* Stellungnahme

zum Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0)

(Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat vom ###)

Berlin, XXX

1. **Einleitung**

Der Verband kommunaler Unternehmen (VKU) vertritt rund 1.460 kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Bei der überwiegenden Zahl der von uns vertretenen Unternehmen handelt es sich um Betreiber von Kritischen Infrastrukturen. Aus diesem Grund sind unsere Mitglieder ganz besonders von der IT-Sicherheitsgesetz 2.0 betroffen.

Erstmals soll auch die Entsorgungswirtschaft in den Anwendungsbereich der Kritischen Infrastrukturen aufgenommen werden (§2 Abs. 10 BSIG-E). Da die Auswirkungen auf unsere Mitgliedsunternehmen ganz maßgeblich von den entsprechenden Schwellenwerten in der noch zu überarbeitenden BSI-Kritisverordnung abhängig sein wird, können an dieser Stelle nur wenige Ausführungen gemacht werden. Wichtig ist hierbei allerdings, dass die entsprechenden Verbände bei der Überarbeitung der BSI-Kritisverordnung frühzeitig mit eingebunden werden und dass kleine und mittelständische Entsorgungsunternehmen nicht durch ein Übermaß an Regulierung benachteiligt werden.

Ferner werden im IT-Sicherheitsgesetz 2.0 Regelungen zu Systemen zur Angriffserkennung eingefügt (§8a Abs. 1a, 2 BSIG-E). Hierbei ist anzumerken, dass eine Verpflichtung zum Aufbau solcher Systeme nicht sinnvoll ist und entsprechende Vorgaben dieser Systeme mit den Branchenverbänden zusammen erarbeitet werden sollten. Auch die regelmäßigen und umfangreichen Meldepflichten an eine Vielzahl von verschiedenen Stellen sollten überdacht werden.

Was genau mit der Vertrauenswürdigkeitserklärung der Hersteller von KRITIS-Kernkomponenten (§ 8a Abs. 6 BSIG-E) erreicht werden soll ist unklar. Auch der Anwendungsbereich der Norm ist extrem weit gefasst. Ferner stellen sich eine Vielzahl von Anschlussproblemen, die im Gesetzesentwurf nicht adressiert werden. Vor diesem Hintergrund sollte diese Norm gestrichen werden oder zumindest deutlich enger und eindeutiger gefasst werden.

Der Adressat der Anordnungsbefugnis im Rahmen der Cyberkritikalität (§8g BSIG-E) ist unklar und die Norm auch im Übrigen zu weit gefasst. Hier muss nachgeschärft werden.

1. **Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)**

1. § 2 Abs. 10 BSIG-E (Aufnahme des Sektors Entsorgung in die Definition der Kritischen Infrastrukturen)

Durch den Neugefassten § 2 Abs. 10 Nr. 1 BSIG-E wird nun erstmals auch die Entsorgungswirtschaft Adressat des BSIG. Dies ist aus unserer Sicht prinzipiell sachgerecht, da auch die Entsorgungswirtschaft von hoher Bedeutung für das Funktionieren des Gemeinwesens ist.

Bei der Einbeziehung des Sektors Entsorgung in den Begriff der Kritischen Infrastrukturen muss jedoch eine finanzielle, bürokratische und personelle Überforderung des Mittelstands vermieden werden. Entscheidend hierfür wird die sich anschließende Novelle der BSI-Kritisverordnung sein (vgl. § 2 Abs. 10 S. 2 BSIG-E i.V.m. § 10 Abs. 1 BSIG-E). Hierbei sollten die entsprechenden Verbände so früh wie möglich eingebunden werden, denn nur so kann die Betroffenheit von Unternehmen realistisch eingeschätzt werden.

Wir gehen davon aus, dass die Entsorgungsunternehmen die Anforderungen aus dem BSIG-E / BSI-Kritisverordnung erst zwei Jahre nach Verabschiedung der entsprechenden Regelungen in der BSI-Kritisverordnung einhalten müssen (vgl. §8a Abs. 1 BSIG-E). Eine Klarstellung in der Gesetzesbegründung wäre für die Rechtssicherheit hier hilfreich. Auf diese Weise können angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse in den Unternehmen abgestimmt, implementiert und/oder weiterentwickelt werden. Seitens der Unternehmen und Verbände können in dieser Zeit branchenspezifische Sicherheitsstandards entwickelt und dem BSI vorgeschlagen werden.

2. § 5b Abs. 1 BSIG-E (Wiederherstellung der Sicherheit oder Funktionsfähigkeit Informationstechnischer Systeme in herausgehobenen Fällen)

Aus dem bisherigen § 5a BSIG soll § 5b BSIG-E werden und insbesondere der Absatz 1 neu gefasst werden. Wir schlagen folgende Änderung in § 5b Abs. 1 BSIG-E vor:

 *„(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Betreibers einer weiteren Anlage im besonderen öffentlichen Interesse um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter“*

Die vorgeschlagenen Änderungen an §5b Abs. 1 finden sich schon bisher wortgleich in §5a Abs. 1 wieder. Diese Passage wurde im Referentenentwurf entfernt.

Nach der wieder eingefügten Passage erhebt das BSI bei ersten Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebs vor Ort keine Gebühren oder Auslagen für die Tätigkeit des BSI selbst. Eine Unterstützung des BSI sollte weiterhin nicht verrechnet werden, da die Kosten des BSI für die Unternehmen nicht kalkulierbar sind im Gegensatz zur Unterstützung durch Dienstleister.

6. §8a Abs. 1a, 2 BSIG-E (Sicherheit in der Informationstechnik Kritischer Infrastrukturen)

1. Verpflichtung zu Systemen zur Angriffserkennung nach Festlegung einer Technischen Richtlinie durch das BSI

Mit dem neu eingefügten §8a Abs. 1a BSIG-E wird festgelegt, dass zu den angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen auch der Einsatz von Systemen zur Angriffserkennung gehört. Die Ausgestaltung soll durch das BSI in einer Technischen Richtlinie festgelegt werden. Dies lehnen wir in dieser Form ab und schlagen dagegen folgende Formulierung vor:

*„(1a) Die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, können ~~umfasst~~ auch den Einsatz von Systemen zur Angriffserkennung umfassen. […]. ~~Die Ausgestaltung des Einsatzes von Systemen zur Angriffserkennung legt das Bundesamt in einer Technischen Richtlinie fest. Hierzu muss die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit angehört werden.~~ […].*

*(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt*

*1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,*

*2.im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.*

*Dieses gilt entsprechend für die Ausgestaltung des Einsatzes von Systemen zur Angriffserkennung nach Absatz 1a, wobei zusätzlich die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit angehört wird.“*

Eine Festlegung der Systeme zur Angriffserkennung ohne Beteiligung der Branchenverbände ist schon deshalb nicht sinnvoll, weil nur die Unternehmen selber ihre IT-Landschaft genau genug kennen, um sinnvolle Systeme zur Angriffserkennung zu erarbeiten. Ggf. haben die Unternehmen bereits so stark in präventive Maßnahmen investiert, dass aus ihrer Sicht eine Detektion kaum noch risikominimierende Auswirkungen hat. Dies muss jedes Unternehmen in den regelmäßig durchzuführenden Risikoanalysen für sich bewerten. Der Stand der Technik wird von Auditoren überprüft (vgl. §8a Abs. 3 BSIG-E), so dass eine Festlegung im Gesetz wenig sinnvoll erscheint.

Ebenfalls ist eine technische Richtlinie für die Ausgestaltung des Einsatzes von Systemen zur Angriffserkennung nicht sinnvoll. Ein solches System sollte an die individuellen Bedürfnisse der Unternehmen angepasst werden, um die bestmögliche Detektion leisten zu können. Die Bindung an die technische Richtlinie könnte somit dazu führen, dass weniger Angriffe erkannt werden. Überdies ist bisher nicht definiert, wann die technischen Richtlinien erstmals anzuwenden wären.

Aus diesem Grund sollte die Ausgestaltung der Angriffserkennung vornehmlich von den Branchenverbänden erarbeitet und dem BSI im Anschluss vorgeschlagen werden. Das BSI kann sodann auf Antrag feststellen, ob die so erarbeiteten Regeln den Anforderungen nach §8a Abs.1a genügen. Dieses Vorgehen entspricht dem bisherigen Vorgehen in Bezug auf die sonstigen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen (vgl. §8a Abs. 2 mit Verweis auf §8 Abs. 1 BSIG-E) und hat sich auch in der Praxis bewährt. Dieser kooperative Ansatz (siehe BT-Drs. 18/4096, S. 26) sollte auch hier beibehalten werden. Insbesondere muss es auch wie bisher möglich sein, dass selbst bei einer Erarbeitung von branchenspezifischen Sicherheitsstandarts es einem einzelnen Betreiber weiterhin offensteht, abweichend davon auch eigene den Stand der Technik berücksichtigende Maßnahmen umzusetzen (siehe BT-Drs. 18/4096, S. 26).

1. Vierteljährliche Meldung von Maßnahmen nach §8a Abs. 1a S. 1 BSIG-E

Weiter heißt es in §8a Abs. 1a S. 7 BSIG-E:

*„[…] Die Betreiber Kritischer Infrastrukturen müssen der oder dem betrieblichen Datenschutzbeauftragten, dem Bundesamt, der jeweiligen Aufsichtsbehörde und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 1 in diesem Zeitraum schriftlich berichten.“*

Zunächst wird somit eine Benachrichtigungspflicht an eine interne Stelle (den betrieblichen Datenschutzbeauftragten) und eine nicht ganz klare Anzahl von externen Stellen definiert (BSI, jeweilige Aufsichtsbehörde und/oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit) geschaffen. Dies ist nicht zielgerecht und wird deshalb in dieser Form abgelehnt. So sind parallele Meldewege nicht effizient und bedeuten für die Unternehmen einen nicht zu vernachlässigenden Mehraufwand. Deutlich effizienter wäre es, hier eine zentrale und eindeutig bestimmte Stelle für die Meldung zu schaffen. Von ihr aus sollten die Meldung dann an die jeweils zuständigen Stellen der öffentlichen Verwaltung intern weitergeleitet werden. Durch ein solches Verfahren können auch keine Unsicherheiten auftreten, an wen die Meldung durch das Unternehmen gegeben werden muss. Hinzuweisen ist hierbei auf §8b Abs. 1 BSIG-E, wonach das BSI die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik ist.

Weiterhin wird nach dem Gesetzeswortlaut nicht klar, worüber Meldung gegeben werden soll. Durch den Verweis auf § 8a Abs. 1a S. 1 BSIG-E liegt das Verständnis nahe, dass nur erkannte Angriffe die durch den Einsatz von Systemen zur Angriffserkennung erkannt wurden, gemeldet werden sollen. Möglich wäre aber auch eine Interpretation, dass auch nur der Einsatz von Systemen der Angriffserkennung als solcher bereits gemeldet werden muss. Hier sollte zumindest in der Gesetzesbegründung eine Klarstellung erfolgen.

Ebenfalls abgelehnt wird die anlassunabhängige, vierteljährliche Pflicht zur Meldung. Deutlich effizienter ist es hier, eine anlassbezogene Meldepflicht zu verankern. Eine solche anlassbezogene Meldepflicht entlastet nicht nur die Unternehmen, sondern auch die zuständigen Aufsichtsbehörden. Im Übrigen sind die regelmäßigen Meldepflichten nach § 8a Abs. 3 BSIG-E ausreichend. Anzumerken ist zudem, dass die Betriebs- und Geschäftsgeheimnisse der Unternehmen bei einer entsprechenden Meldung hinreichend geschützt werden müssen.

7. §8a Abs. 6 BSIG-E (Sicherheit in der Informationstechnik Kritischer Infrastrukturen)

§8a Abs. 6 BSIG-E lautet wie folgt:

*„(6) KRITIS-Kernkomponenten dürfen nur von solchen Herstellern bezogen werden, die vor dem erstmaligen Einsatz der Komponenten eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgeben haben (Vertrauenswürdigkeitserklärung). Diese Verpflichtung erstreckt sich auf die gesamte Lieferkette des Herstellers. Das Bundesministerium des Innern, für Bau und Heimat erlässt die Mindestanforderungen für die Vertrauenswürdigkeitserklärung durch Allgemeinverfügung, die im Bundesanzeiger bekannt zu machen ist. Diese Verpflichtung gilt ab der Bekanntmachung der Allgemeinverfügung nach Satz 3.“*

Zunächst ist dem VKU bisher nicht klar, was genau mit der Vertrauenswürdigkeitserklärung erreicht werden soll. Ob die Abgabe der Vertraulichkeitserklärung den Tatsachen entspricht wird für die Betreiber der Kritischen Infrastrukturen nicht nachprüfbar sein. Die Betreiber der Kritischen Infrastrukturen könnten nur überprüfen, ob die Hersteller die Erklärung (nach der noch zu erlassenden Allgemeinverfügung) formell richtig abgegeben haben. Auch hier wird kein Mehrwert deutlich, denn warum sollte jeder Betreiber der Kritischen Infrastrukturen dies jeweils einzeln für sich prüfen? Die Frage wird sich für alle Betreiber von Kritischen Infrastrukturen gleichermaßen stellen.

Überdies ist der Anwendungsbereich durch die fast uferlose Weite des Begriffs der KRITIS-Kernkomponenten unklar. Nach § 2 Abs. 13 BSIG-E sind KRITIS-Kernkomponenten IT-Produkte, die zum Betrieb von Kritischen Infrastrukturen dienen und für diese Zweck besonders entwickelt oder geändert werden. IT-Produkte sind Softwareprodukte sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte und Hardwarekomponenten, inklusive der zur einwandfreien Funktion eingesetzten Software (§2 Abs. 9a BSIG-E). Unter diese Definition könnte man beispielsweise fast jeden Computer fassen, der in einem Kraftwerk verwendet wird. Auf diesem wird zumindest eine extra angepasste Software installiert sein, die mit dem Betrieb des Kraftwerks (und somit zum Betrieb einer Anlage zur Stromversorgung) in Verbindung steht.

Vor diesem Hintergrund sollte darüber nachgedacht werden diese Norm gänzlich zu streichen

Wenn an einer Vertraulichkeitsprüfung festgehalten werden soll, so sind weitere Punkte zu beachten:

Zum einen fehlt jede Regelung für bestehende Systeme. Müssen hier nachträglich entsprechende Vertrauenswürdigkeitserklärungen der Hersteller eingeholt werden? Wenn ja in welcher Zeit und was ist die Folge, wenn eine solche Erklärung nicht abgegeben wird? Wird ein bestehendes System zu einem neuen System, wenn Komponenten ausgetauscht werden oder ein Softwareupdate durchgeführt wird? Wird der Betreiber eine Kritischen Infrastruktur zu einem Hersteller, wenn er selbstgeschriebene Software auf einem Computer laufen lässt?

Auch bei dem erstmaligen Einsatz stellen sich sehr viele nicht aufgegriffenen Folgefragen: Muss der Hersteller seine Vertrauenswürdigkeitsprüfung auch materiell nachweisen? Wenn ja gegenüber wem (dem BSI? dem Betreiber?). Was sind die Folgen / die Haftungsverteilung, wenn ein Betreiber eine Komponente einbaut und die Vertrauenswürdigkeitserklärung später (z.B. vom BSI) als nicht ausreichend erachtet wird.

An dieser Stelle sollte der Gesetzesentwurf deutlich nachgeschärft werden und hierzu in einen intensiven Austausch mit den beteiligten Stakeholdern getreten werden.

Nicht aus dem Blick verloren werden sollte ferner der enorme Aufwand für die Hersteller um ihre gesamte Lieferkette ihrerseits mit Vertraulichkeitserklärungen abzusichern. Es wird Teile von KRITIS-Kernkomponenten geben, die über eine lange Lieferkette geliefert werden. Wenn dies wiederum für eine Vielzahl von Teilen zutrifft, potenziert sich hier der Aufwand noch einmal. Es steht zu befürchten, dass einen solchen Nachweisaufwand nur durch weniger Hersteller erbracht werden kann, sodass die Betreiber von wenigen Herstellern abhängig wären. Dies würde sicherlich nicht förderlich für den Preiswettbewerb sein und ganz unabhängig davon zu einer veränderten Risikolandschaft bei dem Bezug von Komponenten führen. Dies sollte insbesondere mit den Herstellern intensiv diskutiert werden.

8. § 8g Abs.1 BSIG-E (Cyberkritikalität)

§8g BSIG-E lautet wie folgt:

*„(1) Das Bundesamt kann im Einzelfall Betreibern von Anlagen die Pflichten nach §§ 8a und 8b auch auferlegen, wenn*

*1. die betriebenen Anlagen oder Teile davon den Sektoren oder Bereichen nach § 2 Absatz 10 Satz 1 Nummer 1 sowie § 2 Absatz 13 Nummer 2 oder 3 zuzuordnen sind und*

*2. die Voraussetzungen des § 2 Absatz 10 Nummer 2 sowie § 2 Absatz 14 Nummer 1, 2 oder 3 im Übrigen nicht vorliegen, aber Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, insbesondere wegen des hohen Grades an Vernetzung der eingesetzten Informationstechnik, zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der betroffenen Dienstleistung insgesamt führen würden (Cyberkritikalität).*

*(2) Das Bundesamt kann im Einzelfall einem Unternehmen die Pflichten nach §§ 8a und 8b auferlegen, wenn eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse dieses Unternehmens zu einer tatsächlichen und hinreichend schweren Gefährdung für ein Grundinteresse der Gesellschaft führen würde.*

*(3) Das Bundesamt hat bei der Auferlegung der Pflichten dem Adressaten nach Absatz 1 und 2 mitzuteilen, ab wann die Pflichten nach §§ 8a und 8b gelten. Die Frist darf ein Jahr nicht unterschreiten.“*

Diese Norm wird in dieser Form ablehnt, weil sie zu unbestimmt ist und die Gefahr besteht, dass durch unklare Formulierung faktisch eine Öffnungsklausel für weitreichende Verpflichtungen gegenüber Unternehmen geschaffen werden, die keine Kritischen Infrastrukturen betreiben.

1. Adressat des §8g Abs. 1 BSIG-E unklar

Zunächst ist der Adressat aus §8g Abs. 1 BSIG-E unklar. Laut §8g Abs. 1 Nr. 1 BSIG-E soll es sich um Betreiber von Anlagen handeln, wenn die betriebenen Anlagen oder Teile davon den Sektoren oder Bereichen nach § 2 Absatz 10 Satz 1 Nummer 1 sowie § 2 Absatz 13 Nummer 2 oder 3 zuzuordnen sind. Hierbei ist unklar, ob die Voraussetzungen nach § 2 Abs. 10 Satz 1 Nummer 1 kumulativ oder alternativ zu § 2 Abs. 13 Nummer 2 oder 3 erfüllt sein müssen. Aus beiden Varianten ergeben sich Widersprüche:

Müssen diese Tatbestandsmerkmale nur alternativ erfüllt sein, so stellt sich die Frage, warum dies nötig ist. Beide Normen legen die maßgeblichen Sektoren fest, wobei §2 Abs. 10 Nr. 1 alle genannten Sektoren in § 2 Abs. 13 Nr. 2 und 3 umfasst (sowie weitere Sektoren nennt). Sind die Tatbestandsmerkmale nur alternativ zu erfüllen, würde die Erfüllung eines Sektors aus § 2 Abs. 13 Nr. 2 und 3 dazu führen, dass immer auch ein Sektor aus § 2 Abs. 10 S. 1 Nr. 1 BSIG-E erfüllt ist.

Müssen die Tatbestandsmerkmale kumulativ erfüllt sein, so ist dies ebenfalls überflüssig. Falls ein Fall des § 2 Abs. 13 Nr. 2 und 3 BSIG-E vorliegt, ist immer auch § 2 Abs. 10 S. 1 Nr. 1 BSIG-E erfüllt.

Möglich wäre es auch den Verweis auf § 2 Abs. 13 Nr. 2 und 3 BSIG-E so zu verstehen, dass es sich um keinen Verweis auf die dort genannten Sektoren handelt, sondern ein Verweis auf die IT-Produkte in diesem Bereich.

Diese Unklarheit wird durch die kumulative Verknüpfung von §8g Abs. 1 Nr. 1 BSIG-E mit §8g Abs. 1 Nr. 2 BSIG-E verstärkt. Danach sollen zunächst im Übrigen die Voraussetzungen des § 2 Absatz 10 Nummer 2 BSIG-E sowie § 2 Absatz 14 Nummer 1, 2 oder 3 BSIG-E nicht vorliegen dürfen. Auch hier stellt sich die Frage, ob es sich um alternative oder kumulative Verknüpfung der Tatbestandsmerkmale handelt. Es sei jedoch darauf hingewiesen, dass der Verweis auf § 2 Abs. 14 Nr. 1, 2 oder 3 BSIG-E hier unlogisch ist, da in §8g Abs. 1 Nr. 1 BSIG-E kein Verweis auf § 2 Abs. 14 BSIG-E stattgefunden hat. Es kann nur vermutet werden, dass auf Grund eines Redaktionsversehens in §8g Abs. 1 Nr. 1 BSIG-E ein Verweis auf § 2 Abs. 14 BSIG-E stattfinden sollte und nicht § 2 Abs. 13 BSIG-E.

1. Norm auch im Übrigen zu weit gefasst

Selbst wenn der Adressat klar bestimmt wäre, so ist die Norm insgesamt zu unbestimmt gefasst, womit sie einen fast unbegrenzten Anwendungsbereich hat.

Gemünzt auf die Betreiber von Anlagen in den Sektoren des § 2 Abs. 10 S. Nr. 1 BSIG-E bedeutet dies, dass es sich nicht mehr um Anlagen von hoher Bedeutung für das Funktionieren des Gemeinwesens handeln muss, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (siehe § 2 Abs. 10 S. 1 Nr. 2 BSIG-E i.V.m. der Kritis-VO). Vielmehr soll es ausreichen, dass Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, insbesondere wegen des hohen Grades an Vernetzung der eingesetzten Informationstechnik, zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der betroffenen Dienstleistung insgesamt führen würden (§8g Abs. 1 Nr. 2 BSIG-E). Wenn man die Norm ernst nimmt, so würde dies auf jedes Unternehmen in dem genannten Sektor zutreffen. Inzwischen sind wohl alle Unternehmen rein tatsächlich so sehr auf ihre IT angewiesen, dass sie bei einem Ausfall faktisch ihre Dienstleistungen nicht mehr erbringen können. Dies dürfte im Übrigen auch für jede Behörde gelten. Hier braucht es einer deutlichen Nachschärfung, da durch diese Regelung die fein austarierten Grenzwerte aus der KRITS-Verordnung faktisch ausgehebelt werden. Im Übrigen stellt sich die Frage, wie weit die Anordnungsbefugnis geht, wenn in einem Konzern gewisse Untergesellschaften in den genannten Sektoren tätig sind, während es andere Konzerngesellschaften nicht sind.

1. Verhältnis von § 8g Abs. 2 BSIG-E zu § 8g Abs. 1 BSIG-E

Zu § 8g Abs. 2 BSIG-E lässt sich festhalten, dass hier die Anordnungsbefugnis auf jedes beliebige Unternehmen ausgedehnt werden kann, wenn anderenfalls eine schwere Gefährdung für die Grundinteressen der Gesellschaft bestehen. Hier stellt sich zumindest für die Unternehmen des VKU die Frage, wie das Verhältnis von §8g Abs. 2 BSIG-E zu §8g Abs. 1 BSIG-E zu verstehen ist. Wir gehen davon aus, dass es sich bei §8g Abs. 1 BSIG-E um die speziellere Norm in Verhältnis zu §8g Abs. 2 BSIG-E handelt, sodass für die Sektorenunternehmen nur Anordnungen nach §8g Abs. 1 BSIG-E ergriffen werden können. Hier ist eine Klarstellung nötig.

5. §8h BSIG-E (Hersteller von IT-Produkten)

§8h BSIG-E betrifft Hersteller von IT-Produkten. Ob hier ggf. auch Betreiber von Kritischen Infrastrukturen herunterfallen, die selber IT-Produkte herstellen (s.o. bei §8a Abs. 1a, 2 BSIG-E) ist offen. Unabhängig davon begegnet die Norm aber auch ganz praktischen Problemen: So ist durch die sehr weite Definition des Begriffs IT-Produkt (s.o. bei §8a Abs. 6 BSIG-E) fast jeder Hard- oder Softwarehersteller vom Ansatz her betroffen. Ob dessen Komponenten in irgendeiner Weise im KRITIS-Umfeld eingesetzt wird, kann der Hersteller von IT-Produkten nicht zwangsläufig wissen. Hier sollte gesetzlich nachgeschärft werden und der Anwendungsbereich für den Hersteller sinnvoll eingegrenzt werden. Insbesondere eine enge Einbindung der Hersteller in den Gesetzgebungsprozess ist dringend angezeigt.

6. § 9a BSIG-E (Freiwilliges IT-Sicherheitskennzeichen)

Mit dem §9a BSIG-E werden die Voraussetzungen geschaffen, um ein deutsches (freiwilliges) IT-Sicherheitskennzeichen einzuführen. Hierzu ist zunächst anzumerken, dass mit der Verordnung des Europäischen Parlaments und des Rates über die ENISA Agentur der Europäischen Union für die Cybersicherheit und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013), der am 12. März 2019 vom Europäischen Parlament und am 9. April 2019 vom Ministerrat offiziell angenommen wurde, die Voraussetzungen für einheitliche und europaweite Cybersecurity-Kennzeichen geschaffen wurden. Nach Art. 57 und Erwägungsgrund 94 werden nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen unwirksam. Insoweit fehlen Ausführungen, wie sich in diesem Zusammenhang noch eine nationale Gesetzgebungskompetenz begründet.

Unabhängig davon sollte auf nationale Kennzeichen auch schon deshalb verzichtet werden, da Verbraucher bzw. Käufer von IT-Produkten verwirrt werden, wenn es eine Vielzahl unterschiedlicher Zertifizierungen und Sicherheitskennzeichen gibt.

Sollte eine Rechtsverordnung „IT-Sicherheitskennzeichen“ (vgl. § 9a Abs. 1, 10 Abs.2a BSIG-E) verabschiedet werden, so muss dies im Dialog mit den KRITIS-Betreiber und Hersteller geschehen. Eine Einbindung der UP KRITIS sollte erfolgen.

1. **Änderungen des Telekommunikationsgesetzes (TKG)**
2. § 109 Abs. 2a TKG-E

Nach der Gesetzesbegründung konkretisiert dieser Absatz die Verpflichtung der Diensteanbieter, Schutzmaßnahmen zu treffen und entspricht der Ergänzung in §8a Abs. 1a BSIG-E. Der Entwurf wird in dieser Form abgelehnt.

Um Wiederholungen zu vermeiden, wird zunächst auf die Stellungnahme zu §8a Abs. 1a BSIG-E (s.o.) verwiesen. Ergänzend sei angemerkt, dass in § 109 Abs.2a TKG-E im Vergleich zu §8a Abs. 1a BSIG-E eine weitere Pflicht eingeführt werden soll:

*„[…] Daten, die für die Aufklärung des Angriffs, den Schutz der Informationstechnik und die Strafverfolgung der Angreifer erforderlich sind, haben die Diensteanbieter von sich aus und auf Anforderung den dazu zuständigen Behörden zu übermitteln. […]“*

Hier wird somit mindestens eine weitere Mitteilungspflicht festgelegt (es sind nun minimal 4 verschiedene Stellen, an die Vorfälle gemeldet werden sollen). Eine solche Vielzahl von verschiedenen Mitteilungspflichten ist unnötig und verursacht nur unnötigen Aufwand. Abgesehen davon ist nicht klar, an wen die Diensteanbieter die Daten übermitteln sollen.

Es wird im Übrigen darauf hingewiesen, dass § 109 TKG im Moment im Rahmen der Umsetzung des Europäischen Kodex für die elektronische Kommunikation (Richtlinie (EU) 2018/1972) überarbeitet wird. Es wird darum um eine Abstimmung mit den jeweils zuständigen Ressorts vorzunehmen, damit eine konsistente Regulierung erfolgt und Doppelarbeiten vermieden werden.

1. § 109a TKG-E

In Bezug auf § 109a Abs. 4 TKG-E ist anzumerken, dass kundenfreundliche Provider die Nutzer bereits jetzt auf Gefahren hinweisen. Allerdings ist der Erfolg einer solches Hinweises bisher überschaubar, sodass eine Regulierung aus unserer Sicht nicht erforderlich ist.

Hinzuweisen ist zudem, dass für kleine Provider die zusätzlichen wirtschaftlichen Aufwände für Schnittstellen, sofortige Maßnahmen, Kommunikationsprozesse, Kontaktstellen etc. verhältnismäßig höher als für die großen Provider. Diese unterhalten eigene Abteilungen für diese Themen. Es sollte deshalb darauf geachtet werden, dass eine Regulierung kleine Provider nicht überfordert und somit die Vielfalt der Anbieter auf dem Markt durch Überregulierung zerstört. Es sollten deshalb für kleinere Provider gesetzliche Erleichterungen in dieser Hinsicht vorgesehen werden.

XXXXXXXXXX

XXXXXXXX