Thomas Hailer
Geschäftsführer

DVF
Deutsches Verkehrsforum

> Klingelhöferstraße 7
10785 Berlin

Telefon +49 (30) 26 39 54-10
Telefax +49 (30) 26 39 54-22

hailer@verkehrsforum.de
www.verkehrsforum.de

> Deutsches Verkehrsforum e.V. · Klingelhöferstraße 7 · 10785 Berlin

Herrn Dr. Dürig
Referatsleiter IT II 1
Grundsatzangelegenheiten, IT- und Cybersicherheit;
Schutz im Cyberraum; Cyberabwehrzentrum
Bundesministerium des Innern
Alt-Moabit 140
10557 Berlin

Per Mail : ITII1@bmi.bund.de

16. Dezember 2016
TH/ST

Stellungnahme zum Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 (NIS-RL-Umsetzungsgesetz)

Sehr geehrter Herr Dr. Dürig,

wir bedanken uns für die Möglichkeit zur Stellungnahme zum Entwurf des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS) in der Union. Aufgrund der sehr kurzen Fristsetzung können wir unsere Ausführungen jedoch nur in genereller Form übersenden. Daher weisen wir nachfolgend nur auf einige grundsätzliche Kritikpunkte hin.

Erweiterung der Aufsichtsbefugnis des BSI zurücknehmen

Mit der Neufassung des Absatzes 4 des § 8a werden die Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) über die Anforderungen der NIS-Richtlinie hinaus unbegründet erweitert. Die Forderungen aus der NIS-Richtlinie zu den zu erbringenden Nachweisen sind bereits durch das bestehende IT-Sicherheitsgesetz vollumfänglich erfüllt. Sollte das BSI

> „beim Betreiber die Einhaltung der Anforderungen … überprüfen“ und
> „zu diesem Zweck das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstige Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung“

einfordern können, verfügt es über eine neue Aufsichtsbefugnis. Eine weitere Aufsichtsbehörde ist unnötig, führt zu Doppelstrukturen und Mehrkosten, ohne einen Sicherheitsgewinn zu erbringen. Daher sollte der Satz gestrichen werden.

Erfüllungsaufwände senken

Sowohl in der Begründung der NIS-Richtlinie also auch im Entwurf des BSIG des Jahres 2014 wird betont, dass der Aufwand und Nutzen der Sicherheitsmaßnahmen in einem angemessenen Verhältnis stehen müssen.

So steht in der Begründung der NIS-Richtlinie im Absatz (53) „Damit keine unverhältnismäßige finanzielle und administrative Belastung für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste entsteht, sollten die Verpflichtungen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist."

Die im Teil III der Begründung des aktuell vorliegenden Umsetzungsgesetzes aufgeführten Aufwendungen sind unrealistisch. Der Erfüllungsaufwand ist deutlich höher als beschrieben, womit die Angemessenheit ebenfalls in Frage zu stellen ist. Nach den vom BSI getätigten Konkretisierungen zu den Erwartungen an die Erbringung von Nachweisen (Vergleiche „Orientierungshilfe zu den Nachweisen gemäß § 8a Abs. 3 BSI-Gesetz", V0.9) wurden vom Branchenarbeitskreis Transport und Verkehr realistisch zu erwartende Kosten über die Zahl von ca. 2.000 Unternehmen kalkuliert. Diese wurden dem Bundesministerium des Inneren (BMI) am 22.09.2016 übermittelt und um deren Berücksichtigung gebeten. Dies ist offensichtlich nicht geschehen.

Durch die aktuell formulierten aufwändigen Vorgaben, entstehen der Wirtschaft alle zwei Jahre allein für die Nachweise zusätzliche Aufwände von bis zu EUR 380 Mio. Des Weiteren schränken die detaillierten und weitgreifenden Vorgaben in dieser Orientierungshilfe die Handlungsfreiheit der Betreiber, die hohe Resilienz ihrer IT in den kritischen Infrastrukturen nachzuweisen, ein. Im Ergebnis muss die Wirtschaft erhebliche Mehrkosten schultern, denen kein unmittelbarer Nutzen in Form einer höheren IT-Sicherheit gegenübersteht. Für ein angemessenes Verhältnis von Aufwand und Nutzen sind die Erfüllungsaufwendungen deutlich zu senken. Die Angemessenheit der geforderten Maßnahmen sollte gesetzlich verankert werden.

Ausmaß einer Störung

In der NIS-Richtlinie werden die Kriterien zur Bestimmung der Kritikalität und den zugehörigen Schwellenwerten deutlich klarer formuliert als im vorliegenden Gesetzentwurf. Laut Artikel 6 (1) c der NIS-Richtlinie sind Ausmaß und Dauer der Auswirkungen von Sicherheitsvorfällen zur Bestimmung der Kritikalität heranzuziehen. Ebenso ist nach Artikel 6 (1) f die Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Bereitstellung des jeweiligen Dienstes in die Bestimmung einzubeziehen. Beide Kriterien fehlen im vorliegenden Entwurf des Umsetzungsgesetzes und sind für eine eindeutige Abgrenzung der Vorfallsschwere aufzunehmen.

Wir möchten Sie bitte unsere Anmerkungen im weiteren Abstimmungsprozess zu berücksichtigen und stehen Ihnen gern für Rückfragen zur Verfügung.

Mit freundlichen Grüßen

Thomas Hailer
Geschäftsführer

CC: Abteilung Digitale Gesellschaft, Bundesministerium für Verkehr und digitale Infrastruktur
CC: Nationaler Normenkontrollrat (florian.spengler@bk.bund.de)