Pressekontakt:
Maike Wiehmeier
+49 89 939 49 464
maike.wiehmeier@oliverwyman.com

P R E S S E I N F O R M A T I O N

Oliver Wyman-Analyse zu Cybersicherheit in der Transport- und Logistikbranche

Digitaler Datenklau bedroht internationale Transportketten

Transport- und Logistikanbieter stehen im Fadenkreuz von hochspezialisierten Hackern. Doch Unternehmen mit überzeugendem Risikomanagement können von der Cybergefahr profitieren.

München, 27. Juni 2017 – **Die Transport- und Logistikbranche gerät immer stärker ins Visier von Cyberkriminellen. Mit der zunehmenden Digitalisierung der Prozesse bei Verladern, Spediteuren, Transportunternehmen und Infrastrukturbetreibern wachsen die Gefahren von Datenmissbrauch und -klau. Der weltweiten Logistikbranche drohen bereits 2020 rund sechs Milliarden Euro an Schäden durch Cyberkriminalität, warnt eine Analyse der Strategieberatung Oliver Wyman. Allein in Deutschland könnte sich der Schaden auf 450 Millionen Euro belaufen. Die Berater zeigen auf, dass es bei der Abwehr von Cyberrisiken auf eine Kombination von Technologie und Mitarbeitern ankommt. Logistiker, die Cybersicherheit zu einem Teil ihres Angebotsportfolios machen, können sich vom Wettbewerb abheben und das Risiko zu einer Chance machen.**

Die eingespielten Systeme des internationalen Güterverkehrs sind von Cyberkriminalität vielfältig bedroht. Mit ihren vielen Schnittstellen zwischen zahlreichen beteiligten Unternehmen bieten die Transportketten in großem Umfang Angriffspunkte für illegale Zugriffe. Dies umfasst das Hacken von Kunden- und Mitarbeiterdaten, die Überwindung von Sicherheits- und Kontrolleinrichtungen von Lägern, Eingriffe ins Hafenmanagement oder das „Entführen“ von Lieferdrohnen.

Auch wenn die Branchenführer der Logistik damit begonnen haben, sich auf Cyber-Bedrohungsszenarien einzustellen: Lücken in Sicherheitssystemen verursachen wachsende Schäden in der Logistikbranche. Die Oliver Wyman-Experten rechnen für 2017 mit rund drei Milliarden Euro an Schäden durch Cyberkriminelle. 2020 könnten es bereits rund sechs Milliarden Euro sein. Dies umfasst lediglich die direkten Kosten von Hacking-Angriffen und Datenlecks. Indirekte, langfristige Kosten, wie Reputationsschäden oder Verluste geistigen Eigentums sind dabei noch nicht berücksichtigt. „Unabhängig von der Branche liegen die durchschnittlichen Kosten eines Datenlecks bei einem großen Unternehmen schnell bei mehr als einer Million Euro“, berichtet Claus Herbolzheimer, Partner bei Oliver Wyman und Experte für Cyberrisiken.

Spezialisierte Angriffe, einfach verfügbare Hackingtools
Bereits heute manipulieren hochspezialisierte Hacker Transportketten gezielt für ihre Zwecke – etwa im Zusammenspiel mit Schmugglern: Hacker dringen in Hafen- und Zollsysteme ein, um in Erfahrung zu bringen, ob ein Container, der illegale Ware enthält, vom Zoll als unverdächtig eingestuft wurde. Ein Extremfall ist der Eingriff in die GPS-Navigationssysteme von Schiffen, welche Piraten nutzen, um ihre Angriffe zu planen und abzusichern. „Gezielte Attacken sind eine deutlich größere Gefahr für Transport- und Logistikanbieter als etwa die auf Erpressungssoftware basierende Wannacry-Attacke im Mai diesen Jahres“, sagt Max-Alexander Borreck, Principal bei Oliver Wyman.

Doch nicht nur durch spezialisierte Hacker droht Gefahr. Die Analyse von Oliver Wyman liefert Beispiele, dass im Darknet, einem nicht für alle Nutzer zugänglichen Bereich des Internets, gezielt Daten und Services angeboten werden, die Logistikern schaden können. So fanden die Berater etwa Angebote für Kunden- und Mitarbeiterdaten von Logistikern, Hacking-Software für „Internet of Things“-

Anwendungen wie Drohnen sowie gehackte, anonyme Zugänge zu Paketstationen. Gezahlt wird anonym mit der Internet-Währung Bitcoin. „Die missbräuchliche Nutzung von Daten setzt heute kaum noch tiefer gehende Programmierkenntnisse voraus, denn vieles lässt sich im Darknet bereits als Dienstleistung oder Softwarepaket erwerben“, beschreibt Borreck die Gefahr durch die Verfügbarkeit illegaler Angebote im Darknet.

Firewalls sind nicht genug

Viele Unternehmen konzentrieren ihre Cyberabwehr auf immer höhere Firewalls, um Sicherheitslücken zu schließen. Nach Ansicht der Oliver Wyman-Experten ist das nicht genug. „Das technische Schutzdenken, also die Frage, wie ein Angriff mit technologischen Mitteln vermieden werden kann, ist nur ein Teilaspekt“, meint Herbolzheimer. „Viele Angriffe funktionieren nicht ausschließlich über externe Attacken aus dem Internet. Da werden Mitarbeiter bestochen oder ihre Unwissenheit wird ausgenutzt, um Zugang zu internen Netzwerken zu bekommen.“ Zusätzlich zu technischen Schutzmechanismen komme es daher darauf an, die richtigen Trainings anzubieten, ein entsprechendes Sicherheitsbewusstsein in der Organisation zu schaffen und möglichst widerstandsfähige Prozesse sowie Notfallpläne zu gestalten. „Modernes Risikomanagement gegen Cyberverbrechen muss sich vor allem mit branchenrelevanten Drohszenarien beschäftigen. Diese sind in der Regel recht unterschiedlich, zum Beispiel in der Finanzwelt anders als im Transportgeschäft“, sagt Herbolzheimer. Man müsse zunächst Angriffstypen und potenzielle Angreifer verstehen lernen; das könne die Eintrittswahrscheinlichkeit eines Risikos ebenso wie seine Auswirkungen mindern.

„Der Logistiker ist seit jeher für den zuverlässigen und sicheren Transport der Fracht verantwortlich. Heute muss er zusätzlich die Daten seiner Kunden nachhaltig schützen. Unternehmen, denen es gelingt die Sicherheit von physischer Transportkette und Datenfluss zu gewährleisten, haben zunehmend einen Vorteil im Wettbewerb“, sagt Borreck. Zu den Erfolgsfaktoren zählen die Experten etwa die Berücksichtigung von Cybersicherheit in einem umfassenden Risikomanagement, die Verzahnung der Cyberabwehr von Kunde und Logistiker, einen teilweisen Transfer von Risiko durch Versicherungen und die Installation entsprechender Abwehrtechnologien.

Video zum Darknet-Risiko: http://www.oliverwyman.com/pages/email/cyber-security-threats-in-the-transport-logistics-industry.html#video

Medienkontakt

Maike Wiehmeier
Communications Manager DACH
Oliver Wyman
Tel. +49 89 939 49 464
maike.wiehmeier@oliverwyman.com

ÜBER OLIVER WYMAN

Oliver Wyman ist eine international führende Strategieberatung mit weltweit über 4.500 Mitarbeitern in mehr als 50 Büros in rund 30 Ländern. Wir verbinden ausgeprägte Branchenexpertise mit hoher Methodenkompetenz bei Digitalisierung, Strategieentwicklung, Risikomanagement, Operations und Transformation. Wir schaffen einen Mehrwert für den Kunden, der seine Investitionen um ein Vielfaches übertrifft. Wir sind eine hundertprozentige Tochter von Marsh & McLennan Companies (NYSE: MMC). Unsere Finanzstärke ist die Basis für Stabilität, Wachstum und Innovationskraft. Weitere Informationen finden Sie unter www.oliverwyman.de. Folgen Sie Oliver Wyman auf Twitter @OliverWyman.