Leitfaden: Cybersecurityanforderungen an Straßenbahnen

1. Die IT-Sicherheit der Straßenbahn muss dem "Stand der Technik" entsprechen.
2. Die Netzwerke innerhalb des Fahrzeugs und zwischen Fahrzeug und Leittechnik müssen segmentiert werden, um kritische Steuerungssysteme von weniger sensiblen Systemen (z. B. Fahrgast-WLAN, Infotainment) zu isolieren.
3. Es müssen robuste Zugriffskontrollmechanismen (z. B. starke Authentifizierung, Zwei-Faktor-Authentifizierung) für alle Systeme mit administrativem oder sicherheitsrelevantem Zugriff implementiert werden (Standardpasswörter sind unzulässig).
4. Alle sicherheitsrelevanten Zugriffe und Systemereignisse müssen protokolliert (geloggt) und auf Anomalien überwacht werden (als „Bedrohungslogbuch“ - Integration in ein Security Information and Event Management (SIEM) System).
5. Die Integrität und Verfügbarkeit der sicherheitsrelevanten Daten und Systeme (wie Signalgebung, Kommunikation und Steuerung) muss vorhanden sein, um die Betriebssicherheit sicherzustellen.
6. Es sind regelmäßige Sicherheitsprüfungen und Software-Updates vorzusehen. Hierzu hat der Betreiber ein risikobasiertes Patch-Management-Verfahren zu implementieren, das die umgehende Installation von Patches für kritische Schwachstellen vorschreibt und für reguläre Sicherheits- und Wartungsupdates geeignete Zyklen vorsieht. Die Verfügbarkeit der OT-Systeme (Operational Technology) ist dabei zu gewährleisten.
7. Straßenbahnen müssen mit ausreichend sicheren Kommunikationsprotokollen und Mechanismen ausgestattet werden, die einen klar definierten Zugriff auf Steuerungssysteme über drahtlose Netzwerke (Over-the-Air) gestatten. Insbesondere ist eine robuste Verschlüsselung sämtlicher drahtloser Datenübertragungen und eine strikte Authentifizierung der Fernzugriffsversuche sicherzustellen.
8. Straßenbahnen müssen über eine dezidierte Konfigurationsoption (alternativ: einen "Behördenmodus") verfügen, um nicht betriebsnotwendige Komfort- und Konnektivitätsfunktionen (einschließlich, aber nicht beschränkt auf mobile Datenverbindungen und Infotainment-Dienste) gezielt zu deaktivieren. Das Fahrzeug muss in einen cyber-sicheren Zustand versetzt werden können, so dass ein eingeschränkter Betrieb (mindestens: Notfall- und Evakuierungsfunktionen) sichergestellt ist, ohne diesen von außen kompromittieren zu können
9. Sicherheitsrelevante Kernfunktionen sind auf Basis einer Gefährdungs- und Bedrohungsanalyse zu identifizieren. Für diese Funktionen sind angemessene Maßnahmen, wie beispielsweise eine autarke Notbremsschleife, eine direkte Brandmeldeleitung sowie eine Not-Aus-Kette zur Spannungsfreischaltung, zur Risikoreduktion festzulegen und wirksam umzusetzen (Hardware-Override).