Verband der TÜV e.V.
Präsidium

Friedrichstraße 136
10117 Berlin
Deutschland
Tel. +49 30 760095-400
Fax +49 30 760095-401

berlin@vdtuev.de
www.vdtuev.de

TÜV®

VdTÜV | Friedrichstraße 136 | 10117 Berlin | Deutschland

An den Vorsitzenden des
Innenausschusses des Deutschen Bundestags
Herrn Wolfgang Bosbach MdB

per E-Mail: innenausschuss@bundestag.de

Datum
09.04.2015

VdTÜV-Stellungnahme zum Gesetzesentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) BT-Drucksache 18/4096

Sehr geehrter Herr Vorsitzender,

der VdTÜV begrüßt die im IT-Sicherheitsgesetz vorgeschlagenen Rechtsänderungen, mit denen eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland erreicht werden soll. Wir schlagen jedoch vor, bei der Novellierung des BSI-Gesetzes in Artikel 1 des Gesetzesentwurfs den präventiven Schutz gegen IT-Angriffe und die notwendige Vertrauensinfrastruktur zu stärken.

Aus unserer Sicht findet die notwendige Unabhängigkeit der Stellen, die Sicherheitsaudits, Prüfungen und Zertifizierungen vornehmen können, keine ausreichende Berücksichtigung. Gerade unabhängige IT-Sicherheitsüberprüfungen vermitteln jedoch glaubhaft, dass neue und intelligente Technologien auch sicher und vertrauenswürdig sind, und so diese die nötige Akzeptanz in der Bevölkerung finden. IT-Sicherheit und Vertrauen in kritische Infrastrukturen sind entscheidende Faktoren für die digitale Entwicklung von Wirtschaft und Gesellschaft. Das IT-Sicherheitsgesetz sollte die Chance nutzen, zu einem echten Standortvorteil für Deutschland zu werden. Dabei verweisen wir auf die Ergebnisse der Enquete Kommission des Deutschen Bundestags „Internet und digitale Gesellschaft", und angesichts der Internationalität des Gesetzesentwurfs auf laufende europäischen Gesetzesinitiativen (NIS-Richtlinie) und internationale Standards (z. Bsp. Cybersecurity Framework in den USA), die u.a. für IT-Sicherheitsüberprüfungen kritischer Infrastrukturen unabhängige, qualifizierte Stellen empfohlen haben.

Wir vertreten die Auffassung, dass IT-Sicherheitsvorfälle grundsätzlich einer pseudonymisierten Meldung über eine branchenspezifische Ansprechstelle unterliegen sollen. Im Fall eines Ausfalls oder einer erheblichen Störung der Kritischen Infrastruktur muss die Meldung namentlich erfolgen. Der Gesetzgeber sollte allerdings zeitnah, unter Abwägung der Interessen der Wirtschaft und des Sicherheitsbedürfnisses der Bevölkerung bzw. Dritter, über den Verordnungsweg konkreter definieren, wann „erhebliche Störungen" vorliegen und auch welche Mindestanforderungen letztlich eine entsprechende Ansprechstelle erfüllen muss.

Wir möchten Sie bitten, unsere Ausführungen in Ihren weiteren Beratungen zu berücksichtigen. Für Erläuterungen und Rückfragen stehen wir jederzeit gern zur Verfügung.

Mit freundlichem Gruß

Dr. Klaus Brüggemann
Geschäftsführendes Präsidiumsmitglied

Im Einzelnen:

I. Zu Artikel 1 Änderung des BSI-Gesetzes § 7a *Untersuchung der Sicherheit in der Informationstechnik*

Eine international akzeptierte Qualitäts- und Sicherheitsinfrastruktur ist Kernaufgabe deutscher Wirtschafts- und Industriepolitik. Bei umfassenden Untersuchungen von IT-Produkten,- Systemen und –Diensten müssen vom BSI beauftragte Dritte ihre notwendige Unabhängigkeit nachweisen können, denn die Übertragung von Prüfkompetenz auf „Dritte" setzt voraus, dass diese „Dritten" über das entsprechende Know-How verfügen, qualifiziert zu prüfen. Zur Wahrung von Geschäftsgeheimnissen, Vertraulichkeit und grundsätzlichen Unternehmensinteressen dürfen „Dritte" weder an der Entwicklung, Herstellung, Lieferung, Reparatur oder Wartung des zu bewertenden Gegenstands beteiligt sein. Diese notwendige Unabhängigkeit des beauftragten Dritten vom Betreiber bzw. Hersteller oder Anbieter stärkt zudem die Glaubwürdigkeit der Untersuchung und schafft Vertrauen in die IT-Produkte,- Systeme und -Dienste. Vom BSI beauftragte Dritte müssen zudem ihre fachliche Qualifikation für die Untersuchung von IT-Produkten,- Systemen und Diensten gegenüber der nationalen Sicherheitsbehörde nachweisen. Der Gesetzgeber schafft mit der Beauftragung qualifizierter unabhängiger Dritter ausreichend Prüf- und Begutachtungsressourcen für eine beschleunigte und kompetente Untersuchung von IT-Produkten,- Systemen und –Diensten in Deutschland.

Für eine entsprechende Konkretisierung sollte § 7a (1) auf Seite 10 des IT-Sicherheitsgesetzes wie folgt ergänzt werden (kursiv):

„Das Bundesamt darf zur Erfüllung seiner Aufgaben auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich hierbei der Unterstützung *qualifizierter unabhängiger* Dritter bedienen, [...]."

II. Zu Artikel 1 Änderung des BSI-Gesetzes § 8a *Sicherheit in der Informationstechnik Kritischer Infrastrukturen*

Für Audits, Prüfungen oder Zertifizierungen im Bereich der Informationstechnik Kritischer Infrastrukturen müssen konkrete Anforderungen festgelegt und transparente Regeln aufgestellt werden. In der Begründung zu § 8a Abs. 3 wird unterstrichen, dass die Bundesregierung Auditoren für qualifiziert hält, wenn sie ihre Qualifikation und Kompetenz gegenüber dem BSI formal glaubhaft machen können. Der VdTÜV begrüßt diese Entscheidung: Für Betreiber Kritischer Infrastrukturen ist es essentiell, das Sicherheitsniveau von IT-Lösungen, -Komponenten und -Prozessen kontinuierlich zu überprüfen, sowie u. a. auch das Informationssicherheits-Management-System (ISMS) auf geeignete Weise durch ein Audit, eine Prüfung oder Zertifizierung durch eine qualifizierte Stelle zu optimieren. Zu den Vorteilen eines professionellen Informationssicherheits-Management-Systems zählt insbesondere die wirksame Kontrolle von IT-Risiken durch ein systematisches Risiko-Management. Somit können Schwachstellen aufgedeckt, Risiken sowie potenzielle Schäden und Folgekosten minimiert werden. Nach unserer Auffassung muss dabei vor allem die Unabhängigkeit der Ausgabestelle des Audits, Prüfberichts oder Zertifikats sichergestellt werden. Bei internen Audits, Prüfungen oder Zertifizierungen durch den Betreiber steigt grundsätzlich das Risiko von reinen Routineprüfungen oder auch der ungewollten Beeinflussung, wodurch die Effizienz und Aussagekraft des Audits, der Prüfung oder Zertifizierung geschwächt wird. Unabhängige Prüfungen entlasten Unternehmen eigene Prüfkompetenzen aufbauen zu müssen, zudem erzielen unabhängige, qualifizierte Prüfungen entscheidende Impulse und Anstöße zu einer wirksamen Verbesserung der Betreiber- oder Unternehmens IT-Sicherheitsarchitektur.

Es ist daher wichtig, dass bereits das BSI-Gesetz einen eindeutigen Hinweis auf die notwendige Unabhängigkeit und Qualifikation der Prüfer bzw. Zertifizierer enthält.

Für eine entsprechende Festlegung auf den Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen sollte § 8a (3) auf Seite 11 des IT-Sicherheitsgesetzes wie folgt geändert werden:

„Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen *einer qualifizierten unabhängigen Stelle* erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen."

III. Zu Artikel 1 Änderung des BSI-Gesetzes § 8b *Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen*

Der VdTÜV begrüßt die Pläne zur Einführung einer Meldepflicht von Störungen bei informationstechnischen Systemen, Komponenten oder Prozessen für Betreiber Kritischer Infrastrukturen an das BSI. Diese Regelung muss für alle Kritischen Infrastrukturbetreiber gleichermaßen gelten. Das BSI wird durch die Meldepflicht, entsprechend seiner Aufgabe, in die Lage versetzt, eine Verbesserung des Lagebilds zur IT-Sicherheit zu erreichen. Schwerwiegende Beeinträchtigungen informationstechnischer Systeme, Komponenten oder Prozesse sollten über eine unabhängige Ansprechstelle an die nationale Sicherheitsbehörde gemeldet werden. Hierzu bedarf es noch einer Präzisierung des Rechtsbegriffs „erhebliche Störung", wie in § 8b (4) Satz 1 BSI Gesetz eingeführt, sowie welche Mindestanforderungen eine entsprechende Ansprechstelle erfüllen muss

Grundsätzlich sollte die Meldung in pseudonymisierter Form gefasst sein. Zur Erstellung eines Lagebilds durch das BSI ist die verpflichtende Offenlegung der Identität des meldenden Betreibers nicht zwingend erforderlich. Einerseits wird so das Risiko von Reputationsschäden für das meldende Unternehmen minimiert. Andererseits bleibt dem BSI hierdurch die Möglichkeit, ein uneingeschränktes Lagebild zu erstellen, um mögliche Gegenmaßnahmen zum Schutz anderer Unternehmen bzw. Betreiber Kritischer Infrastrukturen einzuleiten. Gleichzeitig kann ein neutraler Rückkanal von der Sicherheitsbehörde über die benannte Ansprechstelle an das Unternehmen implementiert werden, um aktuelle Informationen über Angriffe von der Behörde zu erhalten. Durch diesen entsprechenden nachvollziehbaren und auditierbaren Übermittlungsprozess in pseudonymisierter Form bleibt der Betreiber der Kritischen Infrastruktur für die Behörde identifizierbar. (§ 8b (4) BSI-Gesetz, S. 12 IT-Sicherheitsgesetz)

Zudem sollte in Anlehnung an das Bundesdatenschutzgesetz (§3 (6a)) in § 8b (5) Satz 2 auf Seite 12 der entsprechende Informationsaustausch zwischen den Kontaktstellen und dem BSI wie folgt konkretisiert bzw. geändert werden:

„Wurde eine solche benannt, erfolgt ~~der~~ *ein pseudonymisierter* Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt über die gemeinsame Ansprechstelle."

IV. Zu B. Lösung S. 3 des IT-Sicherheitsgesetzes – europarechtliche Implikationen

Entsprechend der Stellungnahme des nationalen Normenkontrollrates in Anlage 2 auf Seite 41 der BT-Drucksache 18/4096, gilt es im Hinblick auf die parallel zu diesem Gesetzgebungsverfahren laufenden europäischen Verhandlungen über die NIS-Richtlinie, ein Auseinanderfallen der Regelungen zu vermeiden, da eventuelle spätere Änderungen infolge der Richtlinie zu unnötigem Mehraufwand bei den Adressaten führen würden.

Die Bundesregierung weist selbst auf Seite 3 des Gesetzesentwurfs darauf hin, dass auch auf europäischer Gesetzgebungsebene das Thema IT-Sicherheit behandelt wird, insbesondere in dem von der Europäischen Kommission entwickelten Vorschlag für eine „Richtlinie des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union". Deutlicher als im deutschen Gesetzesentwurf soll hier allerdings die Prüfung der Sicherheit von Netz- und Informationssystemen in Art. 15 Absatz 2b der vorgeschlagenen EU-Richtlinie durch u. a. qualifizierte unabhängige Stellen erfolgen. Dieser Aspekt ist im deutschen Gesetzesentwurf derzeit, wie oben genannt, schwächer formuliert. An dieser Stelle könnte eine Orientierung an der europäischen Richtlinie für Informationssicherheit vorteilhaft sein, um die Aussagekraft und Belastbarkeit der Sicherheitsüberprüfungen zu erhöhen. Unabhängige Stellen unterstreichen die Zuverlässigkeit, Glaubwürdigkeit und das Vertrauen in die Sicherheitsüberprüfungen.

Zudem hat der Deutsche Bundestag bereits 2013 im Neunten Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft", wie der europäische Gesetzgeber, in Drucksache 17/12541 die Position erlangt, dass für besonders schutzbedürftige Bereiche eine gesetzliche Pflicht zu einer unabhängigen Sicherheitsüberprüfung und zugleich Zertifizierungen notwendig erscheint. Aus unserer Sicht sollte diese Erkenntnis in der weiteren parlamentarischen Behandlung des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme berücksichtigt werden.