TAGESSPIEGEL
BACKGROUND

Verkehr & Smart Mobility

Digitaler Schienenverkehr? Aber sicher!

Markus Fritz, Präsidiumsmitglied für Cybersecurity beim Verband der Bahnindustrie FOTO: PROMO

Die Digitalisierung des Bahnverkehrs ist wichtig für den Klimaschutz, denn so wird die Schiene leistungsfähiger. Die Cybersicherheit darf dabei aber nicht vergessen werden. Die Bahnindustrie hat passende Produkte, doch auch die Politik ist gefordert.

von **Markus Fritz**

veröffentlicht am 26.01.2023

Klimaschutz duldet keinen Aufschub mehr: Deutschland soll **bis 2045 klimaneutral** werden. Dafür müssen die Verkehrsemissionen bei stetig steigendem Mobilitätsbedarf um mindestens 50 Prozent sinken. Eine möglichst baldige **Verkehrswende, hin zur Schiene**, ist essenziell für die Erreichung dieser Ziele. Hierbei spielt die zeitnahe **Digitalisierung des Schienenverkehrs** in Deutschland eine kritische Rolle, denn sie ermöglicht mehr klimafreundlichen Bahnverkehr, mehr Energieeffizienz, mehr Pünktlichkeit sowie kürzere Fahr- und Wartezeiten.

Smarte Technologien machen Züge **attraktiver für Reisende** und effizienter für den Güterverkehr. Aber die fortschreitende digitale Vernetzung der Mobilität schafft auch **neue Angriffsflächen für Cyberangriffe** und Datenmissbrauch. Für den Schienenverkehr von morgen ist es deshalb essenziell, bereits heute technologische Lösungen sowie politische Rahmenbedingungen für bestmögliche und stetig entwicklungsfähig bleibende **Cybersicherheitsanwendungen** zu schaffen.

Unsere Schienenverkehrssysteme sind für unser Land nicht nur Verkehrsadern, sondern gleichzeitig **kritische Infrastrukturen**. Ausfälle und Störungen, generell die Nichtverfügbarkeit dieses Systems kann zu dramatischen **Versorgungsengpässen** oder sogar zu einer Bedrohung der öffentlichen Sicherheit führen.

Was wie die Handlung eines Hollywood-Thrillers klingt, ist **reale Gefahr**: Unbefugte schleusen **Malware** in Überwachungskamerasysteme von U-Bahnwagen, gehackte Sensoren in Zügen schneiden heimlich sensible Gespräche mit. Fremde Geheimdienste nutzen Netzdaten zur **Industrie- und Wirtschaftsspionage**, legen Teile des Schienenwegenetzes lahm oder übernehmen gar dessen Fernsteuerung für Sabotageakte. Damit all dies Fiktion bleibt, ist Cybersecurity essenziell für eine moderne, vernetzte und digitale Schiene.

Die deutsche Bahnindustrie beherrscht die notwendigen Technologien und liefert Lösungen, die sie kontinuierlich weiterentwickelt. Dies geschieht in einem dreistufigen Ansatz: **Prävention**, **Erkennung** und **Reaktion**.

1. **Prävention**: Während beim Ansatz „**Security-by-Design**“ Sicherheitsaspekte bereits im Zentrum des Entwicklungsprozesses eines Produkts stehen, konzentriert sich „**Security-by-Default**“ auf eingebettete Sicherheitssettings. Das bedeutet, dass die Standardeinstellungen eines Produkts die sichersten Einstellungen sind, welche aktuell möglich sind. Effektive Prävention setzt nicht nur auf technische Lösungen und hohe Sicherheitsvorschriften, sondern auch auf eine klare Definition von

Prozessen und Verantwortlichkeiten sowie auf eine **breite Sensibilisierung** von Mitarbeitern und Kunden.

2. **Erkennung**: Effektive Erkennungssysteme können Bedrohungen identifizieren und isolieren, bevor diese sich ausbreiten. Hierbei ist entscheidend, dass Systeme leicht zu reparieren und vor allem auch **Upgrade-fähig** sind.

3. **Reaktion**: Eine adäquate Reaktion wird sichergestellt, indem detektierte Sicherheitslücken sofort geschlossen und gegebenenfalls Updates zur Verfügung gestellt werden.

Auch datenschutzrechtlich muss die digitale Schiene integer sein. Der **Schutz von Persönlichkeitsrechten** bildet die Basis des Vertrauens in die Schiene der Zukunft. Fahrgäste haben ein Anrecht auf sichere Mobilität und unbeschwertes Nutzen digitaler Dienstleistungen.

CCTV-, Sensorüberwachung und Apps sammeln **immer größere Datenmengen**. So kann auch die Wahrscheinlichkeit eines missbräuchlichen Umgangs steigen. In der EU werden die Daten anonymisiert und binnen gesetzlich vorgegebener Fristen gelöscht. Doch könnten Unbefugte auf Videomaterial zugreifen? Könnten somit Lücken entstehen im Schutz von Persönlichkeitsrechten der Reisenden? Auch diese bürgerrechtlich sensiblen Fragen gehören auf den Tisch.

Denn obgleich Cybersicherheit eine technische und prozessuale Herausforderung ist, muss sie zwingend auch als **politische Priorität** behandelt werden. Cybersicherheit für den strategischen Eisenbahnsektor ist eine wichtige **Grundlage für die wirtschaftliche und politische Souveränität** Europas. Durch welche Faktoren also lässt sich Cybersecurity im deutschen und europäischen Schienennetz stärken?

1. **Digitalisierung als langfristiges Lebenszyklusmodell denken**: Die Digitalisierung der Schiene ist eine Jahrhundertaufgabe. Entsprechend weitsichtig muss dieses Projekt gedacht, geplant und finanziert werden. Bahnsysteme sind Jahrzehnte in Betrieb. Moderne

Schieneninfrastruktur und Fahrzeuge müssen so designed und ausgerüstet werden, dass sie trotz langer Lebenszyklen flexibel **an Technologiesprünge und Cyber-Innovationszyklen angepasst** werden können. Grundvoraussetzung dafür ist, dass sich der klassische Investitionsbegriff – „Einmalinvestition" inklusive Wartung und Instandhaltung bis zur Ersatz- oder Neuinvestition – in Richtung einer ganzheitlichen, über den gesamten Lebenszyklus erstreckenden Aufgabe weiterentwickelt. Kurz: Digitalisierung, Aus- und Umrüstung sowie die damit verbundene Cybersicherheit sollten nicht als abgeschlossene Einzelpakete, sondern vielmehr als **fortlaufende Lösungen und Dienstleistung** der Bahnindustrie verstanden werden.

2. **Berücksichtigung der Cybersicherheit bei der Vergabe öffentlicher Aufträge:** Cybersicherheit muss im öffentlichen Beschaffungswesen eine konsequent höhere Gewichtung haben. Europäische Wertschöpfung sollte bei Ausschreibungen im Zusammenhang mit kritischer Infrastruktur eine entscheidende Rolle spielen. In Europa sollten alle Bieter nachweislich dieselben Datenschutzstandards gewährleisten.

3. **Ausarbeitung einer Cybersicherheitsstrategie Schiene**: Last but not least sollte die EU eine integrative Expertenkommission aus Politik, Betreibern und Bahnindustrie einberufen, um eine **kohärente Cybersicherheitsstrategie** für die intelligente Schienenmobilität der Zukunft zu entwickeln. Forschung und Ausbildung junger Fachkräfte müssen gefördert und die einschlägigen europäischen Industrien einbezogen werden, um Entwicklungs-, Produktions- und Betriebsprozesse noch widerstandsfähiger zu machen.

Mobilität der Zukunft erfordert beides – Daten intelligent zu nutzen und sie adäquat zu schützen.