

---

## Stellungnahme zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

---

Der Verband Deutscher Verkehrsunternehmen (VDV), Branchenverband für über 600 Unternehmen des Öffentlichen Personen- und Schienengüterverkehrs in Deutschland, begrüßt grundsätzlich die Weiterentwicklung des Ordnungsrahmens zum Schutz informationstechnischer Systeme von Kritischen Infrastrukturen. Denn auch die Anlagen und Einrichtungen sowie technischen Systeme im Nah- und Fernverkehr gehören zu den „Kritischen Infrastrukturen“ (KRITIS) und sind für die Sicherung der Mobilitätsangebote von zentraler Bedeutung. Das betrifft nicht nur den Öffentlichen Personennahverkehr (ÖPNV) als Teil der Daseinsvorsorge, der Versorgungsmöglichkeiten und die gesellschaftliche Teilhabe aller Menschen absichert, sondern auch den Güterverkehr auf der Schiene. Insbesondere zu Beginn der Corona-Pandemie, als viele Grenzübergänge auf den Autobahnen vorübergehend geschlossen worden sind, konnten mit Hilfe der Kapazitäten im Schienengüterverkehr Versorgungsengpässe verhindert werden.

An vielen Stellen trägt der vorliegende Gesetzentwurf „zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz 2.0) diesen und anderen Rahmenbedingungen Rechnung. So sind beispielsweise die **Informationspflichten** zu begrüßen. Demnach muss das Bundesamt für Sicherheit in der Informationstechnik (BSI) Betreiber Kritischer Infrastrukturen vor möglichen Risiken frühzeitig warnen. Zugleich beinhaltet der Gesetzentwurf aber auch Neuregelungen, die im Öffentlichen Personen- und Schienengüterverkehr zu erheblichen Mehrkosten, rechtlichen oder auch betrieblichen Risiken führen können. Das betrifft nicht nur den Eisenbahnverkehr, zu dem im Übrigen auch nicht-bundeseigene Bahnen gehören, sondern auch den Nahverkehr. Vor allem folgende Neuregelungen bedürfen einer Überarbeitung:

Der **§ 3** sieht gegenwärtig vor, dass die Entwicklung und Veröffentlichung von **sicherheitstechnischen Anforderungen an IT-Produkte** ausschließlich durch das BSI erfolgen soll. Da sich der Stand der Technik dynamisch durch etablierte Strukturen der nationalen, europäischen und internationalen Normung weiter entwickelt, besteht durch die angestrebte Regelung die Gefahr, dass die betroffenen Sektoren Kritischer Infrastrukturen von dieser Entwicklung abgekoppelt werden. In der Konsequenz können zum Beispiel die zur Erbringung der kritischen Dienstleistung erforderlichen Komponenten nicht mehr beschafft werden. So ist es sinnvoll, den Passus dahingehend zu ergänzen, dass der Stand der Technik wie bisher auf Basis anerkannter Normen und Standards ausgelegt wird, an deren Erarbeitung die betroffenen Sektoren Kritischer Infrastrukturen und die Wirtschaftsverbände beteiligt sind.

Nachbesserungsbedarf wird darüber hinaus beim **§ 7b** gesehen. Demnach soll das BSI **Angriffssimulationen** auf gesetzlicher Basis durchführen dürfen. Der reinen automatisierten Detektion von Sicherheitslücken in IT-Systemen, die aus dem Internet heraus erreichbar sind, spricht nichts entgegen. Angriffssimulationen auf Betreiber Kritischer Infrastrukturen können aber zu Systemabstürzen führen, die die Erbringung der kritischen Dienstleistung gefährden bzw. unmöglich machen. Mögliche Haftungsansprüche aus diesem Vorgehen sind im vorliegenden Entwurf nicht geregelt. Es muss sichergestellt sein, dass es bei reinen Portscans bleibt und nicht weitere invasive Maßnahmen die Netz- und Informationssicherheit von betroffenen Betreibern gefährden.

Ferner enthält der Gesetzentwurf im **§ 8a (1a)** Anforderungen technischer Art, die praktisch nicht umsetzbar sind. Betroffene Unternehmen stünden vor nicht lösbaren Herausforderungen in rechtlicher und betrieblicher Hinsicht. So ist beispielsweise nicht nachvollziehbar, wie neue Systeme zur Angriffserkennung Störungen im Eisenbahn- oder Nahverkehr eigenständig beseitigen können sollen. Im Übrigen besteht für eine solche automatische Angriffserkennung und Gefahrenbeseitigung in den spezialgesetzlichen Regelungen zur Betriebsdurchführung keine rechtliche Grundlage. Anforderungen dieser Art sollten somit im weiteren Gesetzgebungsverfahren gestrichen werden.

Abschließend ist anzumerken, dass die mit der Gesetzesinitiative vermuteten Kostenbelastungen für die Wirtschaft gem. **E.2 (Erfüllungsaufwand)** nach den bisherigen Erfahrungen und vor dem Hintergrund der aufgewendeten Kosten in den betroffenen Unternehmen zu niedrig angesetzt sind.