CYBERSICHERHEIT

Whitepaper für Cybersicherheit

EINLEITUNG

Die Digitalisierung bringt erhebliche Vorteile für die betriebliche Effizienz im Verkehr (Verfügbarkeit, Kapazität, Pünktlichkeit und Wartungsfähigkeit) sowie eine bessere Erfahrung und mehr Komfort für die Fahrgäste mit sich. Doch zwangsläufig macht sie uns auch anfälliger gegenüber Cyberattacken. Durch diese Tendenz sind Verkehrsunternehmen und Öffentlichkeit beispiellos hohen Risiken hinsichtlich der Cybersicherheit ausgesetzt.

Diese Risiken können die Servicequalität (QoS – Quality of Service) von Verkehrssystemen (die Zuverlässigkeit des Verkehrssystems) und die Sicherheit der Fahrgäste beeinträchtigen. Darüber hinaus kann im Allgemeinen auch die Reputation der Betreiber in Mitleidenschaft gezogen werden. Cyberattacken können sich auch auf Computer und Mobiltelefone der Fahrgäste auswirken.

Der Ansatz für Cybersicherheit muss einen umfassenden Schutz zur Abwehr von Cyberattacken bieten. Gleichzeitig müssen Verkehrsunternehmen gewährleisten, dass sie zur Erfüllung der Compliance-Verpflichtungen bereit sind.

Die Tendenz einer immer umfangreicheren Einbindung von IT-Technologie und Standard-Telekommunikation (TCP/IP, 4G und 5G, WLAN) in wesentliche Verkehrssysteme stellt eine zusätzliche Herausforderung dar. Das wirkt sich nicht nur auf den Aufbau der Verkehrssystemarchitektur, sondern auch auf die Instandhaltung aus. Dabei sind neue Bedrohungen über die gesamte Lebensdauer des Systems hinweg zu berücksichtigen.

CAF – EIN LANGFRISTIG ZUVERLÄSSIGER PARTNER DER AUFTRAGGEBER FÜR SICHERHEIT UND BETRIEBLICHE WIRTSCHAFTLICHKEIT

Digitale Technologien (wie künstliche Intelligenz, gewerbliches IdD, Big Data, Telekommunikation, Blockchain usw.) sowie Standardprodukte wie COTS werden Verkehrsunternehmen maßgeblich bei der Bewältigung dieser neuen Herausforderungen unterstützen. Dafür leisten sie folgende Beiträge:

- Steigerung der Servicequalität (Verfügbarkeit, Zuverlässigkeit),
- Steigerung der Kapazität von Verkehrssystemen bei möglichst geringen Investitionen,
- Senkung der Betriebskosten bei immer stärker zunehmenden Wettbewerbsdruck.

Während dieser große technologische Wandel vollzogen wird, sind die maßgeblichen Eigenschaften des wesentlichen Verkehrssystems und insbesondere die Sicherheit aufrecht zu erhalten.

CAF bietet im Verkehrswesen umfassende Portfolios für Verkehrssysteme an, wie z. B. für 1) Schienenverkehr (als Rückgrat der Mobilitätssysteme) und 2) Straßenverkehr (als europäischer Marktführer im Busgeschäft). Im Rahmen Wertschöpfungskette ist CAF u. a. auch in der Finanzierung, globalen schlüsselfertigen Projekten, Schienenfahrzeugen, Signalisierung, Komponenten und Dienstleistungen sowie in vorbeugender und korrektiver Instandhaltung tätig.

Für CAF war von jeher das wichtigste Ziel, den Verkehrsunternehmen sichere Systeme zur Förderung der betrieblichen Wirtschaftlichkeit bereitzustellen. In Anbetracht der neuen Gefahren hat CAF sich schon früh die Initiative ergriffen: Das interne Team von CAF wurde auf einen angemessen Kenntnisstand hin geschult und die Produkte und Portfolios – sowohl für Schienen- als auch für Straßenverkehr – durch Technikgestaltung vor Cyberattacken geschützt.

LEISTUNGEN UND PORTFOLIO FÜR CYBERSICHERHEITVON CAF

Cybersicherheit wirkt sich auf das Risikomanagement für Telekommunikation, Produkte und Cybersicherheit aus. Das betrifft u. a. die allgemeine Sicherheit, die Betriebssicherheit, die Instandhaltung während der gesamten Lebensdauer von Verkehrssystemen und nicht zuletzt die Sensibilisierung und Schulung der Angestellten von Auftraggebern und Lieferanten. Das Programm für Cybersicherheit von CAF baut auf mehreren Achsen herum auf, um alle erforderlichen Aspekten zu berücksichtigen. Dazu zählen u. a. auch Partner und Subunternehmer von CAF.

- Eine der Hauptachsen des Programms für Cybersicherheit befasst sich mit die Sensibilisierung und Schulung von wichtigen Mitarbeiterinnen und Mitarbeitern von CAF. Dadurch möchten wir nicht nur den Kenntnisstand in der Sicherheitskultur bei CAF gewährleisten. Es sollen auch unsere Auftraggeber in allen Projektphasen – von der Verhandlung über die Lieferung bis hin zur Instandhaltung unterstützt werden.

- Eine zweite Achse befasst sich mit den Lösungen für „Datenschutz durch Technikgestaltung“. Neben den nationalen Normen werden die anerkannten Normen der Industrie wie IEC 62443 und CENELEC TS-50701 für IT-Sicherheit in Bahnanwendungen und die UNECE-Regulierungen R155 und 156 für Busse befolgt.

  Mit der Cybersicherheit unterstützt CAF seine Auftraggeber über mehrere Jahrzehnte hinweg von der Inbetriebnahme der Verkehrssysteme bis hin zu verschiedenen Betriebsphasen. Dabei werden auch Instandhaltung und Sicherheitsüberwachung berücksichtigt. Im Laufe der Inbetriebnahme ermitteln wir gemeinsam mit dem Auftraggeber die größten Risiken bezüglich der Cybersicherheit und treffen mit den Produkten für „Datenschutz durch Technikgestaltung“ von CAF die erforderlichen Vorkehrungen zur Risikominderung.

- Zusätzlich zur vertraglichen Lieferung besteht ein Support-Bedarf bei Auftraggebern in Bezug auf Gefahrenabwehr, Beobachtung und Verwaltung von Schwachstellen, Patchmanagement und Security Operation Center (SOC). Dadurch kann die Sicherheitslage kontinuierlich überwacht und verbessert werden, um so Verletzungen der Cybersicherheit vorzubeugen, zu erkennen, zu analysieren und auf sie zu reagieren. CAF hat eine Roadmap ausgearbeitet, mit der Tools für die Umsetzung solcher Maßnahmen entwickelt werden können. Bei den daraufhin folgenden Schritten werden einerseits die bisherigen Erfahrungen berücksichtigt und andererseits neue Anforderungen des Auftraggebers anhand des wachsenden Kenntnisstandes im Verkehrswesen vorausschauend angenommen.

- Eine weitere Achse ist der Innovation in der Cybersicherheit gewidmet. Cybersicherheit wurde in den globalen Innovationsprozess von CAF integriert. Durch die kontinuierliche Modernisierung der Cybersicherheit von CAF können unsere Auftraggeber die Sicherheit und den Komfort der Fahrgäste sowie die betriebliche Wirtschaftlichkeit der Verkehrssysteme gewährleisten.

Eisenbahnen müssen als wesentliche Verkehrssysteme stets sicher funktionieren, auch wenn sie Ziel von Cyberattacken werden – und das ist leider nicht immer zu vermeiden. Das ist durch den Schutz kritischer Systeme möglich, die im Rahmen der Cybersicherheit entwickelt wurden. Es geht nicht nur um die Qualität des Betriebs, um Angriffe auf die elektronischen Geräte der Fahrgäste oder um wirtschaftliche Verluste, sondern auch um die Sicherheit der Fahrgäste.

Gemäß den bewährten Verfahrensweisen und den Normen für Cybersicherheit engagiert sich CAF für die Ausstattung der Verkehrsunternehmen mit angemessenen Fähigkeiten und Lösungen mit Datenschutz durch Technikgestaltung für die Inbetriebnahme, die Instandhaltung und die Sicherheitsüberwachung von Verkehrssystemen.

FRAGEN UND ANTWORTEN

Ist das Verkehrswesen von vielen Cyberattacken betroffen?
Im Vergleich zur IT-Branche ist das Verkehrswesen von einer eher geringen Anzahl von Cyberattacken ausgesetzt. Verkehrssysteme sind jedoch von wesentlicher Bedeutung. Die Folgen könnten katastrophal sein und den Ruf des Verkehrsunternehmens schaden. Am gefährlichsten für unsere Branche sind die Advanced Persistent Threats (APTs). Diese Angreifer verfügen über erhebliche finanzielle Mittel und werden oft von staatlicher Seite her gesteuert. Jüngste Ereignisse wie der Krieg in der Ukraine haben die dringende Notwendigkeit gezeigt, den Datenschutz zu verstärken. Durch die Tendenz der Digitalisierung und standardisierten Telekommunikation wird sich die Zahl der Angriffe erhöhen.

Welcher Bedarf und welche Anforderungen bestehen bei den Verkehrsunternehmen?
Der Kenntnisstand in Bezug auf Cybersicherheit fällt je nach Verkehrsunternehmen sehr unterschiedlich aus. CAF arbeitet an einigen Projekten in Ländern mit hohen Anforderungen. Als Mindestmaß sind in solchen Ländern Produkte und Systeme mit „Datenschutz durch Technikgestaltung“ zu liefern. Darüber hinaus müssen während der Lebensdauer von wesentlichen Verkehrssystemen häufig Aufrüstungen vorgenommen werden, um den fortschreitenden Gefahren entgegenwirken zu können.

Inwieweit wirkt sich Cybersicherheit auf fahrerlose Systeme aus?
Derzeit wird die fahrerlose Zugtechnologie in U-Bahnen eingesetzt. Doch künftig werden sie sicherlich auch auf Fernstrecken, in Bussen und Straßenbahnen integriert. Es handelt sich um eine wichtige Tendenz in der Branche, da die Kapazität und Servicequalität von Verkehrssystemen zunehmend gesteigert werden muss. Daraus wird sich ein zusätzlicher Bereich für die Risikoanalyse ergeben. Das liegt daran, dass kein Mensch den Entscheidungsprozess steuert und der hohe Grad der Automatisierung auf einer stärker standardisierten Telekommunikation zwischen den fahrzeug- und streckenseitigen Produkten der Züge und Busse aufbaut.

Inwiefern wirkt sich die Cybersicherheit auf die tägliche Arbeit an Projekten von CAF aus?
Es ist von grundlegender Bedeutung, die Cybersicherheit in über den gesamten Projektlebenszyklus zu integrieren. Das reicht von der Prüfung der Anforderungen bis hin zur Endabnahme des Projekts. Das ist ähnlich wie bei der Sicherheitsanalyse. Der wesentliche Unterschied besteht in der Cybersicherheit darin, dass bereits in der Entwicklungsphase die Wartungsfähigkeit des Systems zu berücksichtigen ist, da in der Cybersicherheit neue Gefahren oft durch Patches abzuwenden sind.