Ergänzende Anmerkungen und Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern für Bau und Heimat eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) (Stand 9.12.2020)

Berlin 10. Dezember 2020

Am 9. Dezember 2020 hat eco – Verband der Internetwirtschaft e.V. den am 1. Dezember desselben Jahres veröffentlichten Diskussionsentwurf des Bundesministeriums des Innern für Bau und Heimat (BMI) zum Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – nachfolgend IT-SiG 2.0) kommentiert und hierzu eine umfangreiche Stellungnahme eingereicht.

Am selben Tag übermittelte das BMI einen überarbeiteten Referentenentwurf zur Verbändebeteiligung gem. § 47 (3) der gemeinsamen Geschäftsordnung der Bundesministerien mit Frist zum 10. Dezember 2020.

In Anbetracht der eingeräumten Frist von lediglich einem Tag zur Beteiligung ist eine der Bedeutung und Auswirkungen des IT-SiG 2.0 angemessene und umfassende Würdigung des Gesetzesentwurfs nur sehr eingeschränkt möglich.

eco verweist unbeschadet etwaiger Änderungen in dem nun vorliegenden Referentenentwurf des IT-SiG 2.0 auf seine umfassende Kommentierung.

Ergänzend dazu macht eco noch folgende Anmerkungen zu dem vorliegenden Referentenentwurf. Er beschränkt sich dabei auf Aspekte, die durch den nunmehr vorliegenden Referentenentwurf geändert wurden. Diese Kommentierung ist als Ergänzung zur Stellungnahme über den Diskussionsentwurf zu lesen, die er im Übrigen und sofern hier nicht anders dargelegt aufrechterhält:

Zu Artikel 1 Nr. 1 f

Ergänzend zu den Anmerkungen zum Diskussionsentwurf möchte eco festhalten, dass die Neufassung des § 2 (13) BSI-G-neu nunmehr die Möglichkeit zur Feststellung kritischer Funktionen vorsieht, aus denen wiederum kritische Komponenten abgeleitet werden können.

Die vorliegende Formulierung lässt leider keinen Rückschluss darauf zu, wie genau sich diese kritischen Funktionen aus einem Gesetz ableiten lassen sollen. Auch die Begründung gibt hierzu leider keinerlei sachdienlichen Hinweise. Infolgedessen bleibt unklar, wie sich aus kritischen Funktionen wiederum kritische Komponenten ableiten lassen. Insgesamt erweckt diese Formulierung den Eindruck, dass damit der Vorbehalt, kritische

Komponenten ausschließlich gesetzlich zu definieren, ausgehebelt werden soll. In der Konsequenz ist auch die Umformulierung des Absatzes zur gesetzlichen Grundlage für die Festlegung kritischer Komponenten problematisch.

eco erneuert seine Kritik an dem Gesetzentwurf: Für kritische Komponenten muss eine eindeutige gesetzliche Grundlage bestehen. Eine abstrakte Ableitung aus Gesetzen oder Funktionen, die wiederum aus weiteren Gesetzen abgeleitet sind, ist unkonkret und daher abzulehnen.

Die im Vergleich zum Diskussionsentwurf vom 1. Dezember vorgenommenen Streichungen im § 2 (14) BSI-G-neu zur näheren Bestimmung von Unternehmen von besonderem öffentlichen Interesse sind nach Ansicht des eco ebenfalls als problematisch zu bewerten. Es wird der Eindruck erweckt, dass nicht, wie ursprünglich zu vermuten war, nur wenige ausgewählte Unternehmen von dieser Regelung betroffen sein werden, sondern, dass der Adressatenkreis der Norm deutlich weiter gefasst sein könnte. eco fordert den Gesetzgeber auf, die durch den vorliegenden Entwurf hervorgerufenen Unsicherheiten und Unklarheiten hinsichtlich des Anwendungsbereichs und des Adressatenkreises zu beseitigen und hierdurch Rechtssicherheit bei den betroffenen Unternehmen zu schaffen. Es sind normenklare, nachvollziehbare und verhältnismäßige Anforderungen an die Definition eines Unternehmens von besonderem öffentlichen Interesse zu formulieren.

Zu Artikel 1 Nr. 10

Die in §7c BSI-G-neu geschaffene Anordnungsbefugnis für das BSI begründet eine Doppelzuständigkeit für den Sektor der Telekommunikation für das BSI einerseits und die Bundesnetzagentur (BNetzA) andererseits aufgrund des Telekommunikationsgesetzes. Eine solche Doppelzuständigkeit wird von eco kritisch bewertet und abgelehnt.

Inakzeptabel erscheint zudem die mit dem Referentenentwurf hinzugekommene Auferlegung der Verantwortung zu Lasten der Telekommunikationsanbieter für Router, die deren Kunden käuflich erworben haben. Der Gesetzgeber lässt zwar in der Gesetzesbegründung erkennen, dass ihm bewusst ist, dass rechtlich ein Unterschied zwischen von Anbietern überlassenen Routern und von deren Kunden gekauften Geräten besteht, vgl. S. 77, zweiter Absatz. Gleichwohl will der Gesetzgeber die Verantwortung für die Kaufgeräte auch den TK-Anbietern zuweisen. Damit behandelt er ohne sachliche Rechtfertigung wesentlich Ungleiches gleich.

Zu Artikel 1 Nr. 12

Die gegenüber dem Diskussionsentwurf vorgesehene Verkürzung der Umsetzungsfrist für den Einsatz von Systemen zur Angriffserkennung ist mit einem Werktag deutlich kurz bemessen. Nach Ansicht des eco sollte die Frist zur Umsetzung und Implementierung mindestens 12 Monate betragen. Insbesondere auch, da davon auszugehen ist, dass sich aus der Verpflichtung zum Einsatz entsprechender Systeme weitere Fragestellungen zu den jeweils passenden Detektionssystemen und deren Integration in vorhandene Infrastrukturen ergeben. Unsere grundsätzliche Kritik an der Vorschrift hatten wir bereits in unserer Stellungnahme zum Diskussionsentwurf ausführlich dargelegt.

Zu Artikel 1 Nr. 17

eco möchte ergänzend zu seiner ausführlichen Kommentierung im Rahmen des Diskussionsentwurfs darauf hinweisen, dass die vorgenommene Verkürzung der Frist zur Vorlage von Informationen über Zertifizierungen, Audits und technisch-organisatorische Maßnahmen zu kurz bemessen ist. Gerade vor dem Hintergrund, dass insbesondere bei den Unternehmen von besonderem öffentlichen Interesse ohnehin größerer Anpassungsbedarf ggfs. auch bei deren Zulieferbetrieben und Dienstleistern besteht und vor dem Hintergrund einer deutlichen Erweiterung des Adressatenkreises dieser Norm ist die vorgenommene Fristverkürzung vor allem in Verbindung mit dem gesetzten Bußgeldrahmen nicht nachvollziehbar. Die betroffenen Unternehmen benötigen angemessene Umsetzungs- und Implementierungsfristen.

Zu Artikel 1 Nr. 20

Der § 10 des BSI-Gesetzes sieht einen neuen Absatz 6 vor, der das BMI im Einvernehmen mit dem BMWi dazu ermächtigt, eine Verordnung über die „Offenlegung von Schnittstellen und die Einhaltung etablierter technischer Standards“ zu erlassen. In der vorliegenden Pauschalität ist die Verordnungsermächtigung abzulehnen. Die hier getroffene Regelung wird aller Voraussicht nach nicht mit den ohnehin bestehenden Maßgaben harmonieren. Inwieweit eine Offenlegung von Schnittstellen zur Verbesserung der IT-Sicherheit beitragen soll, wird nicht erläutert. Die Gesetzesbegründung lässt bedauerlicherweise keine weiteren Rückschlüsse zu, da sie gänzlich fehlt. Bisher war an anderer Stelle in Bezug auf die Offenlegung von Schnittstellen meist auf die Ausleitung von Kommunikation von Endnutzern bezogen. eco erachtet die hier getroffene Verordnungsermächtigung als verfassungsrechtlich problematisch, da hiervon unter Umständen auch ein grundrechtssensitiver Bereich tangiert

wird. Zudem sind Schnittstellen oftmals urheberrechtlich geschützt, was zusätzliche Probleme eröffnen dürfte. In der vorliegenden Fassung und Ausgestaltung ist diese Vorschrift abzulehnen.

Zu Artikel 2

Ergänzend zu den ausführlichen Ausführungen zum Diskussionsentwurf erachtet eco die in § 109 TKG-neu vorgeschlagenen Änderungen als Verletzung des Parlamentsvorbehalts. In der Allgemeinverfügung zum Sicherheitskatalog soll festgelegt werden können, was kritische Funktionen sind, anhand deren wiederum kritische Komponenten im Sinne von § 2 Abs. 13 BSIG-neu bestimmt werden und anhand dessen ein Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial einzustufen ist. Allein die beschriebene Herleitung und Verweisung macht deutlich, dass für betroffene Unternehmen keinerlei Vorhersehbarkeit besteht und selbst kleinere Änderungen und Anpassungen auf untergesetzlicher Ebene gravierende Auswirkungen und Konsequenzen für die Unternehmen haben können. Unter anderem sind mit den getroffenen Festlegungen eine Vielzahl intensiver Eingriffe bei den Unternehmen verbunden, wie beispielsweise die Meldepflicht einzelner Komponenten, der Untersagungsvorbehalt, eine Rückbauverpflichtung, die Durchführung von Audits im Zwei-Jahres-Intervall zusätzlich zu Überprüfungen durch BNetzA. Nach Ansicht des eco muss die Entscheidung und Festlegung der kritischen Komponenten sowie kritischen Funktionen innerhalb aller Sektoren auch im Bereich Telekommunikation zwingend durch den parlamentarischen Gesetzgeber getroffen und vorgenommen werden.

Fazit

Vor dem Hintergrund der vom BMI eingeräumten eintägigen Frist zur Beteiligung ist eine der Bedeutung des Gesetzgebungsverfahrens angemessene und umfangreiche Kommentierung nicht möglich. Insbesondere unter Berücksichtigung des Umstands, dass auch der nunmehr zur Verbändebeteiligung freigegebene Gesetzentwurf noch nicht endgültig ressortabgestimmt und weitere Änderungen zu erwarten sind, kann eine abschließende Bewertung des geplanten IT-SiG 2.0 im jetzigen Stadium nicht erfolgen. eco wird sich daher im weiteren Verlauf des Gesetzgebungsverfahrens zum IT-SiG 2.0 einbringen.

Die mit dem vorliegenden Referentenentwurf vorgenommen Anpassungen und neuen Regelungen verstärken die Bedenken, dass mit dem IT-SiG 2.0 in der derzeit diskutierten Form das Ziel einer stringenten, verhältnismäßigen und zielgerichteten IT-Sicherheitsregulierung für Deutschland mit einem klar umrissenen Anwendungsbereich nicht erreicht werden kann. Die bereits bestehenden grundsätzlichen Zweifel an Verfassungsmäßigkeit und

Verhältnismäßigkeit der geplanten Regelungen wurden mit dem nun vorgelegten Referentenentwurf weiter verstärkt und erfordern gravierenden Überarbeitungs- und Nachbesserungsbedarf.

eco – Verband der Internetwirtschaft e.V. empfiehlt in Anerkennung der Konsequenzen für den weiteren Gesetzgebungsvorgang, die Beratungen des IT-SiG 2.0 zurückzustellen und die weiteren Entwicklungen auf europäischer Ebene abzuwarten. Nur so kann eine systematische und stringente IT-Sicherheitsregulierung mit Erfolg umgesetzt werden.

Über eco

Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.