Stellungnahme Deutsches Verkehrsforum e.V.

Behandlung des Bahnsektors im EU-Cyber Resilience Act (CRA)

Berlin, 24.10.2023

Der aktuelle Entwurf des Cyber Resilience Acts (CRA) der EU-Kommission sieht eine Einbeziehung des Bahnsektors in den Anwendungsbereich vor, während Luftverkehr und Automobil explizit ausgenommen sind.

Die Einbeziehung des Bahnsektors in den CRA bringt für den Schienenverkehr und die herstellenden Unternehmen erhebliche zusätzliche Belastungen. Kritische Faktoren sind hier insbesondere

- eine unzureichende Differenzierung von Geschäftsbeziehungen Business-to-Business (B2B) und Business-to-Consumer (B2C),
- die mangelhafte Berücksichtigung von extrem langen Produktlebenszyklen von teilweise über 30 Jahren, wie sie bei Schienenfahrzeugen und Infrastrukturen gegeben sind,
- die fehlende Berücksichtigung bahnspezifischer Besonderheiten, insbesondere der Abgrenzung der dort verwendeten operationalen Technologien mit starker Verzahnung von Computern, Kommunikationssystemen, physischen Einheiten und Infrastrukturen von der herkömmlichen Informationstechnik,
- die unzureichende Rollendefinition von Herstellern, Eigentümern und Betreibern,
- die fehlende Anpassung der Begrifflichkeit des „Patchens“ an den Schienenverkehrssektor, da Änderungen an Modulen in der Regel eine betriebliche Neuzulassung zur Folge haben.

Bestehende Vorschriften in Form der EU Richtlinie (EU) 2016/797 mit ihren Technischen Spezifikationen für die Interoperabilität (TSI) und die Bahnnorm IEC 62443 setzen bereits einen hohen Sicherheitsstandard voraus, der bei der Zulassung jeweils überprüft und bestätigt wird. Die zugrundeliegenden Normen befinden sich zudem aktuell in der weiteren Anpassung, um dem Aspekt der Cybersicherheit noch stärker Rechnung zu tragen. Es droht eine administrative Doppelbelastung durch den CRA, der nun zusätzlich zu den bestehenden schienenspezifischen Richtlinien und Sicherheitsnormen zu berücksichtigen ist.

Im nun anstehenden Trilog-Verfahren sollte die Möglichkeit genutzt werden, den CRA und die Rahmenbedingungen so anzupassen, dass die Besonderheiten der Schienenverkehrsbranche abgebildet werden, das hohe Sicherheitsniveau des Sektors und die verantwortungsvolle Zulassungspraxis erhalten bleiben, sowie bürokratische Prozesse auf ein Minimum beschränkt und nicht dupliziert werden. Die Änderungsvorschläge seitens des Rates und federführendem Ausschuss des EP zeigen hierfür Ansätze auf.

Wichtige Aspekte hierbei sind:

- **Übergangsfristen** sind so zu gestalten, dass die notwendigen Anpassungen bei den Spezifikationen erfolgen und Prozesse umgestellt werden können. Das Datum der Anwendbarkeit für betroffene Hersteller sollte daher mindestens 48 Monate nach dem Zeitpunkt des Inkrafttretens des CRA liegen. Komplexe Bereiche wie der Schienenverkehrssektor benötigen zusätzliche Zeit zur Umsetzung über alle Wertschöpfungsbereiche hinweg, so dass hier in der Kombination mit der Umsetzungszeit der Hersteller von 72 Monaten als realistischen Zeitrahmen für die vollständige Umsetzung des CRA auszugehen ist.
- Der Ansatz des Europäischen Rates, die **Gruppe der kritischen Produkte** in Annex III besser zu strukturieren, zu verdichten und die Klassifizierung anzupassen, ist unbedingt zu unterstützen. Im Sinne eines modularen und risikobasierten Ansatzes sowie unter Beibehaltung des horizontalen Ansatzes geht es darum, Produkte mit digitalen Elementen zu identifizieren, die einer besonderen Aufmerksamkeit unterliegen müssen und damit klare Verantwortungen festzulegen. Die vom Rat für Annex III vorgeschlagene Abgrenzung nach cyberkritischen und systemkritischen Funktionalitäten verbunden mit der risikobasierten Verdichtung auf identifizierte kritische Produktkategorien ist vor diesem Hintergrund der richtige Weg.
- Ein vom Hersteller oder dem Inverkehrbringer erklärter **Support-Zeitraum** (Support-Period) ist transparenter und nachvollziehbarer als eine Anlehnung der Support-Verpflichtung an die **Produktlebensdauer**. Gerade bei extrem langlebigen Produkten ist die transparente Verpflichtung wichtig, den Support zu Cybersicherheitsaspekten für einen festen Zeitraum zuzusichern, anstelle der Zusicherung über eine schwer zu bestimmende Produktlebensdauer. Der Vorschlag des zuständigen ITRE-Ausschusses des Europäischen Parlaments in Artikel 3 (21c) / Artikel 10 (6) ist daher unbedingt zu unterstützen. Die vorgeschlagene Marktbeobachtung stellt dabei sicher, dass Support-Zeitraum und Produktlebensdauer in einem ausreichenden Verhältnis stehen.
- Um sicherzustellen, dass die Zielsetzung des CRA erreicht und gleichzeitig den Besonderheiten des Bahnsektors Rechnung getragen wird, ist die Einführung des Begriffs "**Produktkonfigurationsmanagement**" (via Ergänzung des Art. 3[1]) vorzusehen. So sind die Verpflichtungen der Hersteller für jene Fälle anzupassen, in denen der Hersteller nicht für das Konfigurationsmanagement nach dem Inverkehrbringen des Produkts verantwortlich ist. Hierzu sollte eine vertragliche Vereinbarung zwischen Hersteller und Nutzer erfolgen, die die in Anhang 1 Abschnitt 2 genannten grundlegenden Anforderungen abdeckt. Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte gemäß Artikel 50 zu erlassen, um Leitlinien für den Geltungsbereich solcher vertraglichen Vereinbarungen festzulegen.

[1] Das Produktkonfigurationsmanagement stellt per definitionem sicher, dass Produkte ordnungsgemäß installiert und gewartet werden, und zwar innerhalb der technischen Spezifikationen und Annahmen, für die sie entworfen wurden, oder unter Bedingungen, die vernünftigerweise vorhersehbar sind.

- Die Klarstellungen des Europäischen Rates und des ITRE-Ausschusses, dass **Security Updates** zunächst nicht als maßgebliche Änderung (substantial modification) zu werten sind und daher keine Neuzulassung eines Produktes nach sich ziehen (Anmerkung 22a / Artikel 3 (31)), sind unbedingt zu unterstützen. Eine Einordnung als substanzielle Änderung würde u.U. das Erlöschen der eisenbahnrechtlichen Zulassung und damit das Stilllegen ganzer Fahrzeugflotten oder Infrastrukturbestandteile und damit erhebliche Einschränkungen für die Mobilität bedeuten.
- Der CRA muss sicherstellen, dass auch künftig vorhandene **Sektorenstandards** verbunden mit einem **Self-Assessment** im Einklang mit dem CRA ihre Wirkung entfalten können. Das Aufsetzen auf bereits vorhandenen Sektorenstandards bzw. deren Anpassung ist im Sinne des CRA, da die Umsetzung zügiger erfolgen kann, als durch die Schaffung neuer Standards. EU-Kommission, Zulassungsbehörden und Branche sind aktuell dabei, die vorhandenen Standards so anzupassen, dass alle Belange der Cybersicherheit gemäß CRA adressiert werden. Somit können in den Zulassungsprozessen die Anforderungen des CRA abgebildet und teilweise sogar übertroffen werden. Durch die Verwendung von Produkten mit digitalen Elementen mit CRA-Compliance und die entsprechende Due Diligence bei der Integration wird ein hohes Security-Niveau unter Berücksichtigung der Konformitätsbewertungsverfahren des CRA gewährleistet.