Ergebnisse.

Besonders sensible Unternehmensbereiche innerhalb der digitalen Lieferkette, die effektive Schutzmaßnahmen erfordern, sind laut Umfrage die Daten sowie der Datentransfer. Demnach sieht mehr als die Hälfte der befragten Logistikverantwortlichen (56 Prozent) ein besonders hohes Gefahrenpotenzial beim unerlaubten Zugriff auf Daten von Kundinnen sowie Mitarbeitenden. Für 41 Prozent der Befragten ist der automatisierte Datenaustausch mit Lieferanten und Partnern besonders gefährdet für mögliche Angriffe, bei größeren Unternehmen erreicht dieser Wert sogar 53 Prozent. Die Nutzung von Online-Bezahlsystemen und der Onlinehandel (je 39 Prozent) sowie die IT-gestützte Lagerhaltung (32 Prozent) bewerten hingegen nur rund ein Drittel der Teilnehmenden als besonders durch potenzielle IT-Sicherheitsvorfälle bedroht.

Mit 72 Prozent sagen darüber hinaus fast drei Viertel aller befragten Logistikentscheider, dass sie innerhalb des Unternehmens über das nötige Know-how verfügen, um die Gefährdungen ihrer IT-Systeme auf ein tragbares Maß zu beschränken. Je größer das Unternehmen, desto höher ist das Vertrauen in die eigenen Abwehrmechanismen. Drei Viertel der Unternehmen (78 Prozent) verlässt sich dabei auf interne IT-Abteilungen. Lediglich sieben Prozent der Befragten setzten auf interne Cybersecurity-Experten zur Optimierung der IT-Sicherheit. „Die Absicherung der unternehmenseigenen IT-Umgebung allein reicht innerhalb eines globalen Liefernetzwerks jedoch nicht aus", so Gborglah. „Mit zunehmender Vernetzung empfehlen wir Unternehmen, auch die Systeme ihrer Kooperationspartner im Blick zu haben. Transparenz in der Supply Chain spielt hier eine zentrale Rolle."

58 Prozent der Teilnehmenden gehen davon aus, zunehmend von Sicherheitsvorfällen kooperierender Unternehmen betroffen zu sein. Zwar geben 48 Prozent an, über umfassende Informationen bezüglich der IT-Sicherheitssysteme und -maßnahmen ihrer Zulieferbetriebe zu verfügen – 2017 waren es noch 34

Prozent. Bei größeren Organisationen mit 250 bis 1.000 Beschäftigten sagen das jedoch lediglich 33 Prozent. „Größere Organisationen sind häufig noch weitreichender vernetzt. Hier über alle Maßnahmen innerhalb des Netzwerkes informiert zu sein, ist für Unternehmen nach wie vor eine große Herausforderung“, konstatiert Gborglah.

Für 67 Prozent der Befragten hat die Absicherung des Firmennetzwerkes gegen Datenabfluss höchste Priorität. Die Verschlüsselung von Netzwerkverbindungen und E-Mails halten 57 Prozent der Teilnehmenden für besonders effektiv. Gestiegen ist die Erwartung an positive Effekte durch Information und Weiterbildung von Management und Mitarbeitenden: Erkannten darin 2017 nur 25 Prozent der Entscheiderinnen eine hohe Wirksamkeit, sind es heute 42 Prozent. Bei den größeren Unternehmen zwischen 250 und 1.000 Mitarbeiter*innen stieg der Wert sogar von 29 auf 67 Prozent.

Ein aktives Supply Chain Risk Management (SCRM), verbunden mit dem Einsatz einer Supply Chain Management Software zur Gewährleistung der Transparenz in komplexen Lieferketten spielt für die befragten Unternehmen derzeit noch eine untergeordnete Rolle. Während 42 Prozent der Verantwortlichen die Implementierung von Notfallplänen priorisieren, liegt der Wert für die Einführung eines Supply Chain Risk Managements (SCRM) bei 21 Prozent. Der Nutzung einer SCM-Software schreiben zwölf Prozent der Befragten eine höhere Relevanz für die IT-Sicherheit zu.

Diese Zahlen verwundern, ist doch der Entwurf von Notfallmaßnahmen ein wichtiger Handlungsbereich eines ganzheitlichen SCRM. Zusätzlich profitieren gerade kleinere Unternehmen von der Implementierung eines Supply Chain Risk Managements, digitalem Monitoring sowie einer softwaregestützten Zugriffsprotokollierung, wie diese zum Beispiel im Rahmen einer cloudbasierten SCM-Software möglich ist. „Verantwortliche scheinen sich des großen Potenzials bewährter Mechanismen und Technologien nicht in vollem Maße bewusst zu sein und unterschätzen infolgedessen deren Wirksamkeit im Hinblick auf die Verbesserung der IT-Sicherheit in der Supply Chain“, sagt Moritz Gborglah. Dabei könnten, so der Sicherheitsexperte, gerade solche Mechanismen und Systeme Transparenz schaffen und damit das Fundament für eine verbesserte IT- und Datensicherheit legen.

Sorge von Unternehmen vor Cyberangriffen auf Lieferketten nimmt zu