ERLEBEN, WAS VERBINDET.

DEUTSCHE TELEKOM AG
Friedrich-Ebert-Allee 140, 53113 Bonn

Deutscher Bundestag Innenausschuss
Herrn Ministerialrat Dr. Heynckes
Leiter Sekretariat PA 4
Platz der Republik 1

11011 Berlin

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 A

REFERENZEN
ANSPRECHPARTNER Thomas Tschersich
TELEFONNUMMER 0228 181-75111
DATUM 27.03.2015
BETRIFFT Stellungnahme zum Referentenentwurf des Gesetzes zur „Erhöhung der Sicherheit informationstechnischer Systeme“ (ITSiG)

Sehr geehrter Herr Dr. Heynckes,

die weltweite Digitalisierung und Vernetzung bietet vielfältige Chancen für die Bewältigung der politischen, wirtschaftlichen und gesellschaftlichen Herausforderungen. Angesichts dieser wachsenden Bedeutung des Cyberraums und informationstechnischer Systeme, ist es wichtig, Risiken und Bedrohungen der Netz- und Informationssicherheit zu minimieren. Die Deutsche Telekom begrüßt daher ausdrücklich die vorliegende Initiative zur Verbesserung der Cybersicherheit. Für den Standort Deutschland und Europa ist eine kohärente Cybersicherheitspolitik unerlässlich. Mit Blick auf den baldigen Abschluss der Ressortabstimmungen möchten wir die Gelegenheit nutzen, auf folgende erfolgskritische Aspekte des Gesetzes hinzuweisen.

1. Einbeziehung von Hard- wie Softwareherstellern und sogenannten Over the top Playern

Für eine ganzheitliche Sicherheitsbetrachtung der Wertschöpfungskette der digitalen Welt ist es erforderlich, alle relevanten Marktteilnehmer bei der Umsetzung von Sicherheitsanforderungen zu berücksichtigen, die Produkte oder Dienste im Cyberraum anbieten. Dies betrifft alle Anbieter, bei denen ein Ausfall oder eine Beeinträchtigung ihres Dienstes mit dem Ausfall oder der Beeinträchtigung kritischer Infrastrukturen vergleichbar ist. Mit umfasst sein müssen daher auch Hardware- und Softwarehersteller sowie Internetdienste, die bisher ohne überzeugende sachliche Rechtfertigung nicht in der gebotenen Klarheit vom Anwendungsbereich des Gesetzes erfasst sind. Die Delegation dieser wichtigen Frage auf eine spätere Rechtsverordnung ist unzureichend. Erforderlich ist eine konkrete Nennung von Diensten und Herstellern im Gesetz, beispielsweise durch Einfügung eines § 2 Absatz 11 BSI Gesetz.
Das Ziel des Gesetzes, das Sicherheitsniveau in Gänze zu heben, kann schlicht nicht durch eine singuläre Verpflichtung einzelner Akteure im Cyberraum erfüllt werden, insbesondere nicht, wenn diese ausschließlich

DATUM 27.03.2015
EMPFÄNGER Herrn Ministerialrat Dr. Heynckes

Telekommunikationsanbieter trifft. Denn die Verarbeitung von Daten findet regelmäßig bei den Diensteanbietern selbst statt (etwa den Cloud-Diensten, E-Mail-Diensten oder sozialen Netzwerken). Zudem erfolgen Angriffe auf die Telekommunikationsnetze in der Regel von außen, d.h. mittels manipulierter Hard- und/oder Software. Die Erkennung, Behebung und auch die Mitteilung von Störungen von Komponenten und Diensten ist schnellstmöglich und effektiv nur zu gewährleisten, wenn die genannten Hersteller und Diensteanbieter mit in den Verpflichtungskanon aufgenommen werden.
Im Falle etwaiger Sicherheitsrisiken, deren Beseitigung beispielweise ein Software-Update oder eine anderweitige Anpassung von Systemkonfigurationen voraussetzt, muss es in der Verantwortung der jeweiligen Anbieter liegen, die Schwachstelle unverzüglich zu beheben. Es wäre unbillig, den Telekommunikationsanbietern diese Obliegenheit aufzubürden, insbesondere weil sie in aller Regel auf die Unterstützung der Hard- und Softwarehersteller bzw. Diensteanbieter angewiesen sind. Unseres Erachtens ist der deutsche Gesetzgeber auch nicht daran gehindert, Regelungen für Hersteller und Diensteanbieter zu treffen, selbst wenn diese Hersteller und Diensteanbieter ihren Sitz nicht in Deutschland haben bzw. ihre Leistungen für deutsche Kunden aus dem Ausland erbringen.

2. Absenkung der Meldeschwellen nach § 109 Absatz 5 TKG

Nach der Neufassung des § 109 Abs. 5 TKG sollen zukünftig bereits solche Beeinträchtigungen der Netze und Dienste mitteilungspflichtig sein, die etwa zu Sicherheitsverletzungen und Störungen führen können. Für die Pflicht zur Mitteilung ist es unerheblich, wie wahrscheinlich der Eintritt des Ereignisses und wie wahrscheinlich der Eintritt daraus resultierender Beeinträchtigungen ist.

Nach der aktuellen Rechtslage muss die Störung bereits eingetreten sein, sich also bereits realisiert haben. Die derzeitige Meldepraxis hat sich bewährt. Eine Absenkung der Meldeschwelle ist weder erforderlich noch angemessen. Sie würde die Verwaltungstätigkeit der BNetzA und der Netzbetreiber massiv erhöhen, ohne aber einen signifikanten Mehrwert für die IT Sicherheit zu leisten.
Im Übrigen sehen wir keinen sachlichen Grund, die Möglichkeit anonymer Meldungen ausschließlich den Betreibern sonstiger kritischer Infrastrukturen einzuräumen. Wir schlagen daher vor, die Form der Meldungen für alle Betreiber kritischer Infrastrukturen hinsichtlich der Frage der anonymen Meldemöglichkeit einheitlich zu regeln.

3. Konkretisierung der Informationspflicht gegenüber Nutzern nach § 109a Abs. 4 TKG

Der § 109a Abs. 4 TKG führt neue Benachrichtigungspflichten des Diensteanbieters gegenüber Nutzern ein, wenn Störungen bekannt werden, die von dessen Datenverarbeitungssystemen ausgehen.
Auch an dieser Stelle ist der Diensteanbieter der falsche Regelungsadressat: Die skizzierte Benachrichtigung des Nutzers ist immer dann sinnvoll, wenn die Information geeignet ist, die Behebung von Störungen zu beschleunigen und/oder Schäden der Betroffenen vorzubeugen bzw. diese gering zu halten. Voraussetzung dazu ist, dass die Information aus erster Hand erfolgt und nicht über Dritte an die Betroffenen gelangt. Eine solche Vorgehensweise kostet unter Umständen wertvolle Zeit und birgt das Risiko von (Übertragungs) Fehlern bei der Information der Betroffenen. Störungen von Datenverarbeitungssystemen müssen daher den

ERLEBEN, WAS VERBINDET.

DATUM 27.03.2015
EMPFÄNGER Herrn Ministerialrat Dr. Heynckes

Nutzern selbst bzw. von den Herstellern und Betreibern der Datenverarbeitungssysteme, also den Störern, gemeldet werden und nicht (jedenfalls nicht ausschließlich) von Diensteanbietern.
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. Informationen dazu würden keinen Beitrag zur Erhöhung der IT Sicherheit leisten und wären in der Praxis aufgrund der Vielzahl solcher Störungen nicht handhabbar. Zudem genügt nach der Vorschrift jede Erkenntnisquelle und jede Störungsinformation zur Auslösung der Informationspflicht, unabhängig davon, ob die Information wirklich wahr ist und ob sie den Betroffenen zum Zeitpunkt der Störung hilfreich ist. Auch in diesen Punkten ist die Regelung mithin zu weit gefasst und die daraus folgenden Verpflichtungen in zahlreichen Anwendungsfällen nicht erforderlich und unangemessen.
Nach der Gesetzesbegründung ist eine individuelle Information der Nutzer nicht geschuldet, vielmehr genügen allgemeine Informationen zur Erfüllung der Informationspflicht. Dieser wichtige Punkt sollte explizit im Gesetzestext klargestellt werden.
Zudem möchten wir das Augenmerk des Gesetzgebers auf die Haftungsvorschriften der §§ 44 und 44a TKG lenken. Problematisch erweist sich hier der Umstand, dass Diensteanbieter bei fehlerhaften oder verspäteten Informationen einem Haftungsrisiko ausgesetzt sind. Dies erscheint unbillig, weil die Störungen gerade nicht in eigenen Systemen und Anwendungen des informierenden Diensteanbieters auftreten. Hier bedarf es einer Haftungsfreistellung des benachrichtigenden Diensteanbieters, der nicht selbst Störer im Rechtssinne ist.

Mit freundlichen Grüßen

ppa.
Thomas Tschersich
Leiter Group Security Services