Cyberresilienz von Bahnunternehmen stärken

Artikel vom **21. Juni 2022**
Betriebs- und Verkehrsmanagement

Bei SOC-as-a-Service unterstützen externe Experten Unternehmen dabei, sich gegen Cyberangriffe zu schützen (Bild: AdobeStock/telent).

Cyberangriffe sind für den Personen- und Güterverkehr ein brisantes Thema, denn im schlimmsten Fall steht die Sicherheit von Passagieren und Mitarbeitenden auf dem Spiel. Auch der wirtschaftliche Schaden ist beträchtlich, wenn Züge stundenlang stillstehen, wie Ende März bei einem Hackerangriff auf die Ticketsoftware eines italienischen Eisenbahnunternehmens. Das in Deutschland kürzlich in Kraft getretene IT-Sicherheitsgesetz 2.0 (IT-SIG) verschärft die Anforderungen an Betreiber kritischer Infrastrukturen (KRITIS). Konkret heißt das, Bahnunternehmen müssen mehr tun, um ihre Cyberresilienz zu stärken. Um sich im Sinne des IT-SIG 2.0 zu schützen, benötigen KRITIS-Betreiber im ersten Schritt eine umfassende Inventarisierung ihrer vorhandenen Systeme und Prozesse unter securityrelevanten Gesichtspunkten. Im Rahmen einer solchen ganzheitlichen Betrachtung können Experten wie das Cybersecurity-Team der telent GmbH potenzielle Lücken erkennen und darauf aufbauend eine zielgerichtete Strategie erarbeiten, die das Risiko eines Cyberangriffs minimiert.

Vorgaben ab Mai 2023

Zu den technischen Schutzmaßnahmen, die KRITIS-Betreiber vom 1. Mai 2023 an erfüllen müssen, gehört z. B. eine Angriffserkennung auf dem aktuellen Stand der Technik und ein Monitoring der kritischen Komponenten. Das setzt eine Next-Generation Firewall voraus mit einer integrierten Deep-Packet-Inspection (DPI), die übertragenen Daten in den Netzwerkpaketen detailliert inspiziert. Ein DPI ist wiederum die Voraussetzung für ein kombiniertes System aus Intrusion Detection System (IDS) und Intrusion Prevention System (IPS) – einer mögliche Angriffserkennung, die den gesetzlichen Vorgaben entspricht. Zur Erhöhung der IT-Sicherheit trägt auch der Aufbau eines Information Security Management System (ISMS) bei. Network Access Control, Endpoint Security, Remote Access und eine IT-Notfallplanung sind weitere Sicherheitsmaßnahmen, um nur einige Beispiele zu nennen. Um sämtliche Anforderungen zu erfüllen, die aus dem IT-SIG 2.0 resultieren, fehlt es Unternehmen häufig an ausreichendem Personal und Expertenwissen. Externe Unterstützung bietet ihnen telent mit einem eigenen Security Operation Center (SOC), das Netzwerke von Unternehmen überwacht und aktiv nach Bedrohungen sucht. Ein SOC übernimmt dabei die Funktion einer »Kommandozentrale«, in der alle relevanten Informationen zusammenlaufen, um IT-Sicherheitsvorfälle schnell zu erkennen und effektiv darauf zu reagieren. Zu den Aufgaben des Expertenteams gehören u. a. das Sicherheitsmonitoring, Alarmierungen sowie Informations- und Analysedienste. Hochspezialisierte Sicherheitsanalysten erkennen Bedrohungen nicht nur, sondern setzen ihr Know-how auch ein, um den Vorfall zu bewerten und im Falle eines Alarms die geeigneten Gegenmaßnahmen einzuleiten. telent verfügt über eine jahrzehntelange Erfahrung im Transportsektor. Dadurch kennt der Anbieter maßgeschneiderte Technologielösungen und Services für den KRITIS-Bereich die Anforderungen von Bahnunternehmen bis ins Detail und setzt sie professionell um.

Hersteller aus dieser Kategorie
