In Kürze

Vor allem kleinere Unternehmen haben bei der IT-Sicherheit Nachholbedarf. Ob das Ignorieren von Sicherheitslücken oder mangelnde Mitarbeitersensibilisierung – ein laxer Umgang mit dem Thema öffnet nicht nur Cyberkriminellen Tür und Tor, sondern kann sogar den Versicherungsschutz kosten.

Gefundenes Fressen für Hacker

Gerade kleine und mittlere Unternehmen gehen oft viel zu sorglos mit dem Thema IT-Sicherheit um. Dabei ist die Gefahr auch für Logistiker, Opfer eines Cyberangriffs zu werden, größer denn je.

Kaum ein Tag vergeht, an dem nicht neue Cyberattacken durch die Presse gehen. Die lahmgelegten Supermarktkassen bei 7Eleven in Dänemark oder der schwere Hackerangriff auf die Systeme der Industrie- und Handelskammern (IHK) sind nur zwei prominentere Beispiele des Monats August 2022. Nicht zuletzt macht das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Anbetracht des russischen Angriffskrieges gegen die Ukraine nach wie vor eine erhöhte Bedrohungslage aus. „Das Risiko von Cyberattacken auf Unternehmen ist momentan ohnehin schon hoch, im Logistikbereich ist es unserer Erfahrung nach aktuell sehr hoch“, sagt auch Pascal Eggert, Managing Director des IT-Dienstleisters q.beyond logineer. In den zurückliegenden Wochen und Monaten habe sein Unternehmen vermehrt Angriffe auf mittelständische Logistikbetriebe wahrgenommen. „Sie rücken zunehmend in den Fokus der Angreifer, da sie im Allgemeinen bei ihren Digitalisierungsbestrebungen zurückliegen – und das gilt auch für den Cyberschutz.“ Hinzu komme, dass die Angreifer um das gute Geschäft wüssten, das Logistiker zuletzt aufgrund der hohen Raten gemacht haben. „Und sie wissen auch, dass in der Zeit davor wenig Geld für den Aufbau von Cyber-Abwehr zur Verfügung stand“, so Eggert. Mittelständische Logistikbetriebe seien daher ein „gefundenes Fressen“.

Auch Unternehmen der Logistikbranche geraten immer mehr ins Visier von Cyberkriminellen

NicoElNino/stock.adobe.com

To-dos in der Informationssicherheit

- Der Kampf gegen Cyberkriminalität wird auf organisatorischer Ebene geführt. Prüfen Sie regelmäßig die internen Zuständigkeiten und Prozesse in Sachen Informationssicherheit
- Führen Sie eine Business Impact Analyse durch, vorzugsweise durch externe Experten für Krisenmanagement und mit Verständnis für Ihre Branche
- Führen Sie ein Schwachstellen-Monitoring für die Ableitung weiterer Maßnahmen durch
- Steigern Sie die Mitarbeiter-Awareness – und zwar regelmäßig. Trainings/Schulungen sollten mindestens einmal jährlich stattfinden
- Stellen Sie einen Notfallplan auf – und machen Sie ihn auch offline, etwa als Aushang, zugänglich

Größte Bedrohung für die Lieferkette

Langsam findet in der Logistik, die lange im Verdacht stand, Cyberrisiken zu unterschätzen, aber ein Umdenken statt. „Fast jeder kennt mittlerweile ein Unternehmen in der Branche, das Opfer von Cyberattacken geworden ist – wenn es nicht schon selbst angegriffen wurde“, sagt Eggert. Dass Logistikentscheider Cyberangriffe mittlerweile als besonderes Risiko erkennen, ergab auch eine Befragung unter 150 Logistikverantwortlichen in Deutschland im Rahmen des jüngsten Hermes-Barometers. Darin gaben 51 Prozent an, dass IT-Sicherheitsprobleme inzwischen die größte Bedrohung für ihre Lieferkette darstellen, zehn Prozent mehr als 2017.
Dennoch fühlen sich die Unternehmen gut gewappnet: 72 Prozent sehen sich in der Lage, Gefährdungen ihrer IT-Systeme auf ein tragbares Maß zu beschränken. Das Vertrauen in die eigenen Kompetenzen ist aber stark abhängig von der Unternehmensgröße. Während bei Großunternehmen mit über 1000 Mitarbeitern 100 Prozent glauben, in Sachen IT-Sicherheit ausreichend aufgestellt zu sein, sind es bei den kleineren mit 50 bis 250 Mitarbeitern lediglich 67 Prozent.

Gefährliche Ignoranz im Mittelstand

Dass gerade im Mittelstand noch viel Nachholbedarf besteht, suggeriert auch eine im Auftrag des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV) im April und Mai 2022 durchgeführte Umfrage zum Umgang mit der bereits im Dezember 2021 bekannt gewordenen Sicherheitslücke „Log4J“. Das BSI hatte seinerzeit die höchste Alarmstufe ausgerufen. Umso erschreckender, dass laut GDV-Umfrage nur 40 Prozent der mittelständischen Unternehmen nach dem Bekanntwerden von „Log4J“ ihre Software überprüft haben. Nur 28 Prozent gaben an, zusätzlich die eigenen Systeme auf bereits eingedrungene Schadsoftware untersucht zu haben.
Jedes zweite Unternehmen hat also trotz der extrem hohen Bedrohungslage weder Software noch IT-System geprüft. „Wer darauf nicht reagiert, ist beim Thema IT-Sicherheit zu sorglos – oder hat zu wenig Know-how“, sagt GDV-Hauptgeschäftsführer Jörg Asmussen. Im Zweifel könnten Unternehmen auch ihren Cyberversicherungsschutz verlieren, wenn Hacker über eine lange bekannte, aber dennoch nicht geschlossene IT-Sicherheitslücke angreifen. „Nichts für die Informationssicherheit zu tun, weil man ja eine Versicherung hat – das funktioniert nicht mehr“, konstatiert auch Robert Drexler, Leiter Schunck Competence Center Cyber. Es müsse für den Versicherer erkennbar sein, dass ein Unternehmen das Thema verstanden und sich intensiv damit befasst hat. „Versicherer schauen mittlerweile genau hin, bei großen Unternehmen wird der Versicherungsschutz sogar in Einzelfällen an die Umsetzung bestimmter Maßnahmen gekoppelt“, sagt Drexler.

Regelmäßige Mitarbeitertrainings

Die Basics der Informationssicherheit sollte laut Drexler daher wirklich jedes Unternehmen beherzigen (siehe auch To-do-Liste). Der größte Risikofaktor sind bekanntlich die eigenen Mitarbeitenden. „Eine essenzielle Maßnahme ist daher die Sensibilisierung der Belegschaft für Cybergefahren“, mahnt Drexler. Ob E-Learnings, Trainings oder auch fingierte Phishing-Kampagnen, um herauszufinden, wie viele der Mitarbeitenden potenziell darauf reinfallen würden – Ansätze gebe es viele. Aber: „Alle Maßnahmen müssen regelmäßig wiederholt und an die aktuelle Gefahrenlage angepasst werden – mindestens einmal im Jahr“, sagt Drexler. Must-Have seien ferner die Multi-Faktor-Authentifizierung und natürlich Back-ups. Letztere sollten allerdings nicht nur grundsätzlich gemacht werden, sondern dann auch so durchgeführt werden, dass sie im Krisenfall auch wiederherstellbar sind, betont der Experte. *mh*

VR plus

Online

Playlist Cybersecurity

Ob ein interaktiver Managementkurs zum Schutz vor Phishing oder eine Checkliste zur Auswahl der richtigen Cyberversicherung – hilfreiche Arbeitstools sowie Hintergrundbeiträge rund um die Themen Cyberkriminalität und Cybersicherheit finden Abonnenten auf VR plus. *mh*

www.verkehrsrundschau.de/plus/cybersecurity