Cyber-Resilienz für vernetzte Schienenwege

Artikel vom **11. Mai 2026**
Betriebs- und Verkehrsmanagement

Die fortschreitende Digitalisierung im ÖPNV lässt IT- und OT-Systeme zusammenwachsen. Damit steigen die Anforderungen an die Sicherheit der Betriebsnetze. Ein strukturierter Umgang mit Risiken hilft, Verfügbarkeit und Schutz der Infrastruktur zu gewährleisten.

Um Cyberrisiken frühzeitig zu erkennen und den sicheren Betrieb zu gewährleisten, ist ein kontinuierliches Monitoring vernetzter Betriebsnetze im ÖPNV erforderlich (Bild: telent).

Die Digitalisierung im ÖPNV beschleunigt die Verschmelzung der Bereiche IT und OT. Während früher abgeschottete Systeme dominierten, finden sich heute vernetzte Strukturen. Moderne Betriebsnetze bilden das Rückgrat für die Steuerung von Fahrgastinformationssystemen, und digitale Netze für die Betriebsfunkkommunikation stellen eine unterbrechungsfreie Koordination sicher. Diese Konvergenz steigert die

Effizienz, schafft jedoch auch neue Einfallstore für Cyberrisiken, die über den klassischen Perimeterschutz hinausgehen.

Transparenz als Sicherheitsanker

In gewachsenen Infrastrukturen fehlt häufig der detaillierte Überblick über alle aktiven Assets. Sicherheit beginnt jedoch mit Sichtbarkeit. Nur wer genau weiß, welche Komponenten in den Betriebsnetzen kommunizieren – von der Leitstelle bis zum Sensor am Gleis –, kann Gefahren bewerten. Ein kontinuierliches Monitoring ist erforderlich, um Risiken für den Bahnbetrieb zu minimieren, ohne die Verfügbarkeit der Anlagen zu beeinträchtigen.

Gezieltes Risikomanagement statt Gießkannenprinzip

Ein effizientes Schwachstellenmanagement im ÖPNV darf den Betrieb nicht stören. In sensiblen OT-Umgebungen sind aktive Scans oft mit Risiken verbunden. Stattdessen ist ein kontextbasierter Ansatz erforderlich, der die Kritikalität einzelner Systeme für die Fahrgastsicherheit berücksichtigt. CTEM (Continuous Threat Exposure Management) bietet hierfür einen methodischen Rahmen, indem es Informationen aus Funknetzen sowie Leit- und Informationssystemen zusammenführt und reale Angriffspfade identifiziert.

Ganzheitliche Resilienz

Für Verkehrsbetriebe bedeutet dieser Ansatz eine bessere Planbarkeit. Schutzmaßnahmen werden gezielt dort gebündelt, wo sie wirksam sind, anstatt auf einzelne Alarme isoliert zu reagieren. So bleiben Netze für Kommunikation und Fahrgastinformation auch bei steigender Bedrohungslage stabil, und regulatorische Anforderungen wie NIS 2 lassen sich in den Betriebsalltag integrieren.

Hersteller aus dieser Kategorie
