IEN · Dorotheenstrasse 54 · 10117 Berlin

Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SicherheitsG – BSIG-E)

Hier: Stellungnahme der Initiative Europäischer Netzbetreiber (IEN)

Sehr geehrte Damen und Herren,

das Bundesministerium des Inneren hat am 19. August 2014 einen überarbeiteten Entwurf für ein IT-Sicherheitsgesetz vorgelegt. Zentraler Gegenstand der Regelungen ist die Schaffung von Mindestsicherheitsstandards für Betreiber kritischer Infrastrukturen (KRITIS), sowie eine Meldepflicht für deren Betreiber bei IT-Sicherheitsvorfällen gegenüber dem BSI. Das BSI soll als zentrale Anlaufstelle für IT-Sicherheit in den Zuständigkeiten und Kompetenzen gestärkt werden.

Dieser neue Entwurf soll nunmehr zwischen den Ressorts der zuständigen Ministerien zur Abstimmung gelangen.

I. Allgemeine Anmerkungen:

Die IEN nimmt zur Kenntnis, dass die nicht nur von der IEN, sondern auch anderen Verbänden und Unternehmen geäußerte Kritik zumindest in Teilen aufgenommen wurde. Erkennbar ist eine größere Konzentration auf kritische Infrastrukturen, welche bislang keinen gesonderten Meldepflichten o.ä. unterlagen und Klärungen im Hinblick auf die Zuständigkeiten. Insbesondere sind die deutlicheren Klarstellungen zu begrüßen, dass Anbieter, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen von den neuen Melde- und Nachweispflichten gegenüber dem BSI überwiegend ausgenommen sind.

Allerdings erachtet die IEN die bislang vorgenommenen Änderungen, bzw. auch Neueinfügungen nicht in allen Bereichen für praxistauglich.

Gerade die IEN-Mitgliedsunternehmen, welche überwiegend große, international agierende Unternehmenskunden mit TK-Dienstleistungen versorgen, haben bereits aufgrund ihres eigenen Geschäftsfokus ein erhebliches Interesse an der Sicherheit ihrer Infrastrukturen und räumen diesem Aspekt im Rahmen ihrer Aktivitäten und Strategien einen erheblichen Stellenwert ein. Da ihre Dienstleistungen überwiegend grenzüberschreitend stattfinden,

…

haben diese Unternehmen insbesondere auch ein erhebliches Interesse daran, dass die internen Sicherheitsprozesse möglichst zentralisiert und einheitlich durchgeführt werden und dass entsprechende regulatorische Vorgaben diesen Ansatz unterstützen.

Vor diesem Hintergrund erachtet die IEN nach wie vor insbesondere den nationalen „Alleingang" und die fehlende europäische Einbettung des Gesetzesentwurfes als kritisch. Der gegenständliche Entwurf lässt ungeachtet des gleichen Regelungsgegenstandes das derzeit stattfindende, europäische Gesetzgebungsverfahren zur NIS-Richtlinie vollständig außer Acht. Die bisherige Gesetzesbegründung enthält keinerlei Hinweise zu einem Umgang mit der Richtline. In diesem Zusammenhang ist beispielsweise darauf hinzuweisen, dass etwa die in § 109 TKG bestehenden Verpflichtungen im Einklang mit den Meldeverfahren bei der europäischen Behörde ENISA für die TK-Unternehmen umgesetzt worden. Vor diesem Hintergrund muss sich jede neue Vorgabe daran messen lassen, ob sie mit den bereits bestehenden Vorgaben konform geht und bei den Unternehmen nicht zu kostenerheblichen Doppelbelastungen bei möglicherweise unübersichtlichen Doppelzuständigkeiten mit erheblichem bürokratischem Aufwand führt. An dieser Stelle ist insbesondere zu hinterfragen, inwieweit die vorgesehene Rolle der BNetzA gegenüber dem BSI zu konkretisieren ist.

II. Im Einzelnen

1. Zu den internationalen Bestrebungen, ein einheitliches Sicherheitskonzept zu entwickeln

Die IEN weist im Zusammenhang mit dem gegenständlichen Entwurf auf die jüngsten Entwicklungen auf europäischer Ebene hin. Dort hat die EU gerade im vergangenen Jahr die Cyber Security Strategy verabschiedet und entsprechende regulatorische Vorschläge in Form einer Richtlinie für Netz- und Informationssicherheit (KOM (2013) 48 final, NIS Richtlinie) unterbreitet. Diese betreffen damit insbesondere auch die vorliegend im Fokus stehende Sicherheit von TK-Infrastrukturen.

Im Rahmen der damit einhergehenden Betrachtung der gegenwärtigen Marktgegebenheiten stellte auch die EU Kommission unter anderem fest, dass die TK-Infrastrukturanbieter bereits gegenwärtig entsprechende grenzüberschreitende Vorkommnisse, die die Sicherheit der Infrastrukturen betreffen, an die zuständige europäische Behörde ENISA melden müssen. Vor diesem Hintergrund bestehe jedoch ein Bedarf, europaweit einheitliche Mindestregelungen für die betroffenen Unternehmen in den Mitgliedstaaten unter der Beteiligung von ENISA festzulegen, um in der Branche verstärkt für Rechts- und Planungssicherheit zu sorgen.

Im Frühjahr 2014 stimmte auch das EU Parlament für den Richtlinienentwurf in geänderter Form. Die nunmehr im Rahmen des NIS Richtlinienentwurfs geplanten Vorgaben sind in vielfacher Hinsicht geeignet, die nunmehr seitens der BMI intendierten Maßnahmen zur Wahrung der Sicherheit der Infrastrukturen auf dem TK-Sektor hinreichend, neben den bereits bestehenden Regelungen des TKG, die ebenfalls auf europäischen Vorgaben beruhen, zu gewährleisten.

Es wird daher seitens der IEN als unerlässlich erachtet, nunmehr vorschnelle nationale Alleingänge zu vermeiden, sondern sich vielmehr proaktiv an der Etablierung harmonisierter Regelungen zu beteiligen und diese zu unterstützen. Erst im Anschluss sollte in einem zweiten Schritt, dort wo gemäß den Vorgaben der Richtlinie ergänzender Regelungsbedarf auf nationaler Ebene besteht, die Umsetzung ergänzender Vorgaben erfolgen. Obgleich die Anbieter, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, von den neuen Melde- und Nachweispflichten gegenüber dem BSI überwiegend ausgenommen sein sollen, so enthält der gegenständliche Entwurf auch bezüglich dieser Anbieter neue Verpflichtungen, die über die bisher geltenden Regelungen deutlich hinaus gehen.

Ein vorgezogener nationaler Einzelweg zwingt die betroffenen Unternehmen zur Einrichtung aufwendiger interner Prozesse und Personalstellen, welche etwa nach Inkrafttreten und Umsetzung der Richtlinie in nationales Recht erneut umgestellt werden müssten. Dies wäre stets mit – vorliegend nicht notwendigem - erheblichem finanziellem Aufwand verbunden und kann somit nicht im Sinne der Förderung des Wirtschaftsstandorts Deutschland sein.

Zugleich ist zu berücksichtigen, dass sich die betreffenden TK-Infrastrukturanbieter, deren Dienstleistungen überwiegend grenzüberschreitend erbracht werden, im Fall der Festlegung von nationalen Einzelregelungen häufig unterschiedlichen Vorgaben für ein und dieselbe Dienstleistung für ein und denselben Kunden gegenübersehen. Deren Erfüllung dürfte häufig wegen konträrer Vorgaben, etwa zur Art der Meldung oder Schnittstelle, überhaupt nicht rechtskonform möglich sein, obgleich die TK-Unternehmen, wie bereits ausdrücklich klargestellt, sich rechtstreu verhalten wollen und erheblichen Wert auf die Sicherheit ihrer Infrastrukturen legen.

2. Zu den einzelnen Vorschriften

a. Zu der künftigen Rolle des BSI - § 3 Aufgaben des Bundesamtes

Nach den Regelungen des § 3 Abs. 1 Nr. 16 ist das BSI die zentrale Stelle für Zusammenarbeit mit zuständigen Stellen im Ausland. Entsprechend den Ausführungen in der Begründung des Entwurfs wird dadurch der „gewach-

senen Rolle des BSI als nationalem und internationalem Ansprechpartner in Fragen der IT- und Cybersicherheit in Deutschland“ Rechnung getragen. Nach § 3 Abs. 3 wird diese Regelung ohne Beschränkung auch im nationalen Bereich erweitert, indem das BSI als zentrale Stelle für die Sicherheit der IT- kritischen Infrastrukturen vorgesehen ist.

Ungeachtet der Ausnahmeregelungen in § 8a Abs. 4 und § 8b Abs. 7 stellt sich bei dieser übergeordneten Regelung die Frage, inwieweit das BSI künftig die BNetzA in Fragen der IT-Sicherheit im TK-Bereich ersetzen soll.

Wie bereits in der Stellungnahme der IEN aus April 2013 dargelegt, verfügt die BNetzA für die TK-Branche bereits über eine langjährige Praxiserfahrung im Bereich Sicherheit und arbeitet auch hier in enger Abstimmung mit den Regulierungsbehörden anderer europäischer Mitgliedstaaten. Wie dort ausgeführt, orientiert sich die BNetzA dabei auch an europäischen Vorgaben oder Kriterien, etwa von ENISA bezüglich des Umsetzungskonzepts zu § 109a TKG. Dieses Know-how, auf welches sich die Marktbeteiligten bei der bereits seit langem erfolgten Implementierung der Sicherheitskonzepte verlassen, darf keinesfalls dadurch verwässert werden, dass die BNetzA zum reinen „Meldetrichter“ für das BSI umfunktioniert wird. Dabei ist auch die langjährige Abstimmung der BNetzA mit dem BMWi als bislang zentrales Ministerium für Fragen der TK-Gesetzgebung zu berücksichtigen, welche ebenfalls über langjährige Expertise auch in diesem Gebiet verfügen.

Vor diesem Hintergrund fordert die IEN, dass sämtliche Vorgaben, die eine Abstimmung oder ein Benehmen zwischen der BNetzA und dem BSI vorsehen, für den TK-Bereich die BNetzA als inhaltlich federführend gelten sollte und auch diejenige Behörde bleibt, welche etwaige Maßnahmen oder Verpflichtungen gegenüber den Anbietern öffentlich zugänglicher Telekommunikationsdienste und –netze erlässt.

b. Zu den Erweiterungen der Veröffentlichungsrechte - §§ 7 und 7a

Gemäß § 7 Abs. 1 ist eine Erweiterung des Informationsrechts des BSI gegenüber der Öffentlichkeit auch „im Falle des unberechtigten Abflusses von Daten“ vorgesehen. Weiterhin soll sich das BSI bei der Recherche/Analyse durch Dritte unterstützen lassen. Die Begründung des Entwurfs stellt diesbezüglich klar, dass beispielsweise Provider / Diensteanbieter zur Identifikation der Betroffenen genutzt werden sollen.

Entsprechend der Regelung des § 7a darf das BSI zudem künftig Produkte, Systeme und Dienste untersuchen und die Erkenntnisse bzw. Bewertungen weitergeben und veröffentlichen. Die Hersteller betroffener Produkte sind ggf. zuvor zu informieren.

Diese Vorgaben sind nach Auffassung der IEN zu weitgehend. Wie bereits ausgeführt, handelt es sich bei den von den IEN-Mitgliedsunternehmen mit

TK-Dienstleistungen versorgten Kunden um große Geschäftskunden. Diese belegen die TK-Anbieter mit weitrechenden Vertraulichkeitsregelungen und eigenen Sicherheitsvorgaben. Vielfach unterliegen die TK-Dienstleister empfindlichen Vertragsstrafen gegenüber ihren Kunden, soweit diese eine Verletzung ihrer Geheimhaltungsinteressen als gegeben ansehe. Die pauschale Erweiterung der Rechte zur Veröffentlichung des BSI birgt hier stets die Gefahr, vertrauliche Informationen auch über den Kunden zu veröffentlichen. Hier ist zwingend eine Einschränkung dahingehend vorzunehmen, dass dies im Fall von großen Unternehmenskunden, welche mit den Anbietern von öffentlich zugänglichen TK-Netzen und –Diensten stets nur mit Zustimmung oder nach Information dieser Unternehmen erfolgen darf.

Auch an dieser Stelle ist auf die Praxiserfahrung der BNetzA zu verweisen. Diese hat sich bereits häufig mit den Geheimhaltungs- und Sicherheitsbedenken der Marktbeteiligten auseinandergesetzt und in vielen Fällen, jüngst etwa bei der Datensammlung zum Infrastrukturatlas um einen sinnvollen Ausgleich der Bedenken und Beschränkungen bemüht.

c. Zu den Änderungen des TKG – Art. 3

aa. Klarstellung zur Verwendung von Daten bei Störungen § 100 TKG

In § 100 TKG wird klargestellt, dass Diensteanbieter Bestands- und Verkehrsdaten auch zum Erkennen und Beseitigen von Schadprogrammen und entsprechender Infrastruktur verwenden dürfen. Diese Klarstellung wird von der IEN ausdrücklich begrüßt.

bb. Erweiterung der Pflichten von TK-Unternehmen - § 109 Abs. 5

Ablehnend steht die IEN der Erweiterung der Meldepflichten für TK-Betreiber (§ 109 Abs.5 TKG) gegenüber. Die Erweiterung des die Meldepflicht auslösenden Tatbestands auf sämtliche Beeinträchtigungen, die zu einer Verfügbarkeitsstörung bzw. einem unerlaubtem Zugriff führen können, erscheint uferlos und klingt wie eine Berichtspflicht der Betreiber gegenüber dem BSI über sämtliche Vorgänge in ihren Netzen und Anlagen.

Zunächst weist die IEN daraufhin, dass sich geringfügige Verfügbarkeitseinschränkungen sich 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 nicht zur Erhöhung der Sicherheit der Infrastrukturen sondern lediglich zu erheblichem Mehraufwand auf beiden Seiten, insbesondere auch einem Bürokratieaufwand der BNetzA führt.

…

Schließlich ist 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 der IEN-Mitgliedsunternehmen an der Gewährleistung der Sicherheit auf ihren Infrastrukturen weist die IEN 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 (vgl. Ausführungen unter II 2 a).

cc. Meldepflicht bei Sicherheitslücken beim Nutzer - § 109 a Abs. 4

Hinsichtlich der Benachrichtigungspflicht für die Kunden über die Verletzung der IT-Sicherheit in den von ihnen betriebenen datenverarbeitenden Systemen weist die IEN erneut auf die Sachlage bei der Erbringung von TK-Dienstleistungen mit großen Unternehmenskunden hin.

Wie bereits ausgeführt, geben diese Kunden bereits selbst Vorgaben, nach denen sie über Beeinträchtigungen und Sicherheitsverletzungen, gleich welcher Art oder Verursachung, informiert werden wollen. Insofern steht die neue Vorgabe des § 109 Abs.4 diesen Vereinbarungen zwar nicht entgegen, allerdings dient diese Vorschrift ausweislich der Begründung der Vereinheitlichung der Prozedere. Da die IEN-Mitgliedsunternehmen mit ihren Kunden jedoch stets Individualvereinbarungen nach den Vorgaben des Kunden und dessen IT-Beschaffungsabteilungen abschließen, laufen sie Gefahr, sich in einen Konflikt zu begeben.

Diesbezüglich verweist die IEN auch auf die Diskussionen und gefundenen Lösungsansätze im Rahmen der Entwicklung der Transparenz-VO, welche voraussichtlich noch in diesem Jahr verabschiedet wird. Dort hat man sich ausdrücklich darauf geeinigt, Ausnahmeregelungen zuzulassen, soweit der Anbieter mit Kunden eine Individualvereinbarung getroffen hat.

****

Für Rückfragen stehen die Vertreter der Mitgliedsunternehmen der IEN sowie ich selbst jederzeit gern zur Verfügung. Die Stellungnahme enthält keine Betriebs- und Geschäftsgeheimnisse.