IT muss widerstandsfähig sein

Hackerangriffe auf Logistikdienstleister nehmen zu. Technischer Schutz und Mitarbeitersensibilisierung sind wichtige Maßnahmen dagegen.

Von Bianca Heitmann und Stefan Peter

Kleine und mittlere Logistiker sind gefordert, ihre Prozesse zu digitalisieren. Verpassen sie diese Chance, verlieren sie über kurz oder lang den Anschluss an ihre Zielmärkte – und damit ihre Geschäftsgrundlage. Zugleich greifen Cyberkriminelle vermehrt Logistikunternehmen an. Wer massiven Attacken nicht schutzlos ausgeliefert sein will, sollte die IT ganzheitlich betrachten: Auf der einen Seite stehen Cybersecurity-Strategien, auf der anderen Seite geschulte Mitarbeitende. Mit beiden Faktoren im Blick grenzen Logistiker die realen Gefahren ein.

Die Schnittstellen zwischen den verschiedenen Parteien, zum Beispiel Carriern und Spediteuren, bieten vielerlei Angriffspunkte: vom Überwinden einzelner Kontrolleinrichtungen über Eingriffe in die IT-Infrastruktur bis hin zum Diebstahl von Adress- und Auftragsdaten. Lösungen für die Cyberabwehr wie Firewalls, die sich rein auf die Technik als Angriffsfeld fokussieren, sind allein nicht zielführend. Mit nur einem Klick auf einen E-Mail-Anhang können Mitarbeitende Ransomware die Unternehmenstür öffnen.

Neben Schäden an der IT-Infrastruktur oder Wiederherstellungskosten haben entsprechende Vorfälle durchaus auch Strafzahlungen zur Folge. Ein Verstoß gegen die DSGVO kostet Unternehmen mitunter zweistellige Millionenbeträge sowie Reputation und Erträge.

Verschiedene Sicherheitsansätze

Auf technischer Seite sollten IT-Verantwortliche überprüfen, ob Soft- und Hardware den aktuellen Anforderungen entsprechen. Hier helfen moderne IT-Sicherheitslösungen: Das Vulnerability Management dient der systematischen Schwachstellenanalyse und EDR (Endpoint Detection and Response) dem Schutz aller Endgeräte. Mit SIEM (Security Information and Event Management) erkennen Unternehmen schnell akute Bedrohungen und wehren sich effektiv dagegen – obendrein erfüllen sie damit ihre Compliance-Verpflichtungen.

Vor allem wenn ein Unternehmen einem Ransomware-Angriff ausgesetzt ist, rücken technische Lösungen in den Mittelpunkt. In diesem Fall sollte die IT-Abteilung insbesondere Zugänge zu Cloud- oder VPN-Anwendungen sichern. Auch eine Datenspeicherung auf entfernten Servern ist möglich. Durch die sogenannten Offsite-Backups weichen Logistiker den direkten Angriffen geschickt aus.

Auf der anderen Seite gilt es, die Mitarbeitenden hinsichtlich der Bedrohungen zu sensibilisieren. Ohne ihre Awareness für die realen Gefahren kann IT-Security nicht gelingen. Denn Hacker professionalisieren sich immer mehr. Attacken auf Transportketten, Informationsbeschaffung durch das Eindringen in Zollsysteme oder das Ermitteln von GPS-Koordinaten von Güterschiffen haben sie inzwischen perfektioniert. Deshalb ist ein erster Schritt, den Mitarbeitenden mögliche und besonders wahrscheinliche Szenarien aufzuzeigen. Dazu tragen auch Live-Hacking-Vorführungen und Trainings zum Thema Cybersecurity im Berufsalltag bei.

Notfall- und Kommunikationspläne

Wann ein Cyberkrimineller an die Tür klopft, ist kaum abzuschätzen. Deshalb müssen vorab alle Beteiligten über einzelne Schritte informiert sein. Notfall- und Kommunikationspläne helfen Logistikunternehmen, Angriffssituationen zu definieren und die Reaktion darauf sauber zu strukturieren. Zusammen bilden sie ein effizientes Frühwarnsystem. Wichtig: Diese Pläne sollten stets branchenrelevante Szenarien abbilden.

Für eine vollständige Planung können sich die Fachverantwortlichen maßgebende Informationen aus unterschiedlichen Quellen beschaffen – unter anderem aus der DSGVO. Beispielsweise besteht bei einem Ransomware-Angriff, bei dem personenbezogene Daten geraubt wurden, eine gesetzliche Meldepflicht.

Artikel 33 der DSGVO verlangt, dass Verantwortliche innerhalb von 72 Stunden die Verletzung des Schutzes personenbezogener Daten bei der Aufsichtsbehörde melden. Zusätzlich sollten Notfallpläne relevante Fragestellungen beantworten: Soll das Unternehmen die Polizei einschalten oder benötigt es weitere Kompetenzen, um die Angriffe einzudämmen? Logistiker können sich dafür auch an die Zentrale Ansprechstelle Cybercrime (ZAC) wenden.

Ganzheitliche Sicherheit

Logistiker müssen im Zuge der digitalen Transformation schnell praxisnahe Lösungen finden, um sich gegen aktuelle Cyber-Bedrohungen zu schützen. Es genügt dabei nicht, nur einzelne IT-Komponenten durch neuere Anwendungen zu ersetzen. Vielmehr kommt es auf ein ganzheitliches Sicherheitskonzept an – sowohl bei der Planung als auch bei der Umsetzung modernster Cybersecurity-Lösungen. Fehlt das dafür erforderliche Know-how, können externe Ressourcen Hilfe leisten.

Weltweit aufgestellte Logistikunternehmen sollten auch ihre internationalen Standorte vor Cyberangriffen schützen. Dadurch erlangen Logistiker sogar einen Wettbewerbsvorteil: Wer in der von Angriffen bedrohten Branche die Sicherheit aktiv kommuniziert, weckt gegenüber Kunden und Lieferanten Vertrauen. ***(rok)***

FOTO: LUIS ALVAREZ

In einer IT-Systemarchitektur müssen alle Geräte und Schnittstellen eines Netzwerks gesichert werden.

> Zum Schutz vor Cyber-Bedrohungen genügt es nicht, nur einzelne IT-Komponenten durch neuere Anwendungen zu ersetzen.

Bianca Heitmann ist Solutions Managerin bei der q.beyond logineer GmbH; **Stefan Peter** ist verantwortlich für Cyber Security Services bei der q.beyond AG