Strahl, Claudia

Von: Lutz Könner (ZDS) <lutz.koenner@zds-seehaefen.de>
Gesendet: Freitag, 14. November 2014 13:53
An: ITII1_; Spauschus, Philipp, Dr.
Cc: Tatjana Altmann (ZDS)
Betreff: Spauschus meißner Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Sehr geehrter Herr Dr. Dürig,
sehr geehrter Herr Spauschus,
sehr geehrte Damen und Herren,

haben Sie vielen Dank für die Einräumung der Möglichkeit, uns zu dem o. g. Gesetzesentwurf äußern zu können.

Der **Zentralverband der deutschen Seehafenbetriebe e.V. (ZDS)** gibt folgende Stellungnahme zu dem Entwurf eines IT-Sicherheitsgesetzes ab:

- **§ 2 Absatz 10 und § 10 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik – BSI-Gesetz (Seite 7 und 13 des Entwurfs)**

Zu den „Betreibern kritischer Infrastrukturunternehmen" können auch die Hafenumschlagsbetriebe gehören, sofern sie wegen ihrer bedeutenden Versorgungsfunktion durch Rechtsverordnung als „kritische Infrastruktur" näher bestimmt werden. Diese **Frage des Anwendungsbereichs** stellt einen wesentlichen Regelungsgegenstand dar, der folglich nach Auffassung des ZDS **im Gesetz selber zu regeln** gewesen wäre und nicht im Wege einer Rechtsverordnung ausgelagert werden sollte.

Nach § 10 Absatz 1 des BSI-Gesetzes geht jedoch der anhand der in den jeweiligen Sektoren erbrachten Dienstleistungen vorgenommenen Bestimmung durch Rechtsverordnung, ab welchem Schwellenwert welche Einrichtung, Anlagen oder Teile davon als „kritische Infrastrukturen" im Sinne dieses Gesetzes gelten, u. a. eine **Anhörung der betroffenen Betreiber und Wirtschaftsverbände** voraus.

Sollte am Instrument der **Rechtsverordnung** seitens des BMI festgehalten werden, regt der ZDS eine **detaillierte Ausgestaltung der sektorspezifischen Definitionen unter Beteiligung der Expertisen der Verbändewirtschaft** an (Fortführung des Dialogs zwischen Verwaltung, Politik und Wirtschaft).

- **§ 8a Absätze 1 bis 3 BSI-Gesetz (Seite 9 und 10)**

Positiv ist zu bewerten, dass für angemessene organisatorische und technische Vorkehrungen zur Vermeidung von IT-Störungen nunmehr die Betreiber selbst branchenspezifische Sicherheitsstandards zur Gewährleistung der gesetzlichen Anforderungen vorschlagen können. Der Nachweis der Erfüllung der Anforderungen kann jetzt nicht nur durch Sicherheitsaudits, sondern ebenfalls durch Zertifizierungen oder Prüfungen erfolgen.

Problematisch ist dabei, dass sowohl für den jeweiligen Vorschlag als auch für den Nachweis eine Frist von zwei Jahren nach Inkrafttreten der Rechtsverordnung gelten soll. Dieser Zeitraum erscheint für den Erfüllungsaufwand insgesamt zeitlich zu knapp, da ein zusätzlicher Verwaltungs-, Bürokratie- und Kostenaufwand entsteht. Der ZDS schlägt vor diesem Hintergrund eine **Erhöhung der Umsetzungsfrist auf vier Jahre** vor, um den Anforderungen in vollem Umfang gerecht zu werden.

- **§ 8b Absatz 3 und 4 BSI-Gesetz (Seite 10 und 11)**

Die „**Betreiber kritischer Infrastrukturen**" sind gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentrale Meldestelle unverzüglich im Hinblick auf „**bedeutende Störungen** ihrer Informationstechnischen Systeme, Komponenten oder Prozesse" **meldepflichtig**.
Eine **Störung** liegt nach dem BSI-Gesetz vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken (so z. B. Fälle von Sicherheitslücken, Schadprogrammen, erfolgte, versuchte oder erfolgreich abgewehrte Angriffe auf die Sicherheit der Informationstechnik, Defekte am System nach Softwareupdates). Eine **bedeutende** Störung liegt dann vor, wenn die Funktionsfähigkeit des Betreibers oder die von diesem betriebene kritische Infrastruktur bedroht sind.

Die Einrichtung einer – jetzt fakultativ auch gemeinsamen – Kommunikationsstruktur für Meldepflichten ist unter dem Gesichtspunkt des festgelegten Zeitraumes von sechs Monaten mehr als fragwürdig anzusehen, da dafür erhebliche organisatorische Ressourcen für eine planbare, funktionierende und strategische Vorbereitung notwendig sind. Der ZDS schlägt daher auch hier eine **Erhöhung der Umsetzungsfrist auf vier Jahre** vor.

- **Gefahr der Doppelregulierung**

Zudem regen wir an, dass im Rahmen des Gesetzgebungsverfahrens auch geprüft werden sollte, ob und welche europarechtlichen Vorgaben letztlich in deutsches Recht umgesetzt werden müssen, damit Doppelregelungen sowie strengere Regelungen als vom EU-Gesetzgeber verlangt vermieden werden.

Insbesondere sollte der Kommissionsvorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union vom 07.02.2013 (COM(2013) 48) und der Stand des Rechtsetzungsverfahrens auf EU-Ebene berücksichtigt werden. Der EU-Richtlinienvorschlag COM (2013) 48 enthält eine nicht erschöpfende Liste der „Betreiber kritischer Infrastrukturen" im Anhang II. Dort werden für den Bereich „Verkehr" neben „Betreibern von Verkehrsmanagement- und Verkehrssteuerungssystemen" auch „Unterstützende Logistikdienste: a) Lagerhaltung und Lagerung b) Frachtumschlagsleistungen und c) andere unterstützende Verkehrsleistungen" aufgezählt. Am 13.03.2014 wurde der KOM-Vorschlag vom Europäischen Parlament mit Änderungen angenommen. In den Änderungsvorschlägen des Europäischen Parlaments wird insbesondere ein flexibleres Verfahren der Überprüfung und Überwachung der IT-Sicherheit gefordert.

- **Verpflichtungen aus dem ISPS-Code rechtfertigen Bereichsausnahme**

Schließlich möchten darauf hinweisen, dass **gleichgerichtete Pflichten für Hafenanlagen bereits aufgrund der Vorschriften des Internationalen Codes für die Gefahrenabwehr auf Schiffen und in Hafenanlagen** (International Ship and Port Facility Security Code - ISPS-Code) bestehen.

Im Einzelnen:

- Die auf Schiffen und in Hafenanlagen vorzunehmende Risikobewertung umfasst gemäß Ziffer 8.3.5 und Ziffer 15.3.5 ISPS-Code auch Funk- und Telekommunikationssysteme einschließlich Computersysteme und Netzwerke.

- Zusätzlich schreibt Ziffer 15.16 des ISPS-Codes vor, dass bei der Feststellung von Schwachstellen Maßnahmen zum Schutz von Funk- und Telekommunikationsausrüstung, Hafendiensten und Versorgungseinrichtungen, einschließlich Computersysteme und Netzwerke geprüft werden sollen.

- Nach Ziffer 16.2 des ISPS-Codes müssen bei der Erstellung des Plans zur Gefahrenabwehr in der Hafenanlage die Merkmale der Risikobewertung, die auch Computersysteme und Netzwerke umfasst (s.o.) und andere örtliche oder nationale Erwägungen zur Gefahrenabwehr behandelt und geeignete Maßnahmen zur Gefahrenabwehr festgelegt werden, um die Wahrscheinlichkeit eines Verstoßes gegen Sicherheitsvorschriften und die Folgen potentieller Risiken auf ein Mindestmaß zu beschränken. Somit enthält bereits der für die Hafenanlage zu erstellende Gefahrenabwehrplan insbesondere auch Anforderungen an die IT-Sicherheit.

- Zudem werden hierbei „kritische Infrastrukturen" ebenfalls bereits durch den ISPS-Code berücksichtigt. Nach Ziffer 15.7.3 des ISPS-Codes können Systeme wie Stromverteilungssysteme, Funk- und

Telekommunikationssysteme sowie Computersysteme und Netzwerke zu derjenigen Infrastruktur gehören, deren Schutz als von Bedeutung einzustufen ist. Hierbei ist nach Ziffer 15.6 des ISPS-Codes die Überlegung wichtig, ob die Hafenanlage, das Gebäude oder die Einrichtung auch ohne den Vermögenswert weiter funktionieren kann und in welchem Umfang eine schnelle Wiederherstellung der normalen Funktionsweise möglich ist.

- Da die Risikobewertungen und Gefahrenabwehrpläne der Hafenanlagen regelmäßig zu prüfen und zu aktualisieren sind (Ziffer 15.4 und 16.3.8 des ISPS-Codes), wird bereits auf diese Weise erreicht, dass Schutzmaßnahmen zur IT-Sicherheit dem aktuellen (technischen) Stand entsprechen.

- Der ISPS-Gefahrenabwehrplan jeder Hafenanlage mit den darin enthaltenen IT-Sicherheitsmaßnahmen wird von der zuständigen Behörde regelmäßig überprüft und auditiert. Zusätzlich zu dem Audit, das die für die Gefahrenabwehr zuständige Behörde vornimmt, führen auch Beauftragte der Europäischen Kommission regelmäßige Inspektionen in Hafenanlagen durch (Artikel 4 Absatz 4 bis 6 der Verordnung Nr. 725/2004 vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen).

Mit den ISPS-Vorschriften besteht seit 2004 ein bewährtes Qualitätsprüfungs- und -sicherungssystem für die Sicherheit auf Schiffen und in Hafenanlagen, von dem ausdrücklich auch Computersysteme und Netzwerke erfasst werden. Die ISPS-Vorschriften wurden EU-weit durch die Verordnung Nr. 725/2004 vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen als zwingendes Recht etabliert und durch die Richtlinie 2005/65/EG vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen fortgeschrieben.

Diese weitreichende Sicherheitsvorschriften des ISPS-Codes rechtfertigen es unseres Erachtens, Hafenanlagen, die bereits die Anforderungen des ISPS-Codes zu erfüllen haben, sowohl vom Anwendungsbereich der vorgeschlagenen Richtlinie COM (2013) 48 wie auch vom Anwendungsbereich des Gesetzentwurfs für ein IT-Sicherheitsgesetz auszunehmen.

Bereits heute sind anonyme und freiwillige Meldungen an das BSI möglich. Es liegen uns aus den reihen unserer Mitgliedschaft keine konkreten Anhaltspunkte dafür vor, dass sich das bisherige System der anonymen und freiwilligen Meldungen nicht bewährt hat.

Wir möchten Sie bitten, unsere Anmerkungen im weiteren Gesetzgebungsverfahren zu berücksichtigen.

Mit freundlichen Grüßen

Lutz Könner
Geschäftsführer

Association of German Seaport Operators

ZDS - Zentralverband der deutschen Seehafenbetriebe e. V.
Am Sandtorkai 2, 20457 Hamburg
Tel.-Nr.: 040.366203/04, Fax-Nr.: 040.366377
Email: info@zds-seehaefen.de, Internet: www.zds-seehaefen.de
Hauptgeschäftsführer: Daniel Hosseus, Geschäftsführer: Lutz Könner, Präsident: Klaus-Dieter Peters, Vizepräsident: Dr. Ulfbenno Krüger, Präsidiumsmitglieder: Frank Dreeke, Sören Jurrat, Jan Müller.
Vereinsregister-Nr.: 6833