POSITION STATEMENT

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

Gesetzentwurf der Bundesregierung

Stellungnahme des Telecommunications, Internet, and Media (TIM) Committee der American Chamber of Commerce in Germany e.V.

5. Mai 2015

Hintergrund

Der Deutsche Bundestag beabsichtigt die Verabschiedung eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (sog. IT-Sicherheitsgesetz). Die in der Amerikanischen Handelskammer in Deutschland (AmCham Germany) vertretenen Unternehmen begrüßen grundsätzlich die Bemühungen von Politik und Verwaltung, ein für Deutschland hohes Niveau an IT-Sicherheit zu verwirklichen. So investieren die Mitglieder von AmCham Germany bereits seit Jahren große sachliche und personelle Ressourcen in die Erhöhung der Sicherheit ihrer Produkte und Dienste und befinden sich dazu auch in regelmäßigem Austausch mit Behörden in Deutschland, Europa und darüber hinaus. Zudem tragen zahlreiche namhafte Mitgliedsunternehmen heute schon für ein hohes Maß an Zuverlässigkeit, Sicherheit und Transparenz ihrer Produkte und Dienste bei und stellen damit eine verlässliche technologische Grundlage für das Funktionieren von Staat, Verwaltung und Wirtschaft in Deutschland und darüber hinaus dar.

Das auch aus Sicht von AmCham Germany grundsätzlich begrüßenswerte Ansinnen der Bundesregierung wäre mit Blick auf den beabsichtigten Gesetzeszwecke vorzugsweise in der gegenwärtig in Planung befindlichen europäischen Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (sog. NIS-Richtlinie) am besten aufgehoben. Denn die IT-Sicherheit wie die IKT insgesamt macht bekanntlich an geografischen, nationalen Grenzen nicht halt. Wenn der Deutsche Bundestag allerdings im Vorgriff auf die NIS-Richtlinie national tätig werden will, dann bedarf der Kabinettsentwurf zum IT-Sicherheitsgesetz grundlegender Überarbeitung. In diesem Zusammenhang wird auch auf die Stellungnahme des Bundesrates vom 27.1.2015 verwiesen.

I. Executive Summary

1. Reichweite des Gesetzes klar festlegen:
Die Reichweite des IT-Sicherheitsgesetzes muss bereits im Gesetz selbst und nicht in einer nachgelagerten Rechtsverordnung bestimmt werden.

2. Klarer Fokus auf kritische Infrastrukturen:[1]
Um höchstmögliche Sicherheit zu gewährleisten, ist es von entscheidender Bedeutung, dass alle Betreiber kritischer Infrastrukturen, unabhängig davon ob sie sich in privater oder öffentlicher Hand befinden, von dem Gesetz erfasst werden.

3. Engere Definition eines meldepflichtigen Vorfalls:
Es muss hinreichend klar definiert sein, dass nur solche Vorfälle meldepflichtig sind, die reale Bedrohungen darstellen und/oder tatsächliche Schäden verursachen.

4. Standards müssen sich an internationalen Regelwerken orientieren:
Die sektorspezifischen Standards sollten sich eng an den anerkannten internationalen Standards und Best Practices anlehnen – sowohl bei der IT-Sicherheit wie auch beim Schutz der kritischen Infrastrukturen.

5. Keine Erweiterung der Meldepflichten für TK-Unternehmen:
Die Erweiterung des die Meldepflicht auslösenden Tatbestands auf sämtliche Beeinträchtigungen bei TK-Unternehmen verursacht unverhältnismäßigen Mehraufwand für alle Beteiligten und ist abzulehnen.

6. Sicherheitsauflagen in Telemedien müssen angemessen bleiben:
Benötigt wird eine deutlich eingeschränktere Mittel-Zweck-Relation sowie eine präzisere Definition der Sicherheitsauflagen für Telemedien.

7. Prüfkompetenzen des BSI müssen präzisiert werden:
Der Gesetzesentwurf muss in Hinblick auf Produkt-Bewertungen durch das BSI enger gefasst werden. Das Bewertungsverfahren des BSI für ICT-Produkte, -systeme und -dienstleistungen sollte dazu so transparent wie möglich sein.

8. Produktbewertungen durch das BSI müssen klar geregelt werden:
Aufgrund potentieller Gefahren für das geistige Eigentum und die Innovationsfähigkeit der Anbieter sollten Produkte und Dienstleistungen, die noch nicht auf dem Markt sind, von der Prüfung durch das BSI ausgenommen werden bzw. sollte die Prüfung nur auf freiwilliger Basis erfolgen.

9. Öffentliche Warnungen durch das BSI nach Rücksprache mit Herstellern: Öffentliche Warnungen des BSI müssen mit den IT-Anbietern besser koordiniert werden. Darüber hinaus werden klare Kriterien für diese Warnungen benötigt.

10. Cybersicherheitspolitik muss international harmonisiert werden:
Nationale Sonderwege führen nicht zu mehr IT-Sicherheit, erhöhen den Aufwand und die Kosten und senken die Wettbewerbsfähigkeit vor allem kleiner und mittlerer Anbieter von IT-Sicherheitslösungen. Insbesondere auf europäischer Ebene bedarf es einer Harmonisierung von nationaler Gesetzgebung mit der geplanten Direktive zur Netz- und Informationssicherheit (NIS) der EU Kommission.

---

[1] *Dissenting Vote der Deutschen Telekom AG zur AmCham Germany-Position:*
Die Deutsche Telekom AG vertritt die Position, dass für eine ganzheitliche Sicherheitsbetrachtung im Cyberraum auch Hard- und Softwarehersteller ebenso wie Internetunternehmen in den Anwendungsbereich des IT-Sicherheitsgesetzes einbezogen werden und Verantwortung übernehmen müssen.

II. Anmerkungen zum Entwurf des IT-Sicherheitsgesetzes

Um die IT-Sicherheit nachhaltig zu stärken, ist eine Zusammenarbeit des öffentlichen und privaten Sektors unerlässlich. Insgesamt muss zwischen der Regulierung "von oben nach unten" und den Ansätzen "von unten nach oben" eine Balance gefunden werden, die die schnelle Taktung und die Gesamtdynamik der Informationstechnologie sowie die konstanten Veränderungen in der jeweiligen Bedrohungslandschaft berücksichtigt. Vor diesem Hintergrund kommentiert AmCham Germany den Entwurf für ein IT-Sicherheitsgesetz wie folgt:

1. Klare Definition der Reichweite des Gesetzes in Bezug auf kritische Infrastrukturen

§8a und §8b führen erhebliche Verpflichtungen für Betreiber kritischer Infrastrukturen ein. In Übereinstimmung mit §10 soll die genaue Bestimmung der Infrastrukturen, die im Sinne des Gesetzes als kritisch gelten, in einem separaten Verfahren im Zuge einer Rechtsverordnung erfolgen. Dieses Verfahren soll sowohl qualitative wie auch quantitative Aspekte berücksichtigen. Was sehr wichtig ist: Es sollen Unternehmen angehört werden, die potentiell davon betroffen sind, sowie Industrieverbände und wissenschaftliche Kreise. Die mit diesem Verfahren in Zusammenhang stehenden Akten sollen der Öffentlichkeit nicht zugänglich gemacht werden.

Hierzu werden folgende Überlegungen angeregt:

a. **Erhöhte Transparenz hinsichtlich der Reichweite dieses Gesetzes. Die Reichweite des Gesetzes sollte direkt im Gesetz selbst und nicht nachgelagert in einer Rechtsverordnung festgelegt werden. Ein solches Vorgehen würde erheblich zu Transparenz und Rechtssicherheit beitragen.** Unsicherheit ist bei langfristiger Planung ein ernsthaftes Hindernis und damit sowohl im öffentlichen als auch im privaten Sektor schädlich. AmCham Germany bevorzugt daher eine eindeutige Festlegung bezüglich der Reichweite des geplanten IT-Sicherheitsgesetzes. Dabei gäbe es zwei Hauptwege, diese Reichweite festzulegen: 1) über eine definierte Liste von Funktionen in bestimmten Sektoren und Untersektoren, die geschützt werden müssen, oder 2) über die Erstellung einer klaren Liste von Kriterien und Schwellenwerten für Kritikalität, anhand derer festgestellt werden kann, ob ein bestimmter Betreiber unter das Gesetz fällt oder nicht. Derzeit enthalten die begleitenden Erklärungen des Gesetzesentwurfs einige Informationen zu qualitativen und quantitativen Aspekten, die bei der Festlegung derjenigen kritischen Infrastrukturen, welche unter das Gesetz fallen, berücksichtigt werden sollten. AmCham Germany regt an dieser Stelle an sicherzustellen, dass diese Kriterien weiter verdeutlicht und in den Gesetzestext selbst aufgenommen werden, anstatt sie in einer Rechtsverordnung im Rahmen eines weniger transparenten Verfahrens zu verarbeiten.

b. **Fokussierung des Gesetzes auf Bedrohungen am oberen Ende des Spektrums, da nicht jede von "kritischen Infrastruktur"-Sektoren erbrachte Dienstleistung gleich kritisch ist.** Zur Fokussierung rarer Sicherheitsressourcen im öffentlichen und privaten Sektor sollte sich das Gesetz auf den Schutz vor Bedrohungen am oberen Ende des Bedrohungsspektrums konzentrieren. Insbesondere sollten diejenigen Kerndienstleistungen von kritischen Infrastrukturen im Fokus stehen, die so lebensnotwendig sind, dass durch das Lahmlegen oder Zerstören dieser Infrastrukturen die

nationale Sicherheit, die wirtschaftliche Stabilität, die öffentliche Gesundheit oder Sicherheit oder eine Kombination dieser Faktoren geschwächt würde. Die weiteren Erklärungen zum Gesetzentwurf liefern eine ähnliche Liste "qualitativer" sowie quantitativer Kriterien. In der Begleiterklärung werden die qualitativen Kriterien als solche beschrieben, welche sich auf „die Sicherheit von Leib, Leben, Gesundheit und Eigentum der Teile der Bevölkerung beziehen, die von einem Ausfall unmittelbar oder mittelbar beeinträchtigt wären." Berücksichtigt man dies, so scheinen die vorgeschlagenen Unterkategorien der Betreiber von Datenverarbeitung und -speicherung mit diesen Kriterien nicht kongruent.

c. **Einbeziehung von kritischen öffentlichen Behörden und kritischen Infrastrukturen in öffentlicher Hand.** Wenn auf Grund der obenstehend beschriebenen Kriterien exakt eingeschätzt werden kann, ob eine Infrastruktur als kritisch gilt oder nicht, sollten diese Kriterien auch für Unternehmen in öffentlicher Hand/staatlich betriebene Unternehmen angewandt werden – die in diesem Gesetzesentwurf bisher ausgenommen sind. Die Eigentumsverhältnisse (öffentliches im Gegensatz zu privatem Eigentum) sind nach Ansicht von AmCham Germany kein Maßstab für die Kritikalität einer Dienstleistung. Das Herausnehmen öffentlicher Behörden und kritischer Infrastrukturen in öffentlichem Eigentum aus dem Geltungsbereich des Gesetzes würde ein unvollständiges Bild der kritischen Infrastrukturlandschaft in Deutschland zeichnen, und dadurch auch die Erstellung eines akkuraten Überblicks über die Situation verhindern (siehe unten).

d. **Öffentlich verfügbare (handelsübliche) IT-Produkte und -Dienstleistungen sind keine kritischen Infrastrukturen.** Es ist wichtig klarzustellen, dass in Szenarien, in denen Betreiber kritischer Infrastrukturen IT-Produkte und -Dienstleistungen verwenden um ihre eigenen Dienstleistungen erbringen zu können, es diese Betreiber sind, auf welche sich die Gesetzgebung beziehen sollte und nicht die Anbieter der zugrundeliegenden IT-Produkte. Die Betreiber kritischer Infrastrukturen sollten mit Hilfe von Verträgen und Service-Level-Agreements dafür sorgen, dass die Verpflichtungen, denen sie aufgrund der geplanten Gesetzgebung unterliegen würden, ordnungsgemäß an die IT-Anbieter weitergegeben werden. Im Rahmen der vorgesehenen Meldepflicht könnte dieser Ansatz beispielsweise dabei helfen, kritische von nicht kritischen Vorfällen zu trennen. Dies würde potentielle Mehrfachmeldungen vermeiden (zuerst vom Betreiber und dann zusätzlich Meldungen von IT-Anbietern, welche Vorfälle bei Betreibern kritischer Infrastrukturen zwangsläufig unvollständig und ohne Kontext melden müssten), den zielgerichteten Einsatz von Security-Ressourcen erlauben und durch Minimierung der administrativen Belastungen die beim BSI anfallenden Kosten reduzieren.

2. Erhöhte Transparenz bei Meldepflicht & Sicherheitsstandards

Zu den in §8a und §8b eingeführten Verpflichtungen gehören verschiedene Meldepflichten für Betreiber kritischer Infrastrukturen – die unter anderem mit der Absicht erlassen werden sollen, dass das BSI aktuelle Situationsanalysen / Bedrohungseinschätzungen erstellen und aufrecht erhalten kann. AmCham Germany begrüßt die Möglichkeit, dem BSI über zu diesem Zweck benannte branchenspezifische Kontaktpunkte (single point of contact - SPOC) anonym Ereignisse melden zu können, die ansonsten durch §8b Absatz 4 abgedeckt wären.

AmCham Germany regt hierzu folgende Überlegungen an:

a. **Grundlegend ist anzumerken, dass Vorfallsmeldungen kein Selbstzweck sein sollten, sondern ein Mittel, um ein bestimmtes Ziel zu erreichen.** Allgemein gesagt ist erfolgreiches Risikomanagement von einem effektiven Informationsaustausch abhängig, wozu Pflichtmeldungen im Falle signifikanter Sicherheitsverletzungen gehören können. Es hat sich jedoch in den letzten zehn Jahren deutlich gezeigt, dass ein verpflichtender Informationsaustausch zu „Cybersicherheits-Vorfällen" zwischen der Industrie und dem Staat nur zu begrenztem Erfolg geführt hat. Die wesentliche Lehre daraus ist, dass ein Informationsaustausch dann am besten funktioniert, wenn er durch ergebnisfokussierte Fragen so zielgerichtet und präzise wie möglich ist. Darüber hinaus müssen Informationen in beide Richtungen fließen. Bedrohungen und Risiken werden am besten abgemildert, wenn die *relevanten* Parteien (d.h. die Parteien, die Informationen in praktisch umsetzbare Ergebnisse verwandeln können) alle *relevanten* Informationen austauschen. Es geht nicht darum zu gewährleisten, dass *alle* Parteien *alle* Informationen erhalten. Ein solcher zielgerichteter Austausch trägt auch zum Schutz sensitiver Informationen bei (egal ob in öffentlicher oder privater Hand), unterstützt den gesamten Datenschutz und ermöglicht einen sensiblen Informationsaustausch.

b. **Engere Definition eines "meldepflichtigen" Vorfalls.** In den zusätzlichen Erklärungen für §8a und §8b wird versucht zu definieren, was ein "meldepflichtiger" Vorfall ist. Der vorgeschlagene Ansatz ist leider erheblich weiter gefasst als es aus Sicht eines effektiven Risikomanagements sinnvoll erscheint. Die vorgeschlagenen Definitionen, nach denen "jegliche Auswirkung auf die Technologie" einen "Vorfall" darstellt, kombiniert mit der Tatsache, dass eine "schwerwiegende" Auswirkung als "eine Bedrohung der Funktionsfähigkeit der Technologie" definiert wird, bedeutet im Wesentlichen, dass jegliche Unregelmäßigkeit bei der Nutzung dieser Technologie einen meldepflichtigen Vorfall darstellen könnte. Gleiches trifft auf die Ausweitung der Meldepflichten nach § 109 Abs. 5 TKG zu (siehe hierzu Absatz II.2. f). Eine Meldepflicht mit einem derart breiten Umfang erhöht die Verwirrung, die Kosten und stellt sogar ein potentielles Sicherheitsrisiko dar. Um die Ressourcen des BSI (und die Sicherheitsressourcen eines Betreibers kritischer Infrastrukturen) effektiv zu nutzen, empfiehlt AmCham Germany, diese Definitionen erneut zu überprüfen, sie ggf. präziser zu formulieren und sich auf reale Bedrohungen und/oder tatsächliche Schäden zu beschränken.

c. **Präzisierung der Bewertung und Einschätzung der von der Industrie erhaltenen Informationen.** Insbesondere mit Blick darauf, wie die aus der Meldepflicht generierten Daten analysiert werden, schlägt AmCham Germany mehr Transparenz vor. Eventuell existierende Pläne, Informationen an diejenigen Betreiber kritischer Infrastrukturen zurück zu geben, die unter das geplante Gesetz fallen, sollten ebenfalls transparent gemacht werden. Zusätzlich sollte im Gesetzentwurf präzisiert werden, wie dieser Rückfluss von Informationen an diejenige IT-Anbieter verlaufen kann, welche zwar nicht unter das Gesetz fallen, aber zur weiteren Verbesserung ihres Cyber-Ökosystems aus möglichen Sicherheitsvorfällen lernen wollen. Zwar gibt es diesbezüglich bereits einen auf bestehenden Verträgen beruhenden regen Austausch zwischen Mitgliedsunternehmen von AmCham Germany und dem BSI. Nichts desto trotz wäre es aber aufgrund des zu

erwartenden Meldeaufkommens wünschenswert zu klären wie weitere, aus der Meldepflicht gewonnene Informationen im Einklang mit Datenschutzbestimmungen an IT-Anbieter weitergegeben werden können. Zusätzlich wäre es nützlich klarzustellen, dass das BSI relevante Informationen, die es von Sicherheitsbehörden und/oder CERTs erhalten hat, an Betreiber kritischer Infrastrukturen weitergibt.

d. **BMI & BSI sollten sich in Hinblick auf Angriffstelemetrie mehr mit der Industrie austauschen und Methoden finden, um solche Informationen in effizienter Weise weiterzugeben.** Trotz höherem Datenaufkommen bilden die Informationen, die vermutlich aus der in diesem Gesetz enthaltenen Meldepflicht gewonnen werden können, die Realität nur unzureichend ab. Es müssen voraussichtlich weitere Kanäle für eine verstärkte Zusammenarbeit mit der Industrie in Betracht gezogen werden, um das Ziel zu erreichen "umfassende Informationen zu allen Akteuren und der derzeitigen Situation der Cyberbedrohung" zu sammeln. Eine solche Zusammenarbeit könnte nach Ansicht von AmCham Germany am besten durch das Stärken bestehender vertrauenswürdiger Kanäle zwischen den unterschiedlichen Fachleuten erreicht werden. Solche freiwilligen Kooperationen und Plattformen zum Informationsaustausch - abseits von Meldeverpflichtungen - sind von zentraler Bedeutung. Die Arbeit der Allianz für Cyber-Sicherheit sollte hier im Vordergrund stehen.

e. **Die sektorspezifischen Standards sollten sich eng an die anerkannten internationalen Standards und Best Practices anlehnen.** Das für den kooperativen Ansatz (des öffentlichen & privaten Sektors) vorgeschlagene Modell für die Entwicklung sektorspezifischer Standards bietet durchaus Vorteile, hat aber ebenso Nachteile. AmCham Germany spricht sich dafür aus, die Industrie in den Entwicklungsprozess von Standards mit einzubeziehen: Fakt ist, dass es zahlreiche relevante internationale Standards gibt - sowohl bei der IT-Sicherheit wie auch beim Schutz der kritischen Infrastrukturen, unter anderem die ISO 27000-Serie. Die dem Gesetz beigefügten Zusatzinformationen beziehen sich auf eine Serie spezifischer Sicherheitsmaßnahmen, die in sektorspezifischen Mindeststandards eingeführt werden sollen, darunter

    a. *Informationssicherheitsmanagement (Sicherheitsorganisation, IT-Risikomanagement, etc.)*
    b. *Benennung und Management kritischer Cyber-Assets*
    c. *Maßnahmen zum Schutz und zum Aufspüren von Cyberattacken*
    d. *Business Continuity Management (BCM)*
    e. *Sektorspezifische Standards*

    In diesem Kontext sollte das BMI auf die bereits bestehenden internationalen Standards für jede dieser Maßnahmen zurückgreifen und im Gesetz direkt auf "adäquate internationale Standards" verweisen, um die Gefahr der Standardfragmentierung beziehungsweise das Entstehen nationaler Standards, die den bestehenden internationalen Standards und Best Practices widersprechen, zu reduzieren.

f. **Keine Erweiterung der Meldepflichten für TK-Unternehmen**. AmCham Germany steht einer Erweiterung der Meldepflichten für TK-Betreiber (§ 109 Abs. 5 TKG) ablehnend gegenüber. Die Erweiterung des die Meldepflicht auslösenden Tatbestands auf sämtliche Beeinträchtigun-

gen, die zu einer Verfügbarkeitsstörung bzw. zu einem unerlaubten Zugriff führen können, erscheint uferlos und mündet in einer Berichtspflicht der Betreiber gegenüber dem BSI über sämtliche Vorgänge in ihren Netzen und Anlagen. Wesentlich zu berücksichtigen ist, dass sich geringfügige Verfügbarkeitseinschränkungen in den TK-Infrastruktur-Netzen nicht generell ausschließen lassen. Eine 100%ige Verfügbarkeit wird somit von keinem Infrastrukturanbieter einem Kunden angeboten bzw. vertraglich vereinbart. Vor diesem Hintergrund beziehen sich die bislang vorgesehenen Meldepflichten nach § 109 Abs. 5 TKG auf entsprechend schwerwiegendere Beeinträchtigungen. Eine umfassendere Meldepflicht auch geringfügiger Störungen führt nicht zur Erhöhung der Sicherheit der Infrastrukturen, sondern lediglich zu erheblichem Mehraufwand auf beiden Seiten, insbesondere auch zu einem Bürokratieaufwand der BNetzA. Schließlich ist in diesem Zusammenhang auch auf die Begrifflichkeiten im Rahmen der Regelungen zum Telekommunikationsgeheimnis und Datenschutz zu achten und sicherzustellen, dass diesbezüglich keine Widersprüche entstehen. Im Zusammenhang mit diesem erheblichen Eigeninteresse unserer Mitgliedsunternehmen an der Gewährleistung der Sicherheit auf ihren Infrastrukturen weist AmCham Germany zudem erneut darauf hin, dass die nach § 109 TKG bestehenden Verpflichtungen auch konsequent umgesetzt wurden. Zudem bedarf die Abstimmungspflicht zum Sicherheitskatalog zwischen BNetzA und BSI insoweit zumindest der Klarstellung in der Begründung, dass es hier jedoch maßgeblich auf die Zuständigkeit der BNetzA und deren Praxiserfahrung ankommt.

g. **Sicherheitsauflagen in Telemedien müssen angemessen und praktikabel bleiben.** § 13 Abs. 7 TMG n.F. verlangt von den Adressaten (unter Androhung hoher Bußgelder) „soweit dies technisch möglich und wirtschaftlich zumutbar ist […] sicherzustellen, dass (1.) kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und (2.) diese (a) gegen Verletzungen des Schutzes personenbezogener Daten und (b) Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Maßnahme nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens." Absolute Sicherheit ist in der IT-Welt praktisch nicht erreichbar. Sicherzustellen, dass kein unerlaubter Zugriff möglich ist, ist daher viel zu weitgehend und nahezu unerfüllbar. Zwar wird diese Formulierung vermeintlich durch „wirtschaftlich zumutbar" eingeschränkt, dies nutzt aber allenfalls kleineren Webseitenbetreibern, nicht jedoch einem großen finanzstarken Anbieter von Telemedien, für den je nach Lesart des Gesetzes alleine wegen seiner Größe und Finanzkraft nahezu alles „zumutbar" sein könnte. Der Hinweis im letzten Satz auf ein als sicher anerkanntes Verschlüsselungsverfahren hilft zwar hinsichtlich des Schutzes personenbezogener Daten, nicht jedoch, soweit es um die Sicherung der Systeme und technischen Einrichtungen selbst geht. Hier braucht es eine deutlich eingeschränktere Mittel-Zweck-Relation, außerdem sollte der Begriff „sicherzustellen" durch eine weniger weitgehende Formulierung ersetzt werden.

3. Erhöhte Transparenz bei Produkt-Evaluierungen und öffentlichen Warnungen des BSI

Der derzeitige Gesetzesentwurf stärkt die Befugnis des BSI zur Durchführung von Sicherheitsbewertung von ICT-Produkten, -systemen und -dienstleistungen (§7a). Im Zuge der Durchführung dieser Bewertungen ist das BSI befugt, alle technischen Mittel einzusetzen sowie Dritte zu beauftragen. Die Ergebnisse dieser Bewertung können an Dritte weitergegeben und auch veröffentlicht werden.

Hierzu regt AmCham Germany folgendes an:

a. **Der Entwurf ist in Hinblick auf die Bewertungen sehr weit gefasst. Das Bewertungsverfahren des BSI für ICT-Produkte, -systeme und -dienstleistungen sollte so transparent wie möglich sein.** Die unabhängige Bewertung von Produkten hat in Deutschland eine lange Tradition und Produktbewertungen durch das BSI haben ein großes Gewicht. Aus diesem Grund ist es wichtig, dass diese Bewertungen in transparenter Weise auf der Grundlage einer soliden Methodik durchgeführt werden. Sowohl die Bewertungsschritte als auch die zugrundeliegende Methodik sollten daher den IT-Anbieter der bewerteten Produkte miteinbeziehen, bzw. dem IT-Anbieter mitgeteilt werden und die Möglichkeit für Austausch und Rücksprache vorsehen. Nur so kann sichergestellt werden, dass alle Eigenschaften der besagten Produkte richtig und vollständig verstanden worden sind und die nachfolgenden Schlussfolgerungen so genau wie möglich formuliert werden. Ohne diese Transparenz und ein effektives Feedback des Anbieters würde der geplanten Produktbewertung von Anfang an ihre Glaubwürdigkeit fehlen.

b. **Die Bewertung von Produkten, die noch nicht auf dem Markt sind, wirft erhebliche Bedenken hinsichtlich des Geschäftsgeheimnisses auf und bedroht Innovationen.** Der geplante Entwurf beinhaltet die Möglichkeit, dass das BSI ICT-Produkte bewertet, die noch gar nicht auf dem Markt sind. Solche Produkte und Dienstleistungen beinhalten häufig vertrauliche Geschäftsinformationen. Wenn Informationen über diese Produkte und Dienstleistungen bewertet werden und diese Bewertungen veröffentlicht werden bevor die Produkte bzw. Dienstleistungen in den Handel kommen, stellt dies eine erhebliche Gefahr für das geistige Eigentum des IT-Anbieters dar und wird in der Folge die Innovationsfähigkeit des Anbieters beeinträchtigen. Diese Art der Prüfung verlangsamt Innovationen für große wie für kleine Unternehmen. AmCham Germany empfiehlt dem BMI daher nachdrücklich, Produkte und Dienstleistungen, die nicht im Handel erhältlich sind, von dieser Art der Prüfung durch das BSI und insbesondere durch Dritte entweder auszunehmen oder auf freiwilliger Basis durchzuführen.

c. **Öffentliche Warnungen (§ 7 Warnungen) sollten mit den IT-Anbietern besser koordiniert werden.** Neben der neu eingeführten Regelung der Meldepflicht bei einem Vorfall erhält das BSI darüber hinaus den Auftrag, im Fall von Angreifbarkeiten, Exploits und (neu hinzugefügt) Datendiebstahl öffentliche Warnungen herauszugeben. Unserer Ansicht nach sind Änderungen an dem bestehenden § 7 eine Gelegenheit, das bestehende Warnungsmandat des BSI umfassend zu prüfen und zu verbessern und nicht einfach nur auf Szenarien des Datendiebstahls zu erweitern. Das BMI sollte dabei analysieren, welche Auswirkungen frühere Warnun-

gen seit Einführung der ursprünglichen Befugnis in das BSI Gesetz im Jahr 2009 gehabt haben, um ein klareres Verständnis und eine bessere Methodik für eine Balance zwischen der Verpflichtung zur öffentlichen Warnung und den Interessen der betroffenen Betreiber zu entwickeln. Leider hat das bestehende breite Mandat in vielen Fällen zu Situationen geführt, in denen Warnungen ausgesprochen wurden, obwohl entweder die Bedrohungseinschätzung nicht ausreichend verstanden wurde oder das Verständnis für die tatsächlichen Nutzung mit einem tatsächlich bestehenden Sicherheitsrisiko für die deutsche Bevölkerung nicht da war (z.B. haben längst nicht alle „zero-day exploits" konkrete Auswirkung in allen Märkten gehabt, in denen bestimmte Produkte auch genutzt werden). Das Mandat zur öffentlichen Warnung muss angesichts der Flut von Informationen, die im Rahmen der neuen Regelung der Pflichtmeldungen zu erwarten steht, absolut wasserdicht sein. Eine Möglichkeit, die Regelung zu verbessern, wäre eine Aktualisierung dieses Abschnitts mit der Verpflichtung einer umfassenden Rücksprache mit dem betroffenen Betreiber (oder dem zugrundeliegenden Anbieter des IKT-Produkts) anstelle der einfachen Mitteilung von dem BSI an den Anbieter, so wie dies im Augenblick die Praxis ist.

4. Internationale Harmonisierung von Cybersicherheitspolitik

Es ist das erklärte Ziel der Bundesregierung, dieses Gesetz - auch auf EU-Ebene - als Basis für ihre Positionen in den entsprechenden Verhandlungen zu nutzen, die sich z.B. auf die NIS-Direktive beziehen.

AmCham Germany regt hierzu folgendes an:

a. **Die Bundesregierung sollte die Diskussionen auf EU-Ebene zur stärkeren Harmonisierung nutzen.** Bei den Diskussionen zur Cybersicherheit auf EU-Ebene sollte die Bundesregierung eine noch stärker proaktive Rolle einnehmen, nicht zuletzt, um so auf eine Harmonisierung der Gesetzgebungen in den jeweiligen EU-Staaten hinzuwirken. Dies gilt insbesondere in Hinblick auf die laufenden Gespräche über die Direktive zur Netz- und Informationssicherheit (NIS). So kann sichergestellt werden, dass europäische Grundregeln und der deutsche Ansatz zur IT-Sicherheit harmonisiert werden.

b. **Angleichung der innenpolitischen und europapolitischen Position der Bundesregierung zur IT-Sicherheit.** Deutschland hat auf nationaler Ebene immer dafür plädiert, dass das IT-Sicherheitsgesetz darauf fokussiert sein müsse bessere Sicherheitsergebnisse für kritische Infrastrukturen zu erzielen. Aus Sicht des Risikomanagements ist dies ein sinnvoller Ansatz, der auch auf europäischer Ebene stärker verfolgt werden sollte.

c. **Weitere Harmonisierung der EU-Gesetzgebung zur IT-Sicherheit.** Während klar ist, dass die entsprechende Gesetzgebung angesichts der schnellen Entwicklungen von Technologie und Bedrohungen sehr wahrscheinlich im Laufe der Zeit geändert werden muss, wäre es – auf jeden Fall aus Sicht von in verschiedenen EU-Mitgliedsstaaten aktiven Unternehmen – extrem problematisch, mit 28 unterschiedlichen Versionen von Gesetzen zur IT-Sicherheit mit sich potentiell widersprechenden Anforderungen, Standards etc. konfrontiert zu sein. AmCham Germany setzt sich dementsprechend für die maximal mögliche Harmonisierung der IT-Gesetzgebung in Europa – und am besten weltweit – ein.

d. **Wir empfehlen die Veröffentlichung von in Handlungen umsetzbaren Informationen für öffentliche Behörden, Unternehmen und Verbraucher.** Es entwickeln sich immer neue Bedrohungen der IT-Sicherheit und die gesamte Bedrohungslandschaft ist extrem dynamisch. Die Analyse von 6-Monats-Zeiträumen – statt in einem Jahresbericht – zur Abbildung einer möglichst genauen situativen Darstellung und darüber hinaus die Veröffentlichung von zwei Berichten pro Jahr würde dem BSI die Möglichkeit geben, die öffentliche Wahrnehmung von Bedrohungen der IT-Sicherheit noch stärker zu erhöhen.

Kontakt AmCham Germany
Telecommunications, Internet, and Media (TIM) Committee

Chair
Dr. Nikolaus Lindner, LL.M.
Director, Leiter Government Relations DE / AT / CH, eBay GmbH

Co-Chair
Mike Cosse
Vice President Government Relations Middle & Eastern Europe, SAP SE

Co-Chair
Dr. Gunnar Bender
EVP Corporate Communications, Marketing & Public Policy, arvato AG

Staff Contact
Julia Pollok
Manager, Government Relations
Leiterin Regierungsbeziehungen
American Chamber of Commerce in Germany e.V.
Charlottenstrasse 42, 10117 Berlin
T +49 30 288789-24
F +49 30 288789-29
E jpollok@amcham.de