Berlin, 16.03.2026

Stellungnahme

zum

BMI-Referentenentwurf eines Gesetzes zur Stärkung der Cyber-Sicherheit

Kontakt:
RA Karsten U. Bartels, LL.M.
HK2 Rechtsanwälte
Hausvogteiplatz 11 A
10117 Berlin
-
Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Stellvertretender Vorstandsvorsitzender
Leiter TeleTrusT-AG "IT-Sicherheitsrecht"
bartels@hk2.eu

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

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 breitgefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, 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 Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
https://www.teletrust.de

I. Einleitung

TeleTrusT begrüßt das Ziel des Referentenentwurfs, die Cyber-Sicherheit in Deutschland wirksam zu stärken und die staatliche Handlungsfähigkeit gegenüber schwerwiegenden Cyber-Gefahren zu verbessern. Angesichts der anhaltend hohen Bedrohungslage ist es richtig, die bestehenden Strukturen zur Detektion, Bewertung und Abwehr von Cyber-Gefahren fortzuentwickeln.

Cyber-Sicherheit ist nicht nur Aufgabe der potentiell betroffenen Einrichtungen. Entsprechende Eingriffsbefugnisse für den Staat als Akteur für Cyber-Sicherheit zu schaffen, kann sich als zeitgemäße und effektive Bereicherung eines holistisch verstandenen Cyber-Sicherheitsrechts erweisen. Dazu sind die Eingriffsbefugnisse jedenfalls punktuell, streng cyber-sicherheitsbezogen und technisch sinnvoll umsetzbar auszugestalten. Cyber-Sicherheitsrecht muss den Schutz von Staat, Gesellschaft und Wirtschaft erhöhen; es darf nicht durch unklare Befugnisse, unbestimmte Rechtsbegriffe oder zu geringe verfahrensrechtliche Begrenzungen das Potential missbräuchlicher staatlicher Eingriffe bergen.

Vor diesem Hintergrund erscheint der Referentenentwurf eines Gesetzes zur Stärkung der Cyber-Sicherheit ambivalent: Er enthält einerseits dringend benötigte Eingriffsbefugnisse für Bundespolizei sowie BKA und sieht punktuell sinnvolle Befugniserweiterungen für das BSI vor. Andererseits ermöglicht der Entwurf tiefgreifende Eingriffe in die Netzinfrastruktur selbst, die langfristig das Vertrauen von Unternehmen, Bürgerinnen und Bürgern in integre IT-Systeme signifikant schwächen können. Je tiefer staatliche Maßnahmen in IT-Systeme eingreifen können, desto höher sind die Anforderungen an Normenklarheit, technische Begrenzungen und Verfahrensvorschriften. Eingriffsbefugnisse stellen keinen Sicherheitsgewinn dar, wenn sie ihrerseits neue Angriffsflächen schaffen.

II. BSIG

TeleTrusT unterstützt grundsätzlich das Anliegen, dem BSI in einzelnen Bereichen frühzeitigere und operativ wirksamere Reaktionen auf Cyber-Gefahren zu ermöglichen. So ist der Vorschlag für die Änderungen des § 11 Abs. 1, 3 BSIG-E positiv hervorzuheben, wonach das BSI Maßnahmen nicht erst nach Eintritt einer Beeinträchtigung, sondern bereits bei Anhaltspunkten für deren Eintritt ergreifen und dementsprechend auch Daten verarbeiten kann. Auch die nach § 15 Abs. 6 BSIG-E geplante Pflicht für Anbieter öffentlich zugänglicher Telekommunikationsdienste und Anbieter von digitalen Diensten, dem BSI auf Anforderung Informationen mitzuteilen, die Rückschlüsse auf Cyber-Risiken erlauben, stellt in dem Zusammenhang eine punktuelle Verbesserung dar. Die Auskunftspflicht ist in Hinblick auf ihre technische Durchführbarkeit und wirtschaftliche Zumutbarkeit begrenzt. Wenngleich eine derartige Begrenzung in Anbetracht der ansonsten ausufernden Auskunftspflicht richtig ist, muss die Ausnahme dringend konkretisiert werden, damit betroffene Unternehmen sie auch nutzbar machen können. Ansonsten droht die Informationspflicht für IKT-Diensteanbieter auszuufern.

Ein Schwerpunkt des Gesetzesvorhabens ist die Bekämpfung maliziöser Domains. In §§ 16 Abs. 6, 16a BSIG-E werden DNS-Diensteanbieter, TLD Name Registries und Domain-Name-Registry-Dienstleistern besondere Pflichten auferlegt. Mittelgroße DNS-Diensteanbieter müssen nach § 16 Abs. 6 BSIG-E ihren Kunden einen besonderen DNS-basierten Schutz vor Angriffen in Verbindung mit risikobehafteten Domains bieten. Offen bleibt hier, wie sich diese gesonderte Pflicht zu den allgemeinen Risikomanagementpflichten verhält. Diesen unterliegen DNS-Diensteanbieter sogar größenunabhängig als besonders wichtige Einrichtung i. S. d. § 28 Abs. 1 S. 1 Nr. 2 Var. 3 BSIG. Damit könnte im Umkehrschluss gefolgert werden, dass DNS-basierte Schutzmaßnahmen gegenwärtig pauschal nicht unter § 30 Abs. 1 BSIG fallen würden, obwohl der Wortlaut des § 30 Abs. 1 BSIG dies als technische Maßnahme eindeutig zulassen - und wohl auch erfordern - würde.

§ 16a BSIG-E sieht die Befugnis des BSI vor, gegenüber TLD Name Registries und Domain-Name-Registry-Dienstleistern anzuordnen, dass diese Nameserver-Einträge einer Domain ändern oder neue Einträge hinzufügen müssen. Die Befugnis steht unter der Voraussetzung einer erheblichen Gefahr für Schutzgüter des § 16 Abs. 3 BSIG. Ferner steht die Pflicht erneut unter der Bedingung technischer Durchführbarkeit und wirtschaftlicher Zumutbarkeit. Insbesondere vor dem Hintergrund der Rechtsschutzverkürzung für betroffene Unternehmen

(Widerspruch und Anfechtungsklage sollen hier keine aufschiebende Wirkung entfalten können) und dem intensiven Eingriff in die Netzinfrastruktur durch das BSI ist auch hier eine Konkretisierung dieser Ausnahmeregelung unerlässlich. Die Pflicht des BSI, den oder die BfDI jährlich über die Gesamtzahl angeordneter Nameserverumleitungen zu unterrichten, ist grundsätzlich richtig, stellt aber ohne damit verbundene Evaluationspflichten keine ausreichende Kontrollmaßnahme dar.

TeleTrusT lehnt demgegenüber die in § 31 BSIG-E vorgesehene verpflichtende Anbindung von Systemen zur Angriffserkennung von Betreibern kritischer Anlagen an das BSI in der vorgeschlagenen Form ab. Bereits der behauptete Mehrwert der zusätzlichen Anbindung bleibt im Entwurf unklar. Es ist nicht hinreichend dargelegt, weshalb die bestehenden Melde-, Unterstützungs- und Kooperationsmechanismen nicht ausreichen sollen. Demgegenüber schafft jede weitere Schnittstelle in hochsensiblen IT- und OT-Umgebungen eine neue Angriffsfläche. Gerade bei KRITIS-Betreibern beruht das Schutzkonzept auch darauf, externe Anbindungen auf das zwingend erforderliche Maß zu reduzieren. Besonders problematisch ist in dieser Hinsicht, dass der Entwurf keinerlei tragfähiges Schutzkonzept für diese staatlich veranlasste Anbindung erkennen lässt. Es fehlt an hinreichend klaren gesetzlichen Vorgaben zur sicheren technischen Ausgestaltung und zum sicheren Betrieb der Verbindung. Der bloße Hinweis darauf, dass das BSI die Anforderungen an Anbindung und Ausleitung eigenständig festlegt und veröffentlicht, genügt insoweit nicht.

Hinzu kommt, dass die Kosten- und Haftungsfolgen im Entwurf unzureichend geklärt sind. Wenn durch die verpflichtende Anbindung Sicherheitslücken entstehen, Cyber-Angriffe erleichtert oder Betriebsstörungen verursacht werden, sind Schäden bei KRITIS-Betreibern nicht auszuschließen. Es darf nicht zulasten der Betreiber gehen, wenn eine staatlich angeordnete zusätzliche Anbindung selbst zum Risiko wird. Mindestens müssen die Implementierungs- und Betriebskosten vollständig vom Staat getragen und spezialgesetzliche Haftungsregelungen einschließlich einer Beweislastumkehr zugunsten betroffener Betreiber vorgesehen werden. Andernfalls droht, dass Schäden wirtschaftlich bei den KRITIS-Betreibern verbleiben, obwohl diese die risikobegründende Maßnahme nicht freiwillig geschaffen haben. Dies gilt umso mehr, als allgemeine Staatshaftungsansprüche in der Praxis häufig keine hinreichend effektive und rechtssichere Kompensation gewährleisten.
Im Ergebnis ist § 31 BSIG-E in seiner Konzeption nach diesem Referentenentwurf abzulehnen.

III. TDDDG

Als sinnvoll erachtet TeleTrusT die neuen Nutzerinformationspflichten in § 19 Abs. 5, 6 TDDDG-E. Hiermit kann die Reaktionsfähigkeit und damit die Resilienz auf Endnutzerseite gestärkt und das Schadensausmaß von Cyber-Vorfällen deutlich eingeschränkt werden. Einzig zu kritisieren ist auch hier die fehlende Konkretisierung der technischen Durchführbarkeit und wirtschaftlichen Zumutbarkeit.

IV. BPolG und BKAG

Der Großteil des Referentenentwurfs befasst sich mit einer Anpassung des BPolG und BKAG in Hinblick auf die neue Cyber-Gefahrenlage. TeleTrusT betrachtet diese Vorschriften nicht aus einer polizei- und ordnungsrechtlichen, sondern aus einer Cyber-Sicherheitsrechtlichen Perspektive. TeleTrusT steht dem Schaffen neuer Eingriffsbefugnisse für Bundespolizei und BKA im Cyber-Raum nur insoweit offen gegenüber, als diese strikt defensiv, technisch beherrschbar und rechtsstaatlich klar begrenzt ausgestaltet sind. Der vorliegende Entwurf geht darüber deutlich hinaus. Die Rechtsgrundlagen sehen mitunter drastische Möglichkeiten vor, in informationstechnische Systeme und Datenströme einzugreifen.

Vor diesem Hintergrund sind insbesondere § 41a BPolG-E und § 62e BKAG-E aus Sicht von TeleTrusT in ihrer Grundkonzeption verfehlt. Die dort angelegten Eingriffsmöglichkeiten einer aktiven Cyber-Abwehr beinhalten die Möglichkeit, Maßnahmen durchzuführen, die nicht nur gegen Angreifer-Infrastrukturen, sondern faktisch auch gegen kompromittierte Drittsysteme wirken können. Gerade im Cyber-Raum werden Angriffe regelmäßig über fremde, selbst angegriffene oder missbrauchte Systeme durchgeführt. Damit können Bundespolizei und

BKA solche Behörden, Unternehmen oder sonstigen Einrichtungen adressieren, die selbst Opfer eines Cyber-Angriffs geworden sind.

Die Vorstellung, "aktive Cyber-Abwehr" könne in komplexen realen Angriffsszenarien trennscharf und ohne gravierende Nebenfolgen erfolgen, überzeugt nicht. Werden Maßnahmen ohne Wissen der Betreiber angegriffener oder manipulierter Systeme durchgeführt, können die tatsächlichen Systemzustände und die Folgen des Eingriffs regelmäßig nicht hinreichend verlässlich beurteilt werden. Gerade das für eine sichere Durchführung erforderliche betriebs- und systemspezifische Wissen über Abhängigkeiten, Redundanzen und mögliche Kaskadeneffekte liegt typischerweise nur bei den betroffenen Betreibern selbst vor. Das ist insbesondere bei kritischen oder hochverfügbaren Infrastrukturen risikobehaftet. Schon geringfügige Fehlannahmen können erhebliche Betriebsstörungen, Datenverluste oder sogar flächendeckende Versorgungsausfälle verursachen. Die in § 41a BPolG-E und § 62e BKAG vorgesehenen Befugnisse schaffen damit neue Angriffsflächen, neue Missbrauchsmöglichkeiten und das Risiko unschätzbarer Kollateralschäden.

Dass die Normen die Rückgängigmachung von Datenveränderungen vorsehen und eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung geschützt werden müssen, beseitigt diese Grundprobleme nicht. Die entscheidende Schwäche liegt nicht nur in der technischen Absicherung der eingesetzten Mittel, sondern bereits in der Unbeherrschbarkeit des Eingriffs in fremde, vernetzte und häufig nicht eindeutig zuordnungsfähige Systemumgebungen. Aus Sicht von TeleTrusT sollten diese Befugnisse in ihrer derzeitigen Konzeption nicht weiterverfolgt werden.

Die cyber-sicherheitsbezogenen Rechtsgrundlagen der §§ 62b - 62g BKAG-E sind eng verknüpft mit der Aufgabenzuweisungsnorm des § 3a BKAG-E. Hiernach nimmt das BKA die Aufgabe der Gefahrenabwehr gegen Angriffe auf die IT-Sicherheit wahr bei schwerwiegenden Fällen mit internationaler Abhängigkeit sowie Fällen mit außen- und sicherheitspolitischer Bedeutung. Während Gefahren durch Angriffe auf die IT-Sicherheit in § 3a Abs. 2 BKAG-E und schwerwiegende Fälle in § 3a Abs. 3 BKAG-E definiert werden, fehlt es in Bezug auf "Fälle mit außen- und sicherheitspolitischer Bedeutung" an einer ausreichenden Konkretisierung. Die Möglichkeit der Auswirkung auf die "Stellung der Bundesrepublik Deutschland in der Staatengemeinschaft" ist ebenfalls sehr weit gefasst und als Konturierung der Eingriffsvoraussetzung daher ungeeignet. Damit droht eine uferlose Ausweitung der Ermächtigungsgrundlagen. Gerade vor dem Hintergrund gegenwärtiger hybrider Kriegsführung sind wirksame Maßnahmen zur Abwehr von cyber-sicherheitsbezogenen Angriffen auf die Stellung der Bundesrepublik Deutschland wichtig - sie dürfen jedoch nicht zu einem Blankocheck für intensive Eingriffe in die Netz- und IT-Infrastruktur werden.

Hinsichtlich der Aufgabenzuweisungsvorschrift des § 3a BKAG-E und den damit zusammenhängenden Eingriffsbefugnissen der §§ 62b - 62g BKAG-E sowie auch hinsichtlich des § 41a BPolG treten erhebliche verfassungsrechtliche Bedenken hinzu. Diese Normen verschieben operative Zuständigkeiten im Bereich der Cyber-Gefahrenabwehr in substanziellem Umfang auf Bundesbehörden. Ob und inwieweit diese Kompetenzverlagerung mit der verfassungsrechtlichen Kompetenzordnung vereinbar ist, wird im Entwurf nicht hinreichend klar beantwortet. Gerade bei tiefgreifenden Eingriffsbefugnissen gegenüber informationstechnischen Systemen muss der Gesetzgeber die verfassungsrechtliche Zulässigkeit ausdrücklich und klar darlegen.

V. Fazit

Im Ergebnis unterstützt TeleTrusT das Anliegen des Referentenentwurfs, die Cyber-Sicherheit in Deutschland wirksamer zu schützen und die Reaktionsfähigkeit staatlicher Stellen gegenüber Cyber-Gefahren und -angriffen zu verbessern.

Aus Sicht von TeleTrusT geht der Entwurf in zentralen Punkten jedoch in die falsche Richtung. Insbesondere die vorgesehene Neugestaltung des § 31 BSIG-E überzeugt nicht. Eine staatlich veranlasste zusätzliche Anbindung kritischer Systeme an das BSI ohne klar begrenzten Mehrwert, ohne hinreichendes Schutzkonzept und ohne tragfähige Kosten- und Haftungsregelungen stärkt die Cyber-Sicherheit nicht, sondern schafft neue Risiken für KRITIS-Betreiber.

Ebenso sind die in § 41a BPolG-E und § 62e BKAG-E angelegten Möglichkeiten einer "aktiven Cyber-Abwehr" abzulehnen. Sie eröffnen die Gefahr, dass Bundesbehörden über kompromittierte Drittsysteme gerade solche Stellen in Anspruch nehmen oder beeinträchtigen, die selbst Opfer eines Cyber-Angriffs sind. Dadurch entstehen neue Angriffsflächen, neue Missbrauchsmöglichkeiten und potentiell erhebliche Kollateralschäden.

Schließlich wirft der Entwurf verfassungsrechtliche Fragen auf, insbesondere hinsichtlich der Kompetenzordnung und der Verlagerung operativer Cyber-Befugnisse auf Bundesebene. Diese Fragen müssen im weiteren Gesetzgebungsverfahren eindeutig beantwortet werden.

Im Ergebnis muss das Cyber-Sicherheitsniveau bundesweit gestärkt werden. Dieses Ziel wird aber nicht schon dadurch erreicht, dass zusätzliche Eingriffsbefugnisse geschaffen werden. Entscheidend ist vielmehr, dass staatliche Maßnahmen selbst keine neuen Unsicherheiten erzeugen und das Vertrauen in die Integrität informationstechnischer Systeme nicht schwächen.