bitkom

Auf einen Blick

Stellungnahme zur Änderung der BSI-Kritisverordnung

Unmittelbar nachdem das IT-Sicherheitsgesetz 2.0 im Bundestag verabschiedet wurde hat das Bundesministerium für Inneres, für Bau und Heimat am 26. April 2021 einen Verordnungsentwurf an die betroffenen Wirtschaftsverbände übermittelt, in dem *„die wesentlichen Änderungsbedarfe umgesetzt [werden], die in der zuletzt durchgeführten Evaluierung der BSI-KritisV nach §9 BSI-KritisV identifiziert wurden“*.

Bitkom-Bewertung

Bitkom begrüßt die Überarbeitung der BSI-KritisV und bedankt sich für die eingeräumte – und zeitlich angemessene – Beteiligungs- und Anhörungsmöglichkeit. Auf übergeordneter Ebene gilt es im weiteren und künftigen Änderungsprozess der BSI-KritisV insbesondere die nachfolgenden Punkte hervorzuheben:

- **Notwendigkeit einer nachvollziehbaren Evaluierung**
  Bitkom unterstützt die regelmäßige Evaluierung ausdrücklich. Allerdings erschließt es sich nicht, weshalb die Wirtschaft kein integraler Bestandteil der Evaluierung sein soll und weshalb keine unter Vertraulichkeitsgesichtspunkten vertretbare Teilveröffentlichung der Evaluierungsergebnisse erfolgt. Stattdessen werden die Änderungen *„aufgrund von Feststellungen aus der Evaluierung der BSI-KritisV“* legitimiert. Dies ist unzureichend.
- **Legislative Interdependenz mit- und vorausdenken**
  Die Regularien müssen insgesamt zum Rest der deutschen Gesetzgebung passen und europaweit unbedingt harmonisiert werden. Dies gilt insb. im Hinblick auf derzeit auf EU-Ebene diskutierte sektorübergreifende und sektorspezifische Legislativvorhaben (NIS2, RCE, DORA). Hier greift der Entwurf in Teilen vor und könnte einer EU-weiten Harmonisierung der Sicherheitsstandards ein Stück weit entgegenstehen bzw. zu erheblichen Kosten und Mehraufwänden durch Doppelregulierungen führen.
- **Aktualisiertes Anlageverständnis**
  In Anbetracht der Tatsache, dass in der Praxis ein gesamtheitliches Anlageverständnis bereits die Grundlage für Prüf- und Auditaktivitäten darstellt, ist das gesetzgeberische Nachziehen des für die Verordnung ausschlaggebenden Anlagenbegriffs um Software / IT-Dienste verständlich und grundsätzlich zu begrüßen. Allerdings muss die informationstechnische Kritikalität der Anwendung zur Aufrechterhaltung des versorgungsrelevanten Betriebs explizit als Entscheidungskriterium benannt werden. Andernfalls wäre die BSI-KritisV ein Fass ohne Boden. Es bedarf der Klarstellung, dass es sich beim neuen Anlageverständnis lediglich um die Software / IT-Dienste handelt, die tatsächlich für die Erbringung der kritischen Dienstleistung notwendig sind, also um fachspezifische Anwendungssoftware / IT-Dienste mit hoher Kritikalität.
- **Ausweitung des Anwendungsbereichs**
  Unter der Annahme, dass in der Vergangenheit vermehrt Meldungen über Sicherheitsvorfälle an nicht von der Verordnung erfasste Betreiber zu verzeichnen waren, ist die Ausweitung des Anwendungsbereichs unter Kritikalitätsgesichtspunkten nachvollziehbar und grundsätzlich zu begrüßen. In Ermangelung einer nachvollziehbaren evidenzbasierten Evaluierung und darauf basierender Begründungen stellt die reine Nennung angepasster Berechnungsgrundlagen allerdings keine hinreichende Legitimation dar, um belastbare Schlüsse zur Ausweitung des Geltungsbereichs ziehen zu können.

Stellungnahme zur Änderung der BSI-Kritisverordnung

17. Mai 2021

Vorbemerkungen

Während das IT-Sicherheitsgesetz (2.0) bzw. das BSI-Gesetz (BSIG) den gesetzlichen Überbau darstellt, spezifiziert die BSI-Kritisverordnung (BSI-KritisV) den als hinreichend bedeutsam anzusehenden Versorgungsgrad für die Betreiber in den einzelnen (Teil-) Sektoren. Betreiber, die eine kritische Dienstleistung erbringen und oberhalb der in der BSI-KritisV für die einzelnen KRITIS-Sektoren definierten Schwellenwerte liegen, unterliegen den (nunmehr ausgeweiteten) Anforderungen des IT-Sicherheitsgesetzes (2.0). Mit der neuen BSI-KritisV werden einige branchenspezifische Schwellenwerte abgesenkt sowie neue Teilbereiche aufgenommen. Damit werden mehr Unternehmen in den Geltungsbereich des IT-Sicherheitsgesetzes (2.0) fallen. Laut BMI werden durch die mit der neuen Verordnung vorgenommenen Anpassungen der Bezeichnungen einzelner Anlagenkategorien, einzelner Bemessungskriterien und einzelner Schwellenwerte geschätzte 270 zusätzliche Betreiber von den gesetzlichen Pflichten erfasst, ohne für ausreichende Implementierungszeiträume und Übergangsfristen zu sorgen.

Mit dem vorliegenden Entwurf der aktualisierten BSI-KritisV ist zu konstatieren, dass der Regelungsrahmen immer präziser wird und entsprechend an Komplexität und Umfang zunimmt. Die zunehmende Regelungsdichte führt zu einem schwer zu überschaubaren Gesamtkonstrukt, dessen Interdependenzen kaum abzusehen sind und das mit entsprechend hohen Compliance-Kosten für die Unternehmen einhergeht – vor allem mit Blick auf die z.T. noch unklaren Wechselbeziehungen mit den Vorgaben des IT-Sicherheitsgesetzes 2.0. Vereinfachtes Gedankenspiel: Strom wird außerhalb von Deutschland produziert, an der europäischen Börse gehandelt, ins deutsche Ferntransportnetz eingespeist, ans Verteilnetz übergeben und letztendlich genutzt, um ein Rechenzentrum zu betreiben. Im Rechenzentrum wird dann der TK-Service erbracht, der wiederum gesteuert und überwacht wird. Alle diese Schritte & Prozesse greifen ineinander und werden von IT gesteuert. Letzten Endes sind all diese Schnittstellen zu dokumentieren und entsprechend zu managen. Holistisch betrachtet kann dies nur funktionieren, wenn alle Akteure eine gemeinsame Sprache sprechen, indem sie sich bspw. an anerkannte internationale Standards wie Information Security Management System (ISMS) oder Business Continuity Management System (BCMS) halten. Föderale und sektorspezifische Vorgaben wirken dem gesteckten Ziel eher entgegen.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Sebastian Artz
Referent Informationssicherheit & Sicherheitspolitik
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Die Regularien müssen insgesamt zum Rest der deutschen Gesetzgebung passen und europaweit unbedingt harmonisiert werden. Dies gilt auch im Hinblick auf derzeit auf EU-Ebene diskutierte sektorübergreifende und sektorspezifische Legislativvorhaben. Zu nennen sind hier die Überarbeitung der NIS 2 Directive, die RCE Directive und der für den Finanzsektor und ICT-Service Provider relevante Vorschlag zu DORA. Hier greift der aktuelle Verordnungsentwurf bereits vor und könnte hiermit einer EU-weiten Harmonisierung der Sicherheitsstandards ein Stück weit entgegenstehen bzw. zu erheblichen Kosten und Mehraufwänden führen indem absehbar ggf. unabgestimmte Doppelregulierungen und Redundanzen geschaffen werden. Die notwendige Harmonisierung gilt zudem auch für die Schwellenwerte, die – im Sinne eines gemeinsamen Binnenmarktes – auf europäischer Ebene einheitlich und auf der Basis einer transparenten Evaluierung definiert werden sollten. In Zuge dessen sollte der auf nationaler Ebene genutzte Regelschwellenwert bei der Versorgung von 500.000 Bürgern nochmals einer kritischen Prüfung unterzogen werden.

Inhalt

Seite

§ 1 – Begriffsbestimmungen

Der Gesetzgeber sieht eine 'Klarstellung' des für die Verordnung ausschlaggebenden Anlagenbegriffs vor. Bislang umfasste das Verständnis einer Anlage (1) *Betriebsstätten und sonstige ortsfeste Einrichtungen sowie* (2) *Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen*. Mit den vorgesehenen Änderungen wird die Definition durch (3) *Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind* ergänzt.

In Anbetracht der Tatsache, dass in der gängigen Praxis ein gesamtheitliches Anlageverständnis bereits Berücksichtigung findet und die Grundlage für Prüfaktivitäten und Audits darstellt, ist das gesetzgeberische Nachziehen verständlich und zu begrüßen. Allerdings wirft die gewählte Formulierung des Anlageverständnisses um Software und IT-Dienste ohne ergänzende Erläuterung kritische Folgefragen auf.

Für Bitkom muss die informationstechnische Kritikalität die BSI-KritisV klar eingrenzen. Es bedarf der Klarstellung, dass es sich beim Anlageverständnis um Software / IT-Dienste handelt, die tatsächlich für die Erbringung einer kritischen Dienstleistung notwendig sind, also um fachspezifische Anwendungssoftware / IT-Dienste. **Die eindeutig an den übergeordneten Schutzzielen und der Kritikalität im Einsatzkontext orientierte Leitfrage muss lauten: Kann der versorgungsrelevante Betrieb vorläufig aufrechterhalten werden, wenn ein konkreter IT-Dienst oder eine bestimmte Software nicht funktioniert?**

Aufgezeigt am Beispiel eines Krankenhauses sind ein Patientenverwaltungs- und Managementsystem, die Software zur Medikamentenbestellung sowie die Personal- und Einsatzplanungssoftware durchaus betriebskritisch. Dagegen ist bspw. das verwendete Betriebssystem oder die Rechnungserstellungssoftware unkritisch zur Erbringung der Dienstleistung und darf nicht in den Regelungsgegenstand hineingezogen werden. Andernfalls würden wir uns in einem Fass ohne Boden wiederfinden, weil die Einbeziehung über den Anlagenbegriff erfolgt und sich horizontal über alle Sektoren erstrecken soll. Dieser Logik und der pauschalen Ausdehnung auf den Software-Layer folgend müssten künftig quasi für jede denkbare Anwendungsklasse separate Mindeststandards definiert werden.

Wie so oft kommt auch in diesem Kontext zum Tragen, dass der gesamte Sektor Informationstechnologie innerhalb des KRITIS Regimes gleichzeitig horizontal über den anderen Sektoren liegt. Dieser Besonderheit wird die aktuelle Formulierung und Erläuterung des Anlagebegriffs nicht im ausreichenden Maße gerecht.

Gemäß § 1 Nr.1 Satz 3 (neu) gelten mehrere Anlagen, die durch einen betriebstechnischen Zusammenhang verbunden sind, nun als gemeinsame Anlage, wenn sie zur Erbringung derselben kritischen Dienstleistung notwendig sind. Dies kann die aufzubringenden

Aufwände für Dokumentation, Schnittstellenmanagement, Audits etc. reduzieren und ist daher grundsätzlich zu begrüßen.

§1 Nr. 2 Satz 2 (neu) lautet: „*Betreiben zwei oder mehr Personen gemeinsam eine Anlage, so ist jeder für die Erfüllung der Pflichten als Betreiber verantwortlich*." Anstelle von „Personen" sollte auf „juristische Personen" abgestellt und gleichzeitig klargestellt werden, was genau mit dieser Änderung bezweckt wird. Sofern die Aufnahme einer gesamtschuldnerischen Haftung intendiert sein sollte, ist dies aus Sicht des Bitkom zurückzuweisen. Darüber hinaus stellt sich die Frage, wie die Abgrenzung vorzunehmen ist, wenn, wie bspw. im Bankensektor üblich, eine Outsourcingkaskade vorliegt: Bank lagert IT und ggf. bankfachliche Prozesse (Backoffice) aus; Dienstleister lagert wiederum Teile (z.B. RZ-Betrieb,...) aus. Wer ist Betreiber? Zumindest die Möglichkeit der gemeinsamen Meldung und somit gemeinsamen Veranlagung gegenüber dem BSI sollte den Betreibern auch hier (wie bei der „zentralen Stelle") möglich sein. Andernfalls wird ein und dieselbe Anlage bzw. Anlagenteile ggf. mehrfach unabhängig voneinander an das BSI gemeldet, was nicht im Sinne der Effizienz und Transparenz aus Sicht des BSI sein kann.

Die in §1 Nr. 4 und 5 enthaltenen Definitionen von Schwellwert und Versorgungsgrad bleibt unverändert. Bitkom regt an, den Regelschwellenwert bei der Versorgung von 500.000 Personen nochmals einer kritischen Prüfung zu unterziehen. Während in bestimmten Teilsektoren eine evidenzbasierte Absenkung des Schwellenwertes zu Recht angezeigt ist, sollte bspw. im Bank- und Finanzsektor dahingehend präzisiert werden, dass der Schwellenwert nicht als alleiniges Entscheidungskriterium zum Versorgungsgrad herangezogen wird. Beispiel: Ein Kunde einer Bank erzeugt 100.000 Depottransaktionen (wie bei Institutionellen Anlegern durchaus gang und gäbe). Wenn die Bank auch nur 10 derartige Kunden hat, erzielen diese bereits ein Volumen größer als der Schwellwert und die Bank wäre gem. der BSI-KritisV Betreiber einer kritischen Dienstleistung, obwohl diese nur 10 Personen versorgt. Dies kann nicht im Sinne der BSI-KritisV sein, die ja erklärtermaßen vor erheblichen Versorgungsengpässen schützen soll. Bei 10 betroffenen Bürgern kann davon nicht die Rede sein. Besser wäre es, wenn die Schwellwerte mit der Anzahl der versorgten Personen gekoppelt würde; nur wenn auch diese Anzahl der die schwellwertbezogenen Transaktionen auslösenden Personen über dem für die Schwellwertberechnung zugrunde gelegten Anzahl (meist 500.000) liegt, erfolgt die Einstufung als kritische Dienstleistung. Mit Blick auf die Handelsplätze sollte ein Grenzwerte von > 15 Mio. ausgeführter Transaktionen p.a. aufgenommen und ein Durchschnitt des Grenzwertes über mindestens zwei Jahre angelegt werden, da das Orderaufkommen an Handelsplätzen immer sehr volatil ist (z.B. Ausbruch der Corona-Krise vs. Ferienmonate).

§ 2 – Sektor Energie

Im Zuge der Novellierung wird die Absenkung der bisherigen Schwellenwerte zur Identifikation von Energieerzeugungsanlagen als Kritische Infrastruktur von derzeit 420 MW auf 36 MW installierter elektrischer Netto-Nennleistung erwogen. Für Bitkom ist die Absenkung des Schwellenwertes nachvollziehbar und grundsätzlich richtig.

Allerdings wird dies zu einem erheblichen Mehraufwand hinsichtlich der Auditierung nach dem IT-Sicherheitsgesetz (2.0) führen. Angesichts des Regelungsziels, den Schutz der informationstechnischen Systeme derjenigen Anlagen zu fördern, die für eine sichere und störungsfreie Stromversorgung wichtig sind, ist es unerlässlich, neben der reinen Netto-Nennleistung (quantitativ) zusätzlich auf die technischen Eigenschaften einer Anlage (qualitativ) abzustellen. Eine rein monokausale Bestimmung einer Anlage als KRITIS kann diesem Ziel nicht gerecht werden. Vor diesem Hintergrund sollte eine neue Kategorie in Anhang 1 Teil 3 BSI-KritisV aufgenommen werden:

- *„Anlagen ab 36 bis 420 MW installierter elektrischer Netto-Nennleistung UND Primärregelfähigkeit bzw. Fähigkeit zur schnellen Neusynchronisierung, sofern technisch möglich und vertraglich vereinbart mit den relevanten Übertragungsnetzbetreiber(n)“*

Die administrativen Aufwände im Rahmen der Umsetzung des IT-Sicherheitskatalogs nach § 11 1b EnWG sind erheblich und stellen einen Großteil des Erfüllungsaufwands dar. Der Mehrwert, der hieraus für die operative IT-Sicherheit einer Anlage erwächst, ist eng begrenzt.

Dagegen ist die Einbeziehung des Gas- und Mineralölhandels in die BSI-KritisV aus Sicht des Bitkom zu begrüßen. Allerdings schlagen wir auch hier ebenfalls eine Erhöhung des Schwellenwertes z.B. für den Gashandel vor. Der vorgegebene Wert erscheint hier unplausibel, da 5.3 TWh Gas in Deutschland im Winter bereits an einem einzigen Tag verbraucht werden – der in der Verordnung definierte Schwellwert im Strom entspricht hingegen dem deutschen Verbrauch von ca. 6 Jahren. Hinzu kommt, dass die Kritikalität der Handelsinfrastruktur infolge der Speicherfähigkeit von Gas und des Netzpuffers viel niedriger ist als im Strombereich. Ferner ergibt sich im Gashandel eine Tagesbilanzierung: wenn der Gasmarkt eine Stunde „steht“, ist dies zumindest aus Sicht der Versorgungssicherheit irrelevant. Im Strombereich hätte dies schwerwiegendere Konsequenzen. Dies scheint in der Gesamtheit inkonsistent und spricht daher für eine Anhebung der Schwellenwerte im Gasbereich.

Im Bereich der Fernwärmeversorgung könnte unter Kritikalitätsgesichtspunkten eine Halbierung der bisherigen Schwellenwerte in Betracht gezogen werden, da viele Städte sich– nicht zuletzt aus Gründen der CO2-Reduktion – auf den Einsatz von Fernwärme fokussieren. Eine alternative Wärmeversorgung ist in den Häusern bzw. Wohnungen nicht

vorgesehen. Sollte hier die Fernwärmeversorgung nicht mehr funktionieren, sind nicht genügend Ersatzmaßnahmen verfügbar - das gilt nicht nur für 250.000 Wohnungen, sondern auch für Krankenhäuser, Bürogebäude in Wirtschaft und Verwaltung sowie für zahlreiche weitere Einrichtungen wir Bahnhöfe, Einkaufseinrichtungen etc.

§ 3 – Sektor Wasser

Die Außerachtlassung von Stauanlagen in der BSI-KritisV war bisher ein Blindspot. In Anbetracht der Kritikalität dieser Anlagen ist die Ausweitung des Geltungsbereichs gerechtfertigt. Bedauerlicherweise lässt der Gesetzgeber die Frage nach dem Warum unbeantwortet.

§ 4 – Sektor Ernährung

Die erstmalige Aufnahme der Produktion von Getränken mit einem Alkoholgehalt von bis zu 1,2% erschließt sich Bitkom nicht. Aus welchem Grund sollten alkoholische Getränke überhaupt versorgungsrelevant sein? Diese Änderung sollte gestrichen werden.

§ 5 – Sektor Informationstechnik und Telekommunikation

Der Gesetzgeber sieht die Unterscheidung zwischen physischen und virtuellen Instanzen vor. Die Frage, ob dies Cloud inkludiert, bleibt unbeantwortet.

Im Bereich Housing und Hosting ist neu und durchaus problematisch, dass die Stichtagsregelung zur Messung der vertraglich vereinbarten IT-Leistung weggefallen ist, da Unternehmen die sich in unmittelbarer Nähe der Schwelle befinden, insb. Rechenzentren aber auch Hosting-Provider, diese für wenige Monate überschreiten und danach wieder darunter liegen könnten. Hier wäre zukünftig in allen betroffenen Sektoren, bei jeder größerer Vertragsänderung eine Korrektur der Schwellwerte notwendig. Je nach Gewerk ist eine fortwährende Neujustierung zu befürchten. Die Stichtagsregelung ist ein bewährtes Konzept, branchenweit bekannt und sollte daher beibehalten werden.

Für Rechenzentren ist eine Änderung des Berechnungswertes von 5 auf 3,5 MW vorgesehen. Erneut stellt sich die Frage nach dem Warum. Gleiches gilt für die vorgesehene Absenkung der Schwellenwerte von 300 auf 100 angeschlossener autonomer Systemen zur Erfassung weiterer, bisher nicht erfasster Netzknoten (IXP). In Anbetracht der Kritikalität erscheint das Vorhaben durchaus nachvollziehbar und sinnvoll. Allerdings ist keinerlei zugrundeliegende Systematik ersichtlich, weshalb erneut der Weg zum finalen Resultat und die damit verbundene Entscheidung zur Absenkung der Schwellenwerte zu kritisieren sind.

Bzgl. "Anlagenkategorie" 2.6 "Top-Level-Domain-Name-Registry" in Anhang 4 ist anzumerken, dass der zur Definition der Registry gewählte Begriff der Einrichtung auf den Betreiber insgesamt statt auf die kritische Komponente (Anlage, Einrichtung) zielt und damit nicht konsistent mit den sonstigen Definitionen in der Verordnung ist. Hier ist eine entsprechende Fokussierung der Definition notwendig.

§ 7 – Sektor Finanz- & Versicherungswesen

Grundsätzlich würden wir uns eine enge Abstimmung verschiedener Aufsichtsbehörden wünschen, um die Komplexität zu reduzieren und zukünftig gemeinsame Prozesse etablieren zu können. Hier wären neben dem Finanzministerium bspw. die BaFin und die Börsenaufsichtsbehörden der Länder gem. § 3 Abs. 1 BörsG zu nennen. Dies ist besonders vor dem Hintergrund aktueller EU-Gesetzesvorhaben zu DORA, NIS2 und RCE von Bedeutung.

Hinsichtlich des Geltungsbereiches der BSI Verordnung ist zu beachten, dass DORA als „lex-specialis“ des Finanzsektors zukünftig vermutlich Vorrang gegenüber europäischen und nationalen Regelungen zum Thema IT-Sicherheit und Resilienz haben wird. Das Vorhaben der EU, mit DORA eine unionsweit harmonisierte IKT-Regulierung für den Finanzsektor zu schaffen, unterstützen wir ausdrücklich. Dies sollte in der Überarbeitung der Verordnung hinsichtlich des Geltungsbereichs bereits antizipiert werden. In jedem Fall ist es nötig darauf zu achten, dass die nationalen und europäischen Regelungen möglichst gut abgestimmt sind und dass es nicht zu Ineffizienzen und Kosten durch Doppelregulierungen kommt.

§7 Abs. 3 (und 4): Beim Zahlungsverkehr gilt das Prinzip der Buchung und Gegenbuchung. Ist jede dieser Buchung ("Belastung auf dem Konto des Zahlers" und "Gutschrift auf dem Konto des Zahlungsempfängers") als einzelne Transaktion zu zählen oder gelten Buchung und Gegenbuchung als eine Transaktion im Sinne des Schwellwertes?

§7 Abs. 5: Unmittelbar anknüpfend an den vorherigen Punkt kommt hier erschwerend hinzu, dass beim Handel von Wertpapieren mitunter ein Wertvorgang eine Vielzahl der aufgeführten verschiedenen Transaktionen auslöst. Bsp. Handelsausführung, Buchung des WP in den Kundenbestand, Ausbuchung des WP aus dem Depot des Verkäufer, Einbuchung des WP in das Depot des Käufers, ggf. ein oder mehrere Zahlungsaufträge zum Ausgleich von Wertdifferenzen, etc.). Hier kann ein WP Auftrag also 10++ Transaktionen im Sinne des §7 Abs. 5 auslösen. Wie ist hier zu zählen: gilt jede einzelne Transaktion als eigenständig zu zählen.

§7 Abs. 8: Wie bereits in der aktuellen BSI-KritisV bleibt unbestimmt, wie „Sachherrschaft“ zu interpretieren ist. Wie ist bei geteilter Sachherrschaft vorzugehen (vgl. Beispiel der Outsourcingkette aus §1 Abs 2.)

Anhang 6 Teil 1 Abs. 1: 1.13 Der Verweis auf die EU-Verordnungen ist ein unnötige Schachtelung und erschwert das klare Verständnis, was der Ersteller der BSI-KritisV hier wirklich will. Wunsch: es sollte eine klare in sich abgeschlossene Definition aufgeführt werden, ohne Verweis auf andere (EU) Regelungen, welche ebenfalls wieder Verweise enthalten (Kaskadenverweis).

Anhang 6 Teil 1 Abs. 1.22: "Finanzmarktinfrastrukturbetreiber" sollte klar definiert werden. Wir schlagen vor es mit bestehenden Formulierungen aus MiFID II und nationalen Regeln in Einklang zu bringen.

Anhang 6 Teil 1 Teil 1 Abs. 3: Die „Durchschnittsregel über 3 Jahre“ sollte auch auf Teil 3 Spalte A Nummer 3 und 4 angewandt werden können. Begründung: Im Jahr 2020 wurden ausgelöst durch die COVID-19 Pandemie außerordentlich viele Börsentransaktionen (WP-Handel) verzeichnet. Im mehrjährigen Mittel waren im März/April/Mai 2020 bis zu +200% Transaktionen und mehr zu verzeichnen. Derartige Sondereffekte sollten durch ein mehrjähriges Mittel geglättet werden, andernfalls kommt es zu einer Vielzahl von Erstmeldungen an das BSI und unmittelbar im Folgejahr zur Abmeldung. Der damit verbundene Aufwand kann nicht im Sinne des BSI sein.

Anhang 6 Teil 1 Abs. 6: Ist mit "gemeinsamer Leitung" die "gemeinsame Sachherrschaft" gemeint?

Anhang 6 Teil 2 Abs. 12: Wie schon in der aktuellen BSI-KritisV sind die angesetzten 1,7 Transaktionen pro Person und Jahr unrealistisch und setzen viel zu niedrig an, da nicht nur Privatpersonen, sondern auch Unternehmen verschiedene Finanzinstrumente handeln. Die vorgeschlagenen Werte würden eine Vielzahl von Handelsplätzen in den Geltungsbereich der Verordnung integrieren und als kritisch deklarieren, unabhängig von der tatsächlichen Relevanz eines einzelnen Handelsplatzes für das Finanzsystem.

§ 8 – Sektor Transport & Verkehr

Die Pandemie hat einmal mehr gezeigt, dass auch die Logistik-Branche kritische Dienstleistungen bereitstellt. Mit Blick auf die bisher gültigen Schwellenwerte ist die Anzahl der Unternehmen, die im dem Bereich Logistik kritische Dienstleistungen erbringt, allerdings vergleichsweise gering.

Einführung des zusätzlichen Bemessungskriteriums „Anzahl der Sendungen pro Jahr“ [Änderung Nr. 16 b) ee)]

Zur Kritikalitätsbemessung sind ausschließlich Kriterien heranzuziehen, die verkehrsübergreifend eindeutig bestimmbar sind und eine objektive Vergleichbarkeit erlauben. Das im Verordnungsentwurf eingebrachte neue Bemessungskriterium „Anzahl der Sendungen pro Jahr“ ist für die Kritikalitätsbestimmung von Logistikanlagen generell ungeeignet. Auch wenn die Einführung als Erleichterung für die Betreiber gedacht ist, hätte sie für die gesamte Logistikbranche weitreichende Folgen. Alle Betreiber müssten ihre operativen Logistikdienstleistungen auch anhand der Sendungsmenge abbilden, unabhängig davon, ob es sinnvoll und praktikabel ist. Sie wären dann gezwungen, etwas zu erfassen, was nicht einheitlich definiert ist und selbst innerhalb betrieblicher Abläufe unterschiedlich erfasst sein kann. Enorme Rechtsunsicherheiten wären die Folge.

Da durch logistische Produktions- und Verarbeitungsprozesse, bspw. Konsolidierungen, Umverpackungen, Palettierung sowie vice versa die Erfassung einer Stückzahl oder Sendungsmenge selbst innerhalb von einzelnen Bearbeitungsprozessen und somit innerhalb von Logistikzentren selbst extremen Schwankungen unterliegt, ließe sich diese Messgröße nicht übergreifend, einheitlich und vergleichbar erfassen. Die BSI-KritisV unterscheidet die operativen logistischen Dienstleistungen nicht nach qualitativen Kriterien und/oder nach den transportierten kritischen Warengruppen. Jede transportierte Ware ist Teil der Berechnung des bestehenden Schwellenwertes „Gütermenge in Tonnen/Jahr“. Erst dadurch entsteht der relativ hohe Schwellenwert von 17 Mio. Tonnen pro Jahr. Er berechnet sich auf der Basis, dass jede Person pro Jahr 34 Tonnen an logistischen Gütern erhält und jede Anlage zur Versorgung von 500.000 Personen beiträgt. Die Einführung der Sendungsmenge als zusätzliches Bemessungskriteriums konterkariert diese Logik: die Gütermenge lässt sich nicht mit Hilfe einer unterkomplexen Sendungs-Definition in ein qualitativ anderes Bemessungskriterium umrechnen.

Das angenommene Durchschnittsgewicht von 330 Kilogramm pro Stückgutsendung, der maßgeblich für die Berechnung des neuen Bemessungskriteriums ist, ist willkürlich. Der Verordnungsgeber stellt nicht nachvollziehbar dar, auf welcher Datenbasis dieser Wert ermittelt wurde und warum er allgemein zur Bemessung aller Anlagen oder Systeme zur Erbringung operativer Logistikleistungen herangezogen werden kann. Die BSI-KritisV definiert einen einheitlichen Logistik-Anlagenbegriff, unter dem alle operativen logistischen Dienstleistungen (Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik) subsumiert sind. Es ist unverständlich, warum ein zusätzliches Bemessungskriterium, welches sich eindimensional am Gewicht einer Stückgutsendung orientiert, notwendig ist und angewendet werden soll.

Die „Anzahl der Sendungen pro Jahr“ als Bemessungskriterium wurde bereits im Rahmen des kooperativen Ansatzes beraten und im Ergebnis vom Verordnungsgeber als

ungeeignet erachtet worden, da weder eine logistik- noch branchenweite Datenbasis für die Ableitung eines derartigen Schwellenwertes existiert. Branchenvertreter haben wiederholt auf diese Problematik hingewiesen. Es ist daher nicht nachvollziehbar, warum im nun vorliegenden Änderungsentwurf dieses Kriterium erneut aufgegriffen wird.

Das alleinige Bemessungskriterium jährliche Gütermenge in Tonnen sowie der dazu festgelegte Schwellenwert haben sich in der Praxis bewährt. Aufgrund seiner einheitlichen Anwendbarkeit und definitorischen Bestimmtheit ist er das einzige Bemessungskriterium im Bereich Logistik, das die an ein Bemessungskriterium zwingend anzulegenden Maßstäbe erfüllt.

Erweiterung des Bemessungskriteriums „Gütermengen in Tonnen/Jahr“ um „Transportmengen im Im- und Export, der Transitverkehre sowie Leercontainer in Tonnen/Jahr“ [Änderung Nr. 16 c) 1.6.1 und 1.6.2]

Im BSIG §2 Absatz (10) wird ausdrücklich vom Gesetzgeber darauf verwiesen, dass kritische Infrastrukturen solche sind, deren Ausfall eine Gefahr für die Sicherheit oder Versorgung der Bevölkerung in Deutschland wäre. Beide Risiken sind bei Transitverkehren offensichtlich nicht gegeben, da sie nicht für die Versorgung in Deutschland bestimmt sind. Gleichwohl droht durch Überregulierung ein weiterer Wirtschaftlicher Standortnachteil für deutsche Unternehmen im europäischen und internationalen Vergleich, ohne, in Bezug auf den Transitverkehr, einen Sicherheitsmehrwert zu leisten. Gleiches gilt für Exporte, die nicht für die Versorgung Deutschlands bestimmt sind und daher auch keine unmittelbare Auswirkung auf die Versorgung mit kritischen Waren haben können. Daher sollten diese Gütermengen nicht bei der Bemessung der Kritikalität einer Anlage oder eines Systems zur Erbringung operativer Logistikleistungen berücksichtigt werden.

Der Umgang mit Leercontainern ist eine Herausforderung bei der Organisation logistischer Prozesse, die von professionellen Unternehmen und ihren Experten tagtäglich in Deutschland gemeistert wird. Es ist weder Regelungsziel des BSIG, logistische Prozesse auf ihre Effizienz hin zu überprüfen, noch bietet das Gesetz das richtige Rüstzeug dazu. Leercontainer können zudem nicht in den Schwellenwerten erfasst werden. Den betroffenen Betreibern sollte es ermöglicht werden, die für den Export oder Transitverkehr bestimmte Transportmengen sowie die Leercontainer bei der Berechnung einer möglichen Kritikalität zu exkludieren.

Die Ausweitung des Bemessungskriteriums auf nicht für die Versorgung bestimmte Gütervolumen ist nicht vom gesetzgeberischen Auftrag gedeckt. Der vom Gesetzgeber bewusst eng gefasste definitorische Rahmen zur Bestimmung der essentiellen nationalen Infrastrukturen ist auch vom Verordnungsgeber bei der Bestimmung der kritischen Infrastrukturbetreiber unbedingt einzuhalten.

§ 9 – Evaluierung

Gemäß § 9 soll auch zukünftig im zweijährigen Rhythmus unter Federführung des BMI und im Einvernehmen mit den zuständigen Ressorts eine Evaluierung der BSI-KritisV erfolgen. Bitkom unterstützt die regelmäßige Evaluierung ausdrücklich. Allerdings erschließt es sich nicht, weshalb die Wirtschaft nicht integraler Bestandteil der Evaluierung sein soll und weshalb die Erkenntnisse nicht partnerschaftlich geteilt werden. Stattdessen werden die aktuellen Änderungen an der BSI-KritisV *„aufgrund von Feststellungen aus der Evaluierung der BSI-Kritisverordnung“* legitimiert. Für Bitkom ist das kein hinreichender Beleg zur Begründung signifikanter Änderungsvorhaben. Für Bitkom existiert ein signifikanter Unterschied zwischen einer umfassenden Evaluierung und der Einarbeitung von Feedback des BSI auf Basis vermeintlich gemeldeter Sicherheitsvorfälle bei bis dato nicht-KRITIS Betreibern.

Bitkom spricht sich für eine unter Vertraulichkeitsgesichtspunkten vertretbare Teilveröffentlichung der Evaluierungsergebnisse aus und empfiehlt künftig die explizite Verzahnung mit der von uns befürworteten (neu festgeschriebenen) Aufgabenerfüllung des BSI auf der *„Grundlage wissenschaftlich-technischer Erkenntnisse“* (§1 BSIG).

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.