trans aktuell

DIE ZEITUNG FÜR TRANSPORT, VERKEHR UND MANAGEMENT

SONDERDRUCK AUS NR. 8/2018 www.transaktuell.de

Stillstand und Erpressungen

Millionenschäden durch Cyberkriminalität – Angriffe mit falschen Identitäten – wie sich Speditionen schützen können

Wie können sich Transport- und Logistikunternehmen gegen Cybercrime schützen? Zu diesem Thema richtete der Verband Spedition und Logistik Baden-Württemberg (VSL) kürzlich eine Veranstaltung im Stuttgarter Haus der Wirtschaft aus. Als Experte sprach Sascha Michel Kessel, Leiter des Competence Center Cyber beim Versicherungsmakler Oskar Schunck.

„Die Kosten für die Wiederherstellung der Reputation sind kaum messbar“

SASCHA MICHEL KESSEL, LEITER COMPETENCE CENTER CYBER BEI OSKAR SCHUNCK

Die Bedrohung durch Cyberangriffe nimmt seit Jahren zu. Am häufigsten betroffen sind Unternehmen aus Handel, IT und Medien. An vierter Stelle folgt bereits die Transport- und Logistikbranche. Betroffen waren voriges Jahr etwa Raben Logistics und Maersk. Motivation und Personen hinter den Attacken sind höchst unterschiedlich. So gibt es manchmal auch persönliche Verbindungen zum Ziel, etwa durch Wettbewerber oder ehemalige Mitarbeiter. Die Angreifer müssen nicht unbedingt eigene IT-Kenntnisse besitzen. Vielmehr kann dieser Personenkreis inzwischen über verschiedene Plattformen die Cyberattacken in Auftrag geben – und das zu teilweise günstigen Prämien.

Die Möglichkeiten sind vielfältig und reichen von virenbehafteten Mails, Überspielen von Schadsoftware bis hin zum Abziehen sensibler Daten über imitierte Internetseiten (Phishing). Im Kommen ist verstärkt „Social Engineering“. Bei dieser Masche behaupten Hacker unter Vorspiegelung falscher Identitäten, beispielsweise kompromittierendes Material über Mitarbeiter zu besitzen. Das „Beweismaterial“ wird gleich frei Haus mitgeliefert, etwa in Form eines Videolinks, hinter dem sich Schadsoftware verbirgt. An der Tagesordnung sind zudem Erpressungen. Nur gegen Geld sollen Daten wieder zurückgegeben oder Verschlüsselungen an der IT-Infrastruktur behoben werden. Eine Reihe von Transportunternehmen hat bereits Lehrgeld zahlen müssen, denn ein weiterer Tag Stillstand wäre noch teurer gewesen.

Wenn wegen der Hackerangriffe etwa vertraglich vereinbarte Termine platzen, so addieren sich zu den Kosten dafür noch der Aufwand für Datenverlust, Betriebsunterbrechung bis hin zu Vertragsstrafen an die Kunden. Hinzu kommt noch der Reputationsschaden wegen „mangelnder Vertragstreue.“ Laut Kessel geht der durchschnittliche Gesamtschaden pro Hackerangriff in die Millionen, wobei die Kosten für Krisenstab und Juristen bis zu 50 Prozent ausmachen können.

Um sich gegen Cyberattacken zu schützen, können Unternehmen jedoch einiges tun. Dazu gehören beispielsweise Schulungen für die Mitarbeiter, ein Krisenplan oder Datenschutzvereinbarungen. Als organisatorische Maßnahmen bieten sich regelmäßige Sicherheitsaudits durch Spezialisten an. In technischer Hinsicht haben sich die Absicherung des Firmennetzwerks durch Datenverschlüsselung bewährt, ebenso Backups, Sicherheitszertifizierungen, Zugangsbeschränkungen und Passwortschutz.

Auch sogenannte Cyberversicherungen, die zahlreiche etablierte Versicherungsunternehmen anbieten, können zumindest die finanziellen Schäden abfedern. Vor Vertragsabschluss sind jedoch zahlreiche Fragen zu beantworten, etwa zum Stand der Technik oder generell zum IT-Sicherheitsmanagement. Achtung: Vor Vertragsabschluss sind die Ausschlüsse von Leistungen gut zu prüfen.

Zu erwähnen ist beim Thema Cybercrime auch die EU-Datenschutz-Grundverordnung (EU-DSGVO), die am 25. Mai in Kraft tritt und wegen der zahlreichen personenbezogenen Daten auch die Transport- und Logistikbranche betrifft (siehe auch trans aktuell 2/3 2018). Bei Verstößen können teils empfindliche Bußgelder fällig sein. So stehen etwa bis zu 20 Millionen Euro Strafe oder vier Prozent des weltweit erzielten Gesamtumsatzes im Raum – je nachdem welcher Betrag höher ist. Zudem liegt die Nachweispflicht über die Einhaltung der Datenschutz-Grundsätze beim Unternehmen.

Überhaupt bringt die EU-DSGVO eine intensivierte Managementverantwortung mit sich. Bei Pflichtverletzungen beim Datenschutz haftet das Leitungsorgan verschuldensunabhängig persönlich und unter Umständen mit dem Privatvermögen.

Text: Ralf Lanzinger | Fotos: Fotolia/James Thew, Schunck

TIPPS FÜR PRÄVENTION GEGEN CYBERATTACKEN

- Die wichtigsten und systemrelevanten Daten – ohne die der Betrieb stillsteht – identifizieren und den Schutz dieser Daten hinterfragen.
- Fragen stellen: Welche Einfallstore kann es geben? Etwa Schnittstellen mit anderen Unternehmen? Ist das gefährdete Unternehmen selbst ein Provider und bietet es IT-basierte Logistikdienstleistungen an? Kann einer dieser Kunden das Unternehmen lahmlegen? Wie kann sich das Unternehmen absichern? Welche Nachweise kann es anfordern?
- Könnte das eigene Unternehmen für andere Betriebe eine Gefahr darstellen? Könnten diese eine Zertifizierung oder den Nachweis einer Cyberversicherung anfordern?
- Den Ernstfall durchspielen: Hat das Unternehmen eine Strategie im Fall einer Cyberpanne oder -attacke – und wie gut ist sie?
- Wer unterstützt das Unternehmen im Ernstfall? Gibt es einen Cybersecurity-Spezialisten und stehen die richtigen Fachanwälte zur Verfügung?

Impressum: Sonderdruck des ETM Verlags aus trans aktuell 8/2018. Verantwortlich: Karin Schilling, Telefon (07 11) 7 84 98-45 · www.etm.de