TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der IT-Sicherheitsverband.

Berlin, 16.12.2016

Stellungnahme

zum Referentenentwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 06.07.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL-Umsetzungsgesetz)

(TeleTrusT-Arbeitsgruppe "Recht")

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.), "TeleTrusT Engineer for System Security" (T.E.S.S.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Qualitätszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Stellungnahme
Am 09.12.2016 wurde den betroffenen Verbänden der Entwurf eines Gesetzes zur Umsetzung der sogenannten NIS-Richtlinie zur Stellungnahme vorgelegt. Auch wenn der vorgelegte Referentenentwurf wie auch der Gesetzgebungsprozess des IT-Sicherheitsgesetzes 2015 mit seiner vorauseilenden Schaffung einer nationalen Einzelregelung und deren nachlaufender Anpassung an die gemeinschaftsrechtlichen Vorgaben der NIS-Richtlinie 2016 weitreichenden Erörterungsbedarf bieten, fokussiert die Stellungnahme auf die für die Anbieter digitaler Dienste neu geschaffenen Pflichten. Diesem legislativen Vorgehen Deutschlands sind jedoch diverse Anwendungsprobleme geschuldet.

Als zentrale Norm schafft § 8c BSiG-E nun neue Verpflichtungen für Anbieter digitaler Dienste, die nahezu wortgleich durch die NIS-Richtlinie vorgegeben werden. Dieses Vorgehen ist im Sinne der Vollharmonisierung grundsätzlich nicht zu beanstanden. Art. 16 Abs. 10 der NIS-Richtlinie verbietet den Mitgliedstaaten für den Bereich der digitalen Dienste ausdrücklich, den Anbietern weitergehende Pflichten aufzuerlegen.

Das vorab beschlossene deutsche IT-Sicherheitsgesetz enthält keine ausdrücklichen Pflichten für Anbieter digitaler Dienste im Sinne der Richtlinie, die einer solchen Harmonisierung entgegenstehen. Allerdings wurde § 13 Absatz 7 Telemediengesetz (TMG) geschaffen, der für Telemediendiensteanbieter im weiteren Sinne vergleichbare Sicherungspflichten trifft. Anders als die sonstigen auf deutscher oder europäischer Ebene geschaffenen Regelungen zur Stärkung der IT-Sicherheit, treffen diese aber nicht nur Betreiber einzelner kritischer bzw. wesentlicher Leistungen. Stattdessen genügt bereits eine geschäftsmäßig betriebene Website. Ein derart breiter Verpflichtetenkreis ist sowohl dem IT-Sicherheitsgesetz hinsichtlich der Betreiber kritischer Infrastrukturen als auch der NIS-Richtlinie hinsichtlich der Betreiber wesentlicher Dienste und auch Anbieter digitaler Dienste fremd.

Von den Möglichkeiten, überschießende Regelungen angesichts fehlender EU-Vorgaben wieder zu streichen, wurde kein Gebrauch gemacht. Dies führt dazu, dass die neuen Verpflichtungen der Anbieter digitaler Dienste nun auf ein teils bestelltes Feld treffen. Auf Grundlage der Definition digitaler Dienste in § 2 Absatz 9 BSiG-E ist festzustellen, dass die Anbieter digitaler Dienste stets auch Telemediendiensteanbieter und damit gemäß TMG verpflichtet sind. Die Pflichten des BSiG-E gelten dabei jedoch nur für juristische Personen, sowie nicht für Kleinstunternehmen und kleine Unternehmen. § 8d BSiG sieht für Anbieter digitaler Dienste keine Verwei-

sung auf ein bereichsspezifisches Gesetz (i. e. TMG) vor, wie es das BSIG für diverse KRITIS-Betreiber vorsieht. Angesichts der Tatsache, dass Anbieter digitaler Dienste immer auch Telemediendiensteanbieter sind, ist dies konsequent, da die Regelung des § 8c BSiG-E sonst leerliefe.

Bereits vor Umsetzung der NIS-Richtlinie war es für die Normverpflichteten des § 13 Absatz 7 TMG kaum valide zu ermitteln, welche Sicherheitsmaßnahmen sich aus den einzelnen Tatbestandsmerkmalen, die sich in den gleichzeitig eingeführten Pflichten für Betreiber kritischer Infrastrukturen nur teilweise wiederfanden, ergab. Soweit sie nun als Anbieter digitaler Inhalte gelten, werden diese Pflichten nun von den neuen Vorgaben des § 8c BSiG-E überlagert, die sich einer Terminologie bedienen, die sich sowohl von der des § 13 Abs. 7 TMG als auch von den parallelen Normen des BSiG unterscheidet.

Der Normverpflichtete sieht sich somit mehreren, sich teilweise überlagernden, mittels unklarer und in den Bereichsgesetzen abweichend formulierten Tatbestandsmerkmalen zu bestimmenden Sicherheitsverpflichtungen gegenüber, die er selbst kaum durchdringen, geschweige denn umsetzen können wird. Dieser Wildwuchs IT-sicherheitsgesetzlicher Regelungen ist der Steigerung des Schutzniveaus nicht förderlich.

Der Regelungskonflikt scheint dem Entwurfsgeber nicht aufgefallen zu sein, da in der Stellungnahme zum Umsetzungsbedarf für die betroffenen Unternehmen auf § 13 Abs. 7 TMG und den Unterschied zu den nach dieser Norm bereits verpflichtenden Sicherheitsmaßnahmen in keiner Weise eingegangen wird.

Aufgrund der verpflichtenden Vollharmonisierung müssen sich die Pflichten des § 13 Abs. 7 TMG im Rahmen des § 8c BSiG-E halten, zumindest soweit Anbieter digitaler Dienste betroffen sind. Aufgrund des wesentlich breiteren Kreises an Normverpflichteten dürften die Pflichten für Telemediendiensteanbieter tatsächlich auch geringere Sicherheitsanforderungen mit sich bringen als für die als zentral eingestuften Anbieter digitaler Inhalte. Vor diesem Hintergrund sollten die Terminologien beider Normen so angeglichen werden, dass sich ein abgleichbares Verpflichtungsbild ergibt. Nur so kann ein Normadressat leicht erkennen, dass bei Erfüllung seiner Pflichten nach § 8c BSiG-E automatisch auch die Pflichten § 13 Abs. 7 TMG erfüllt sind. Eine Abweichung von den Formulierungen der NIS-Richtlinie bietet sich vor dem Hintergrund der Vollharmonisierung nicht an. Zu lösen ist der beschriebene Konflikt somit über die entsprechende Anpassung des nationalen § 13 Abs.7 TMG.

Die Komplexität der konfligierenden Normen wird nicht zuletzt dadurch erhöht, dass die Datenschutzgrundverordnung ab dem 25.05.2018 eine Änderung des § 13 Absatz 7 TMG erfordert, die im Rahmen des vorgelegten Entwurfs sogleich hätte vorweggenommen werden können.

Der Regelungsgehalt des § 13 Abs. 7 TMG lässt sich ohne Weiteres mit den Anforderungen des § 8c BSiG-E erfassen. Die Normziele der TMG-Regelung sind die Sicherung gegen den unerlaubten Zugriff auf das Telemedienangebot, den Schutzes gegen Zugriffe auf personenbezogene Daten sowie gegen Störungen durch äußere Eingriffe. Diese Normziele lassen sich ohne Absenkung des Schutzniveaus unter die Verhinderung bzw. Minimierung von Sicherheitsvorfällen und deren Folgen im Sinne von § 8c BSIG-E fassen. Die Auswahl und Umsetzung der technischen und organisatorischen Maßnahmen im Rahmen der "wirtschaftlichen Zumutbarkeit" gemäß § 13 Abs. 7 TMG lässt sich gleichermaßen unter die im Rahmen der Verhältnismäßigkeit vorzunehmenden allgemeinen Zumutbarkeitsprüfung ziehen. Die "technische Möglichkeit" als eigenständiges Kriterium kann und sollte gestrichen werden, da ein vorwerfbarer Verstoß wegen unterlassener Maßnahmen, die subjektiv-technisch unmöglich sind.

Der Hinweis auf den zu berücksichtigenden "Stand der Technik" ist in beiden Normen inhaltsgleich enthalten. Aufgrund der rechtlichen und tatsächlichen Bedeutung dieses Verweisungsbegriffes wäre eine gesetzliche Definition nach wie vor wünschenswert und nützlich.

Ausdrücklich wird vorgeschlagen, die auseinanderfallenden behördlichen Zuständigkeiten aufzulösen: Für Anbieter digitaler Dienste wird das BSI zuständig werden, für die Umsetzung des § 13 Abs. 7 TMG ist je nach Verletzung von S. 1 Ziff. 1 und 2b) die Landesmedienaufsicht, bei Verletzungen von Ziff. 2a) die Landesdatenschutzbehörde zuständig. Hier sollte eine einheitliche Zuständigkeit des BSI geschaffen werden.

Ansprechpartner für Rückfragen:

RA Karsten U. Bartels LL.M.
Leiter der TeleTrusT-AG "Recht"
bartels@hk2.eu