STELLUNGNAHME

Berlin, 17. April 2015

Deutscher Industrie- und Handelskammertag

Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Die Bundesregierung hat dem Deutschen Bundestag den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme zugeleitet. Mit dem geplanten IT-Sicherheitsgesetz sollen in erster Linie die Betreiber kritischer Infrastrukturen dazu verpflichtet werden, ihre IT-Systeme gegen Angriffe abzusichern. Darüber hinaus soll die Zusammenarbeit zwischen Sicherheitsbehörden und Betreibern kritischer Infrastrukturen verbessert werden. Die IHK-Organisation setzt sich intensiv für eine Verbesserung der Widerstandsfähigkeit der deutschen Wirtschaft gegenüber der Vielzahl von Bedrohungen im Cyberraum ein und nimmt die Gelegenheit wahr, zum o. g. Entwurf Stellung zu nehmen.

Dieses IT-Sicherheitsgesetz sollte – seinem ursprünglichen Anlass entsprechend – sich auf die volkswirtschaftlich wichtigen Infrastrukturen konzentrieren, d. h. die Betreiber kritischer Infrastrukturen im engeren Sinne adressieren und in diesem Bereich verlässliche Regelungen schaffen, die die IT-Sicherheit wirklich verbessern. Eine solche Fokussierung ist unserer Ansicht nach auch wichtig, um die Diskussion und die anschließende Umsetzung nicht zu überfrachten. Darüber hinaus gehende Maßnahmen – jenseits des Gesetzes – im Sinne einer Ende zu Ende-Sicherheit vom Hersteller bis zum Nutzer sollten in einem breiten Diskussionsprozess aller Beteiligten erarbeitet werden, der auch die genaue Rollen- und Aufgabenverteilung zwischen Staat, Wirtschaft und dem einzelnen Nutzer umfasst.

Das gesetzgeberische Ziel muss sich in der Umsetzung widerspiegeln. An einigen Stellen des Gesetzentwurfes bestehen jedoch Lücken (z. B. bei der Definition der Leistungen des BSI gegenüber den meldepflichtigen Unternehmen in Form von Service Level Agreements für Warnhinweise an Betreiber kritischer Infrastrukturen oder bei der Erstellung eines Lageberichts auf der Basis relativ weniger erwarteter Meldungen), an anderen Stellen wird dagegen über das Ziel hinausgeschossen (z. B. mit unverhältnismäßigen Verpflichtungen auch für kleine Webseitenbetreiber).

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Im Einzelnen:

Fokussierung auf kritische Infrastrukturen

In der Tat müssen die IT-Netze und -Systeme sicherer gemacht werden, denn die Zahl von Netzstörungen, Internetangriffen und sicherheitsrelevanten Zwischenfällen ist erheblich gestiegen. Dabei gehen wir davon aus, dass Unternehmen grundsätzlich für die Sicherheit ihrer Systeme selbst verantwortlich sind. Viele freiwillige Initiativen – auch der IHK-Organisation – setzen richtiger Weise hier an und stärken die Sensibilität dafür. Besonderes Augenmerk verlangt der Bereich der sog. kritischen Infrastrukturen, denn von Schäden in diesem Bereich geht immer zugleich auch ein Risiko für andere Unternehmen und das Gemeinwesen aus. Gesetzliche Verpflichtungen zu Sicherheitsmaßnahmen, so auch der vorliegende Gesetzentwurf, sollten sich auf diesen Bereich konzentrieren. Die Betreiber dieser Infrastrukturen haben eine besondere Verantwortung für die Funktionsfähigkeit unserer Volkswirtschaft. Insofern begrüßen wir das grundsätzliche Anliegen, mit dem IT-Sicherheitsgesetz die kritischen Infrastrukturen sicherer zu machen und den Austausch zu Sicherheitsvorfällen und die Reaktionsfähigkeit von Staat und Wirtschaft in diesem speziellen Bereich zu verbessern. Ziel des Gesetzes sollte unserer Ansicht nach sein, bei Betreibern kritischer Infrastrukturen ein Informations-Sicherheitsmanagementsystem einzuführen und den Austausch zu Sicherheitsvorfällen effektiv zu gestalten. Auf diesen Ansatz sollte sich die gesetzliche Regelung konzentrieren.

Im neuen Entwurf des § 7a BSIG-E fehlt jeglicher Bezug zu den Betreibern Kritischer Infrastrukturen – also dem wesentlichen Regelungsgegenstand des Gesetzes. Vielmehr wird das BSI hier mit einer Generalklausel artigen, anlassunabhängigen Marktbeobachtungsfunktion ausgestattet, die bisher nicht zu seinen Aufgaben gehört. Wir erwarten, dass Anlass, Ablauf, Zweckbestimmung, Grenzen und die Modalitäten zur Informationsweitergabe klar umrissen werden.

Um den Schutz wichtiger Einrichtungen des Gemeinwesens zu gewährleisten, ist es sinnvoll, IT-Sicherheitsstandards für kritische Infrastrukturen zu etablieren (§ 8a BSIG-E). Eine gesetzliche Grundlage bedeutet für die betroffenen Unternehmen auch Rechtssicherheit und damit die Chance, zukunftssicher zu planen.

Mehr Rechtssicherheit durch klarere Begriffsbestimmungen

Zu mehr Rechts- und Planungssicherheit würde eine klare Definition der zahlreichen unbestimmten Rechtsbegriffe beitragen. Wir sehen das Problem, dass dies insbesondere in einem Bereich, der sich durch schnelle technologische Veränderungen auszeichnet, nicht einfach zu operationalisieren

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

ist. Wir regen allerdings an, die unbestimmten Rechtsbegriffe auf das allernotwendigste Maß zu beschränken und erwarten zumindes bei den folgenden Begriffen Präzisierungen: die Definition kritische Infrastrukturen und eine Konkretisierung des Begriffs Versorgungsengpässe (§ 2 Absatz 10 BSIG-E), eine Definition der Meldeschwelle für Telekommunikationsunternehmen bei auftretenden beträchtlichen Sicherheitsverletzungen (§ 109 Absatz 5 TKG-E), eine Präzisierung des Begriffs Stand der Technik (§ 8a Absatz 1 Satz 2 BSIG-E) und bei der Definition einer erheblichen Störung.

Anwendungsbereich klar regeln

Die erste grobe Liste zu den möglicherweise betroffenen Unternehmen im Gesetzentwurf erschwert nicht nur eine Beurteilung der Angemessenheit der Verpflichtungen, sondern auch des Beitrags der Vorgaben zur Verbesserung der IT-Sicherheitslage. Die betreffende Rechtsverordnung zum Anwendungsbereich des Gesetzes sollte zeitnah, möglichst schon parallel zum Gesetzgebungsverfahren erarbeitet werden. Mit den dann verfügbaren Informationen würde die tatsächliche Betroffenheit im Vorfeld viel transparenter werden. Das könnte auch die Akzeptanz in der Wirtschaft verbessern.

Wir empfehlen, den Anwendungsbereich des Gesetzes möglichst restriktiv zu fassen. In einer digital vernetzten Volkswirtschaft kommt der Funktionsfähigkeit der zugrunde liegenden Infrastrukturen eine wesentliche Bedeutung zu. In der Rechtsverordnung muss genau dieser Bereich klar abgegrenzt werden. Dazu gehört auch eine Einbeziehung kritischer Bereiche des öffentlichen Sektors, die ebenfalls Infrastrukturcharakter haben. Die Nicht-Einbeziehung kritischer Infrastrukturen der öffentlichen Hand ist nicht nachvollziehbar.

Zweifel an Verhältnis von Aufwand und Nutzen der vorgesehenen Meldepflicht

Verständlicher Weise sind Unternehmen sehr zurückhaltend mit der Meldung erlittener Angriffe. Der DIHK hat im Oktober 2014 Unternehmen aus den in den Erläuterungen des Gesetzentwurfs genannten Branchen zur (in erster Linie freiwilligen) Zusammenarbeit mit Sicherheitsbehörden befragt. Ein Großteil dieser Unternehmen wäre demnach bereit, Sicherheitsvorfälle zu melden – unter bestimmten Voraussetzungen:

1. die absolute Vertraulichkeit der Information muss gewährleistet sein, die Meldungen müssen anonymisiert abgegeben werden können,
2. die Unternehmen erwarten einen Mehrwert von der Zusammenarbeit, z. B. als konkrete Warnhinweise,

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

3. wenn eine gesetzliche Meldepflicht eingeführt wird, muss verbindlich festgelegt sein, dass nur wirklich schwerwiegende Fälle gemeldet werden müssen und
4. der Aufwand für die Meldungen muss sich in Grenzen halten.

Vor diesem Hintergrund bitten wir, im weiteren Gesetzgebungsverfahren folgende Aspekte zu berücksichtigen:

Wir erkennen ausdrücklich an, dass der Entwurf eine unserer zentralen Forderungen aufgreift und zumindest pseudonymisierte Meldungen von Sicherheitsvorfällen vorsieht, die zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastrukturen führen können. Das ist ein wichtiger Beitrag zur Steigerung der Akzeptanz des Gesetzentwurfes in der Wirtschaft. Richtig ist, dass für einfache und unkomplizierte Meldewege die bereits mit dem UP KRITIS etablierten Ansprechstellen genutzt werden können. Es gibt aber keinen sachlichen Grund, die Möglichkeit anonymer Meldungen nur einigen Adressaten des neuen Gesetzes einzuräumen. Wir schlagen stattdessen vor, die Frage der anonymen Meldemöglichkeit für alle Anbieter einheitlich zu regeln.

Ein wesentlicher Beitrag für eine funktionierende Zusammenarbeit zwischen Unternehmen und Behörden besteht darüber hinaus darin, eine Basis für den vertrauensvollen Austausch zu Sicherheitslücken und -schwachstellen herzustellen – diese wird von den Unternehmen grundsätzlich als wünschenswert erachtet. Ein sinnvoller Ansatz wäre, bestehende Initiativen – wie die Allianz für Cybersicherheit – auszubauen und stärker bei den Unternehmen bekannt zu machen. Die IHK-Organisation sieht sich hier auch selbst in der Pflicht.

Die gesetzlich vorgeschriebenen Meldungen führen zu erheblichen Aufwänden bei den Unternehmen – bei nicht einschätzbarem Nutzen. Diese müssten vor einer Meldung mögliche Konsequenzen für das Unternehmen prüfen. Börsennotierte Unternehmen müssen zudem überlegen, ob eine Meldung über einen IT-Sicherheitsvorfall börsenrelevant sein könnte. Dann wären sie verpflichtet, ihre Aktionäre zu warnen. Bis diese Fragen geklärt sind, dürfte es für eine Warnung anderer Unternehmen oft zu spät sein. Eventuell auftretende Haftungsfragen müssen geklärt werden (Abgleich mit Aktien- und Versicherungsrecht), wenn Unternehmen etwa dadurch geschädigt werden, dass z. B. Informationen zu einem Sicherheitsvorfall öffentlich werden, die sich schlimmstenfalls sogar im Nachhinein als falsch herausstellen.

Genauer definiert werden sollte in §§ 4 und 7 BSIG-E die Leistung, die vom BSI an die Unternehmen zurückgegeben wird. Diese ist – im Verhältnis zu den umfangreichen Verpflichtungen für die Betreiber kritischer Infrastrukturen – kaum umschrieben.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Pflichten für Telekommunikationsanbieter zu weitgehend

§ 109a Abs. 4 TKG führt neue Benachrichtigungspflichten für Telekommunikations-Diensteanbieter gegenüber Nutzern ein, wenn Störungen bekannt werden, die von dessen Datenverarbeitungssystemen ausgehen. Störungen entstehen aber in erster Linie in den vorgelagerten Systemen, z. B. beim Internetanbieter, Cloudanbieter oder auf Internetplattformen. Die Information der Nutzer sollte in erster Linie vom Störer selbst und nicht über Dritte (also Telekommunikations-Diensteanbieter) erfolgen. Die hier vorgesehene Vorgehensweise würde unter Umständen wertvolle Zeit kosten und birgt zudem das Risiko von (Übertragungs-)Fehlern bei der Information der Betroffenen.

Unabhängig davon ist die Pflicht zur Information nicht hinreichend konkret gefasst. Nach der Entwurfsfassung ist jedwede Art von Störung zu melden, unabhängig davon, wie viele Nutzer sie betrifft und welche Auswirkungen und Schäden sie zur Folge haben kann. Danach wäre bereits jede auf einen Nutzer beschränkte mit geringem Schadenpotenzial versehene Störung meldepflichtig. Die Regelung ist zu weit gefasst und die daraus folgenden Verpflichtungen in zahlreichen Anwendungsfällen nicht erforderlich und unangemessen.

Problematisch ist auch, dass TK-Diensteanbieter bei fehlerhaften oder verspäteten Informationen einem Haftungsrisiko ausgesetzt sind (§§ 44 und 44a TKG). Dies erscheint unbillig, weil Störungen häufig gerade nicht in eigenen Systemen und Anwendungen des informierenden TK-Dienste-anbieters auftreten. Hier bedarf es einer Haftungsfreistellung des benachrichtigenden TK-Dienste-anbieters, der nicht selbst Störer im Rechtssinne ist.

Künftige Rolle des BSI klarer definieren

Die Bundesregierung sollte sich auf Maßnahmen konzentrieren, die den Unternehmen wirklich helfen. In einer ‚Wirtschaft 4.0' kommt der Sicherheit informationstechnischer Systeme eine essentielle Bedeutung für die Funktions- und Wettbewerbsfähigkeit der Unternehmen zu. Vor diesem Hintergrund begrüßen wir die vorgesehene Stärkung des BSI als zentrale Behörde zur Bündelung und Auswertung von Informationen zur Cybersicherheit in Deutschland. Dies zeigt, dass die Bundesregierung sich ihrer Verantwortung insbes. beim Schutz kritischer Infrastrukturen bewusst ist.

Wesentlich aus unserer Sicht sind:

- ein vertrauensvoller Informations- und Erfahrungsaustausch zwischen BSI und Unternehmen/Branchenverbänden/CERTs etc., insbesondere bei schwerwiegenden Sicherheitsvorfällen,

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

- ein einheitliches Bewertungsschema für Sicherheitsvorfälle (Kritikalität, Impact etc.),
- die Definition abgestimmter Reaktionsprozesse von Unternehmen und Behörden bei übergreifenden Sicherheitsvorfällen sowie
- eine aktuelle, transparente und aussagekräftige Beschreibung der aktuellen Sicherheits- bzw. Bedrohungslage.

Die künftige Rolle des BSI und das Zusammenspiel mit den Unternehmen sollten in einem Diskussionsprozess von Staat und Wirtschaft gemeinsam definiert werden. Ein gemeinsames Verständnis über die Rollenverteilung und das konkrete Zusammenspiel von Unternehmen und BSI ist wesentliche Grundlage für die Bereitschaft der Unternehmen zur Zusammenarbeit mit dem BSI.

Nach Implementierung des Gesetzes branchenspezifische Ansatz organisatorisch und prozessual weiter ausdifferenziert werden – insbesondere in Bezug auf das Zusammenspiel zwischen Unternehmen, Verbänden und dem BSI. Unserem Verständnis nach sollten operative Tätigkeiten bei der Prävention und der Schadensbeseitigung von den Unternehmen selbst erbracht werden. Deutsche IT-Sicherheitsanbieter verfügen über entsprechende Kompetenzen und eine ausreichende Anzahl von Experten. Der Austausch zu Sicherheitsvorfällen kann innerhalb von Branchen über Verbandsstrukturen schnell und effektiv organisiert werden. Die Verbände sollten in engem Austausch mit dem BSI stehen, das als Vernetzungsstelle agiert, die Meldungen über die Branchenverbände empfängt, die Betroffenheit weiterer Branchen prüft und diese informiert. Das BSI könnte darüber hinaus Methoden zur Überprüfung der IT-Sicherheit technischer Systeme, Komponenten und Prozesse zur Verfügung stellen, ein Gesamtlagebild erstellen und Warnhinweise in die Fläche bringen.

Darüber hinaus muss organisatorisch sichergestellt sein, dass unternehmensrelevante Informationen nicht in falsche Hände geraten. Der Umgang mit den Daten aus den eingehenden Meldungen beim BSI muss transparent und nachvollziehbar gestaltet und an den Zweck des Gesetzes gebunden sein. Vor diesem Hintergrund sollte die Unabhängigkeit des BSI gestärkt werden.

Keine unangemessenen Verpflichtungen für Webseitenbetreiber

Vor dem Hintergrund, dass sich die gesetzlichen Vorgaben auf den Bereich der kritischen Infrastrukturen konzentrieren sollten, fordern wir den Deutschen Bundestag auf, die geplante Änderung des Telemediengesetzes aus dem Gesetzentwurf zu streichen. Wir erkennen an, dass eine Verbesserung der IT-Sicherheit in diesem Bereich erstrebenswert ist, allerdings passen die Vorgaben für Anbieter von Telemediendiensten nicht in die Gesetzessystematik und schießen

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

darüber hinaus weit über das Ziel hinaus – sowohl was den Adressatenkreis betrifft (schon jeder kleine Verein oder eine Privatperson, die Werbebanner auf der Webseite hat), als auch in Bezug auf die Reichweite der Verpflichtung: Anbieter von Telemediendiensten sollen verpflichtet werden „sicherzustellen, dass kein unerlaubter Zugriff auf ihre Telekommunikations- und Datenverarbeitungssysteme möglich ist“. Eine solche umfassende Sicherheitsgarantie ist kaum zu erfüllen und unverhältnismäßig. Hinzu kommt, dass die unangemessene Verpflichtung auch noch mit einer Bußgeldandrohung versehen ist. Wir gehen davon aus, dass dies nicht im Sinne des Gesetzgebers sein kann.

Grundsätzlich stellt sich die Frage, ob mit der „Update-Pflicht“ für Webseiten überhaupt eine relevante Schutzwirkung für die Allgemeinheit erzeugt werden kann. Infizierte Webseiten sind lediglich ein Teilbereich einer längeren Kette von potenziellen Software-Schwachstellen. Ihre tatsächlich schädigende Wirkung hängt von weiteren Faktoren ab. Zu einem Großteil erfolgt die Infektion von Rechnern durch mangelnde Software-Aktualität beim Nutzer und nur zum Teil durch deutsche Telemediendienste. Schließlich stellt sich die Frage, ob nicht die Mehrzahl der infizierten Webseiten von ausländischen Servern abgerufen und damit nicht von der Verpflichtung nach dem TMG erfasst wird.

Kein nationaler Alleingang

Notwendig ist ein abgestimmtes Vorgehen zwischen nationaler Gesetzgebung und der europäischen Legislativinitiative zur Netz- und Informationssicherheit (NIS-Richtlinie) – insbesondere im Hinblick auf Zielsetzung und Anwendungsbereich. Es darf nicht zu Wettbewerbsverzerrungen aufgrund unterschiedlicher nationaler Regelungen in der EU kommen, die – wenn sie erst einmal eingeführt sind – schwer wieder auf ein einheitliches Niveau gebracht werden können.

Überprüfung der Zielerreichung des Gesetzes richtig

Wir begrüßen ausdrücklich die vorgesehene Evaluierung nach Inkrafttreten der Rechtsverordnung, insbesondere im Hinblick auf die Erfassung der relevanten Branchen/Unternehmen und im Hinblick auf die Effizienz der Meldepflicht.

Übergangsfristen angemessen gestalten

Die vorgesehenen 2 Jahre Übergangsfrist zur Umsetzung der geforderten Mindeststandards nach Inkrafttreten des Gesetzes sind viel zu kurz. Die potenziell betroffenen Unternehmen rechnen damit,

dass der größte Teil dieses Zeitraums für die Ausgestaltung der jeweiligen branchenspezifischen Mindeststandards und die Zulassung durch das BSI erforderlich ist. Damit bleibt den Unternehmen zu wenig Zeit für eine angemessene Umsetzung. Wir empfehlen daher eine Verlängerung der Übergangsfrist. Diese sollte erst dann beginnen, wenn die Mindeststandards festgelegt und vom BSI freigegeben sind. Gleiches gilt für die vorgesehene Frist von 2 Jahren zur ersten Erfüllung der geforderten Nachweispflichten.

Ansprechpartnerin im DIHK:
Dr. Katrin Sobania, Tel. 030 20308-2109, sobania.katrin@dihk.de