UTV Unabhängiger Tanklagerverband e.V.

Stellungnahme

zum

Entwurf eines zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Stand: 09.12.2020) (Zweites IT-Sicherheitsgesetz - IT-SiG 2.0)

1 Vorbemerkung

Der Unabhängige Tanklagerverband e.V. („UTV“) vertritt die Interessen der in Deutschland angesiedelten und mehrheitlich mittelständisch geprägten unabhängigen Tanklager-Betriebe. Die Mitgliederstruktur zeichnet sich dabei durch eine große Heterogenität aus und umfasst sowohl große Unternehmungen mit deutlich mehr als 100 Mitarbeitern als auch kleine Betriebe im Inland mit teilweise weniger als 15 Mitarbeitern.

Der UTV begrüßt grundsätzlich das Bestreben der Bundesregierung, die Sicherheit im Bereich der IT-Infrastruktur in Deutschland signifikant zu stärken. Cyber- und IT-Sicherheit sind eine wesentliche Grundlage für eine langfristige sichere digitale Transformation von Staat, Wirtschaft und Gesellschaft und ermöglichen es der Wirtschaft, ihre Service- und Dienstleistungen nachhaltig und sicher ausüben und anbieten zu können.
Andererseits fordert der UTV, bezüglich der sich aus dem IT-Sicherheitsgesetz 2.0 ergebenden Pflichten für die Wirtschaft auf die Verhältnismäßigkeit der Maßnahmen und Mittel zu achten. Diese Beachtung der Verhältnismäßigkeit beginnt bereits mit der Definition des Geltungsbereiches, der aus Sicht des UTV und bezogen auf einige Sektoren in einem unverhältnismäßigen Maß erweitert werden soll. Dieses stellt insbesondere die mittelständisch geprägten Unternehmen vor gewaltige Herausforderungen und führt zu einer Schwächung der Wettbewerbsfähigkeit.

Georgenstr. 23 - 10117 Berlin - Telefon: +49-30-206 44 190
E-mail: info@tanklagerverband.de - www.tanklagerverband.de

2 Der UTV hat im Einzelnen nachfolgende Forderungen und Anmerkungen:

2.1 Zu E.2 Erfüllungsaufwand für die Wirtschaft

Der vom BMI ermittelte Erfüllungsaufwand für die Wirtschaft Personal- und Sachkosten liegt nach unserer Schätzung deutlich und unverändert unterhalb der realistisch anzusetzenden Kosten.
So hat eine Erhebung der Mineralölwirtschaft (Raffinerie-Produktion und Tanklager-Logistik) ergeben, dass im Rahmen der Umsetzung des IT-Sicherheitsgesetz 1.0 allein für diesen Sektor die jährlichen Personalkosten um ca. 3 Millionen € und die Sachkosten um ca. 10 Millionen Euro gestiegen sind.
Angesichts der Tatsache, dass diese Kosten lediglich einen Sektor repräsentieren und der zukünftige Geltungsbereich gemäß dem vorliegenden Referentenentwurf zum IT-SiG 2.0 noch erweitert werden soll, erscheinen uns die vom BMI ermittelten Kosten als deutlich zu gering angesetzt.

2.2 Zu § 2 f) Abs. (14) Nr. 3. – „Unternehmen im besonderen öffentlichen Interesse“

Die Definition von Betriebsbereichen der oberen Klasse im Sinne der Störfallverordnung als „Unternehmen im besonderen öffentlichen Interesse“ ist nicht nachvollziehbar und erscheint uns darüber hinaus unverhältnismäßig.

Die Zielsetzung des IT-Sicherheitsgesetzes sollte sein, die Versorgung der Bevölkerung mit Leistungen und Produkten, die von Betreibern einer Kritischen Infrastruktur erbracht bzw. geliefert werden, sicherzustellen. Zur Erreichung dieser Zielsetzung wurden im Rahmen der BSI Kritis-Verordnung (BSI KritisV) entsprechende Schwellenwerte definiert, ab deren Überschreitung ein Unternehmen als Kritische Infrastruktur zu definieren ist. In der Praxis hat sich dieses Prinzip seit Inkrafttreten bewährt und eine sichere Versorgung der Bevölkerung beispielsweise mit Kraft- und Brennstoffen durch auf diese Weise definierte Kritische Infrastrukturen kann als gesichert angenommen werden.
Die Störfallverordnung hat darüber hinaus eine gänzlich andere Zielsetzung im Hinblick auf die Bevölkerung – der Schutz der Bevölkerung vor Störfällen und nicht die Sicherstellung der Versorgung steht hier im Fokus.

Mit der geplanten Ausweitung des Geltungsbereiches auf Betriebsbereiche der oberen Klasse im Sinne der Störfallverordnung sollen nunmehr für einige Teil-Sektoren im Bereich der Mineralölversorgung die genannten Schwellenwerte indirekt und unverhältnismäßig stark nach unten angepasst werden.

Mit dieser Regel würde eine nicht unerhebliche, zusätzliche Anzahl von Tanklagerbetrieben als „Unternehmen im besonderen öffentlichen Interesse“ eingestuft. Diese überwiegend der Gruppe der KMU zuzuordnenden Betriebe haben aus betriebswirtschaftlichen

Motiven heraus in den letzten Jahren ihre IT-Sicherheitssysteme auf einen hohen Sicherheitsstandard gebracht. Die zukünftige Einstufung als „Unternehmen im besonderen öffentlichen Interesse“ bedeutet für diese Betriebe einen unverhältnismäßig höheren Personal-, Verwaltungs- und Sachaufwand.

Der UTV fordert das BMI daher auf, aus den zuvor genannten Gründen der Relevanz sowie der Verhältnismäßigkeit die Nummer 3. in § 2 f) Abs. (14) ersatzlos zu streichen.

2.3 Zu § 8a – „Sicherheit in der Informationstechnik von KRITIS“

Die beabsichtigten Änderungen bezogen auf § 8a Abs. 1 BSIG resultieren aus unserer Sicht in einer Undeutlichkeit bezogen auf den Zeitpunkt der Nachweiserbringung für (neue) Kritische Infrastrukturen, die erstmalig den entsprechenden Schwellenwert überschritten haben. Die entsprechende Passage im vorliegenden Referentenentwurf kann so interpretiert werden, dass betroffene Unternehmen bereits 1 Tag nach Überschreiten des Schwellenwertes den geforderten Nachweis gegenüber dem BSI zu erbringen haben.
Für ein Unternehmen in der Tanklager-Logistik ist es schwierig, das Erreichen eines Schwellenwertes verlässlich zu prognostizieren, da der Schwellenwert durch das jährliche Umschlagsvolumen definiert ist. Dieses Umschlagsvolumen wird jedoch durch die Lager- und Umschlagsvertragspartner der Unternehmen bestimmt – das Tanklager-Unternehmen hat hierauf keinen direkten Einfluss.
Daher halten wir es für notwendig und verhältnismäßig, den betroffenen Unternehmen ab dem Zeitpunkt des erstmaligen Überschreitens des für ihn relevanten Schwellenwertes eine realistische Übergangszeit einzuräumen.
Der UTV fordert daher, denjenigen Unternehmen, die erstmalig den für sie relevanten Schwellenwert überschreiten, einen angemessenen Übergangszeitraum von 1 Jahr ab dem Zeitpunkt des Überschreitens zu gewähren.

§ 8a Abs. (1b) legt fest, dass Betreiber Kritischer Infrastrukturen für die Angriffserkennung und -nachverfolgung relevante nicht-personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens vier Jahre speichern müssen.
Der UTV lehnt diese Anforderung als völlig realitätsfern ab. Betreiber Kritischer Infrastrukturen werden in § 8a Abs. (1a) dazu verpflichtet, Systeme zur Angriffserkennung zu installieren, um „fortwährend Bedrohungen zu identifizieren und zu vermeiden“. Es ist nicht ersichtlich, warum diese Daten für vier Jahre gespeichert werden müssen. Bei Unternehmen fallen täglich und zunehmend große Datenmengen pro Tag an. Diese verpflichtend für vier Jahre speichern zu müssen, ist insbesondere aus mittelständischer Unternehmersicht nicht darstellbar.

Der UTV fordert daher, die im bisherigen Entwurf definierte Pflicht zur Speicherung von Daten deutlich zu reduzieren. Wir halten eine Speicherzeit von mindestens 3 Monaten im Normal-Betrieb sowie von maximal 12 Monaten bei Verdacht auf einen Cyber-Angriff für realistisch und verhältnismäßig.

2.4 Zu § 14 – „Bußgeldvorschriften“

Der UTV unterstützt vor dem Hintergrund der steigenden Bedeutung einer sicheren IT-Sicherheitsstruktur in Wirtschaftsunternehmen grundsätzlich eine maßvolle Anpassung der aktuell geltenden Bußgelder. Eine Erhöhung der Bußgelder von derzeit 50.000 € bzw. 100.000 € auf bis zu 2.000.000 € erachten wir als vollkommen überzogen und fordern daher eine deutliche Reduzierung.

Grundsätzlich möchten wir diesbezüglich darauf verweisen, dass nationale Alleingänge im Europäischen Binnenmarkt wettbewerbsverzerrend wirken können. Eine harmonisierte Betrachtung der Schutzziele für den europäischen Binnenmarkt und eine durch alle Partner und Beteiligte europäisch erarbeitete Umsetzung im Rahmen von EU-Richtlinien und -Verordnungen ist aus unserer Sicht der zu präferierende Ansatz.

Berlin, 10. Dezember 2020