Stellungnahme

Zum Entwurf einer Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Felix Dembski, LL.M.
Bereichsleiter Intelligente Netze & Energie
T +49 30 27576-204
f.dembski@bitkom.org

Marc Fliehe
Bereichsleiter Sicherheit
T +49 30 27576-242
m.fliehe@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlands-umsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Einleitung

Das erste IT-Sicherheitsgesetz wurde am 12. Juni 2015 im Bundestag beschlossen und trat am 25. Juli 2015 in Kraft. Das Gesetz verweist in §10 auf eine Rechtsverordnung, nach der bestimmt wird, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten.
Bitkom begrüßt ausdrücklich die enge Zusammenarbeit zwischen BMI, BSI, BMWi und der Wirtschaft, die auch im Vorfeld des Referentenentwurfes einen stetigen Informationsaustausch zwischen Staat und den Betreibern Kritischer Infrastrukturen ermöglicht hat und so einen insgesamt zeiteffizienten Prozess zur Erstellung der Rechtsverordnung unterstütz und zu einer praxisnahen Ausgestaltung der Inhalte beigetragen hat.

Am 2. Februar 2016 hat das Bundesministerium des Innern den Referentenentwurf zur „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ vorgelegt und die Verbände aufgefordert, hierzu bis zum 23. Februar 2016 Stellung zu nehmen. Bitkom nimmt gerne die Gelegenheit wahr, seine Position zum Referentenentwurf darzustellen.

Begriffsbestimmungen – § 1

In diesem Abschnitt werden auch „Nebeneinrichtungen“ von Kritischen Infrastrukturen aufgegriffen, worunter Anlagenteilen und Verfahrensschritte gemeint sind, die mit der Anlage in einem „betriebstechnischen Zusammenhang“ stehen und „die für die Erbringung einer kritischen Dienstleistung von Bedeutung sein können“. Beide Formulierungen hält Bitkom nicht für hinreichend umfänglich definiert. Diese Unschärfe der Begrifflichkeit wird dadurch noch verstärkt, indem sich beide Materien wechselseitig aufeinander beziehen. Bitkom schlägt daher vor, den Konjunktiv in dieser Formulierung durch konkrete Beispiele und Kriterien zu ersetzen. Wir halten es für nötig, hier im Sinne einer Rechts- und Planungssicherheit der Unternehmen und im Sinne der Wirkungsentfaltung des Gesetzes möglichst eindeutige Vorgaben zu schaffen, welches Unternehmen und welcher Unternehmensteil als Betreiber einer Kritischen Infrastruktur zu verstehen ist.
Ferner hält der Bitkom einheitliche Begriffsdefinition für erforderlich:
§ 2 Absatz 10 Satz 1 BSI-Gesetz definiert den Begriff der kritischen Infrastruktur im Sinne des BSI-Gesetzes. Danach sind solche „Einrichtungen, Anlagen oder Teile davon [gemeint], die ...
2.
von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“
Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt, vgl. § 2 Absatz 10 Satz 2 BSI-Gesetz.
§ 1 Nr. 3 KRITIS VO (E) definiert den Begriff der kritischen Dienstleistung. Darunter soll „eine Dienstleistung zur Versorgung der Allgemeinheit... deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit oder zu vergleichbaren Folgen führen würde. Hinsichtlich der „vergleichbaren Folgen“ geht die Definition der KRITIS VO (E) über § 2 Absatz 10 BSI-Gesetz hinaus und ist insofern nicht von einer gesetzlichen Ermächtigungsgrundlage gedeckt. Wir regen daher die Streichung dieser Passage an.

Schwellenwerte Energie, § 2

Wir weisen darauf hin, dass nach unserer Lesart im Bereich Energie nicht die Schwellenwerte gewählt wurden, die tatsächlich den Versorgungsgrad von 500.000 Bürgern widerspiegeln. Der zugrunde gelegte Durchschnittsverbrauch pro Person von 7.375 kWh basiert scheinbar darauf, dass der deutsche Jahresstromverbrauch von 590 TWh durch 80 Millionen Einwohner geteilt wurde. Dabei wird aber verkannt, dass Privathaushalte nur 25 Prozent des Stroms verbrauchen. Legte man dies zugrunde, ergäben sich andere Schwellenwerte, nämlich:

25 Prozent des Gesamtverbrauchs von 590 TWh = ~148TWh
Durchschnittsverbrauch pro versorgter Person so ca. 1844kWh/Jahr
Bei einem Regelschwellenwert von 500.000 versorgten Personen resultiert dies bei den Netzen bei ca. 920 GWh/Jahr
Die durchschnittliche elektrische Arbeit von Kraftwerken zur Versorgung von 500.000 Personen im Jahr entspricht dann einer Leistung von ca. 105 MW.

Cloud-Services / Serverfarmen – Begründung, § 5, zu Abs. 1 Nr. 2

Bitkom sieht hier eine unzureichende Begriffsklärung von „Rechenzentrum“ und „Anlagen“ im Zusammenhang mit Cloud Services, die unter Zuhilfenahme von Co-Lo Rechenzentren erbracht werden. Es bleibt unklar, ob in der Schwellwertberechnung genutzte Co-Locations in Deutschland erfasst sind oder nicht. Auch hierbei ist unklar ob der Cloud Service mit internationaler Infrastruktur gesplittet werden muss, um nur die in Deutschland ansässigen Anlagenteile für den Schwellenwert zu erfassen, oder ob hier der Service als Ganzes mit seiner im Ausland ansässigen Rechenzentren zu verstehen ist. Ganz praktisch sollte die Verordnung klarstellen, ob bei der Berechnung des Schwellenwertes von 25.000 Instanzen diese *in einem Rechenzentrum* betrieben werden müssen, um als Kritische Infrastruktur zu gelten, oder ob bereits ein Unternehmen Kritische Infrastruktur ist, das in mehreren Rechenzentren insgesamt 25.000 Instanzen betreibt.

Wir weisen auch darauf hin, dass die Einbeziehung virtueller Instanzen die Gefahr birgt, dass die Realität die Verordnung schnell überholt. Denn bei der Verwendung virtueller Instanzen besteht faktisch keine Limitierung. Über das Ziel, allein die 30 größten Rechenzentren / Serverfarmen in Deutschland zu erfassen, könnte schnell hinausgeschossen werden. Entsprechend müsste eine Regelung vorgesehen werden, wie dies verhindert werden kann.

Definition Rechenzentrum (Housing) – Begründung Teil B, § 5, zu Abs. 4 Nr. 1

Die Definition des Rechenzentrums (Housing) sollte präzisiert werden, um Missverständnissen vorzubeugen. Es muss zunächst präzisiert werden, wie mit mehreren auf einem Campus zusammengefassten Rechenzentren umgegangen wird. Diese gemeinsame Ansiedlung dient dem schnellen Datenaustausch untereinander. In manchen Rechtsgebieten, etwa im Immissionsschutzrecht, werden dann solche verschiedenen Anlagen manchmal wie eine Anlage behandelt. Dies sollte bei der Kritischen Infrastruktur nicht geschehen, solange es sich um eigenständige Einheiten handelt.

Ebenso muss klargestellt werden, dass von Unternehmen zu eigenen Zwecken genutzte Rechenzentren nicht erfasst sind. Sie sollten nur erfasst sein, wenn das Unternehmen selbst zur Kritischen Infrastruktur gehört (z. B. das Rechenzentrum einer großen Bank sollte erfasst sein, das Forschungs-Rechenzentrum eines Pharmaunternehmens nicht).

Wir regen daher an, die Definition Rechenzentrum (Housing) wie folgt zu präzisieren:

„*Einzelnes* Gebäude, zumindest aber ein geschlossener Raum mit dem vorrangigen Zweck, eine geeignete Umgebung für die Unterbringung und den Betrieb von zentralen IT-Komponenten, (z. B. Server, Storage, Netzwerktechnik) *Dritter, nicht mit dem RZ-Betreiber verbundener Unternehmen* in mindestens zehn Racks bereitzustellen.“

Grundsätze und Fristen – Anhang 4, Teil 1, Ziffer 1

Wir regen an, Nr. 1, Satz 1 im Hinblick auf den Anwendungsbereich von § 8a BSI-Gesetz zu konkretisieren: „Eine Anlage, die unter den Anwendungsbereich von § 8a BSI-G fällt und die einer Teil 3, Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt…".

Schwellenwerte Sektor IKT – Anhang 4, Teil 1, Ziffer 4

Zur Ermittlung des Versorgungsgrades „ist auf den rechtlich und tatsächlich möglichen Betriebsumfang der Anlage abzustellen." Bitkom regt an, die genutzte Kapazität zur Ermittlung des Versorgungsgrades heranzuziehen. Der tatsächlich mögliche Betriebsumfang ist im IKT-Bereich – je nach Einsatzgebiet – nur durch Schätzungen möglich.

Berechnungsformel zur Ermittlung der branchenspezifischen Schwellenwerte – Anhang 4, Teil 2, Ziffer 5

„Der für die Anlagenkategorien des Teils 3, Nummer 1.1.1 und 1.1.1 genannte Schwellenwert ergibt sich aus § 1 Absatz 1 Nummer 2 des Post- und Telekommunikationssicherstellungsgesetzes vom 24. März 2011 (BGBl. I S. 506, 941)."
Der genannte Punkt bezieht sich offensichtlich auf die folgenden in Anhang 4 Teil 3 genannten Anlagen in den Punkten 1.1.1, 1.1.2, 1.2.1 und 1.2.2.
Unter Punkt 1.1 wird der „Zugang" behandelt. Insofern sollten die Anlagenbezeichnungen hier nicht auf die öffentlichen Netze insgesamt abheben, sondern den Zugangsaspekt betonen. Ein geeigneter Begriff wäre „Teilnehmeranschluss" (gemäß § 3 Nr. 21 TKG). Die Verweise in 1.2.1 und 1.2.2 auf 1.1.1 und 1.1.2 wären dann zu ersetzen durch Verweise auf beispielsweise „Öffentliches Telekommunikationsnetz". Im Übrigen erscheint die Differenzierung zwischen 1.1.1 (Öffentliches Telefonnetz) und 1.1.2 (Öffentliches Telekommunikationsnetz) hier nicht angebracht, da jedes öffentliche Telefonnetz auch ein öffentliches Telekommunikationsnetz ist.
Auch die Differenzierung zwischen 1.2.1 (Telekommunikationslinie) und 1.2.2 (Übertragungsweg) ist nicht plausibel. Physische Darstellung und tatsächliche Nutzung von Übertragungsmöglichkeiten erscheinen hier vermischt bzw. redundant.

Wie kann zudem zu 1.2.3 (Standortkopplung) differenziert werden? Wir schlagen folgende Ergänzung zu 1.2.3, Spalte B vor: „1.2.3 Standortkopplung, die nicht zu einem öffentlichen Telefon-/Telekommunikationsnetz nach Nummer 1.1.1 oder 1.1.2 gehört".

Schwellenwerte Sektor Housing / Rechenzentrum - Anhang 4, Teil 3, Ziffer 2.1.1

Die Ermittlung der kontrahierten Serverleistung sollte nicht im Jahresdurchschnitt erfolgen, sondern bezogen auf einen bestimmten **Stichtag**.
Hintergrund: Die kontrahierte Serverleistung ist keine gemessene Verbrauchszahl, sondern eine aus den Verträgen abzuleitenden Größe. Es wäre extrem aufwendig die im Laufe eines Jahres geschlossenen oder gekündigten (größe-

ren) Verträge und deren Vertragswert gewichtet zu mitteln. Für jeden Vertrag müsste ermittelt werden, wieviel MW für welche der 365 Tage zugesichert wurden, und für welche nicht mehr.
Wir regen an unter Ziffer 2.1.1, Spalte C die Worte „im Jahresdurchschnitt“ durch „am 1. April eines Kalenderjahres“ zu ersetzen.

Kritikalität von Zertifikaten - Anhang 4 Teil 3 Punkt 2.3

Vertrauensdienste, bspw. Zertifikate zur Identifizierung, Authentifizierung etc., werden bei der Nutzung andere Dienste (z. B. Online-Banking) eingesetzt. Insofern ist nach unserem Verständnis für die Einordnung eines Vertrauensdienstes als kritische Infrastruktur entscheidend, ob der Dienst, der mit dem Vertrauensdienst unterstützt wird, ein kritischer Dienst im Sinne des BSI-Gesetzes ist. Ist nämlich der Dienst selbst nicht kritisch, ist auch der diesen „unkritischen“ Dienst unterstützende Vertrauensdienst nicht kritisch. Insoweit sollte die KRITIS VO nur solche Vertrauensdienste umfassen, bei deren Ausfall oder Beeinträchtigung zugleich auch kritische Dienste beeinträchtigt werden oder ausfallen. Zudem sei darauf hingewiesen, dass der Bereich der Vertrauensdienste bereits umfassend in einer Vielzahl von Vorschriften, und deshalb unübersichtlich, geregelt ist (Zertifizierung nach BSI-IT-Grundschutz (BSI 100-2), BSI Secure CA operation (TR-03145), Akkreditierter Betrieb nach SigG/ SigV mit Aufsichtsbehörde BNetzA, ETSI 102.042 Zertifizierung, Webtrust/ CA/Browser Forum, eIDAS). Weitere gesetzliche Regelungen steigern diese Unübersichtlichkeit und gehen zulasten der Handhabbarkeit und der praktischen Umsetzung, ohne deswegen einen Mehrwert zu bieten.

Bemessungskriterium für Trust-Center im Sektor IKT - Anhang 4, Teil 3, Ziffer 2.3.1

Eine Festlegung auf eine konkrete Technologien (hier: TLS) in der Rechtsverordnung erscheint fraglich. In der technischen Entwicklung können sich immer wieder neue Standards zur Absicherung etablieren oder es kann zu einer Weiterentwicklung und Neubenennung von bestehenden Verfahren kommen (z. B. SSL / TLS). Hier sieht Bitkom das Potential, durch einen Verzicht auf diese Konkretisierung und eine Anpassung des Schwellenwertes im Falle eines erneuten Technologiesprunges auf eine Änderung der Rechtsverordnung verzichten zu können. Alternativ kann auf den jeweiligen Stand der IT-Sicherheit referenziert werden. Dieser müsste vom BSI durch eine Veröffentlichung bekannt gegeben werden.

Weiterhin sieht Bitkom hier Konkretisierungsbedarf in Hinblick auf die genannten Bemessungskriterien. Sowohl die Anzahl an personengebunden Zertifikaten, als auch die Anzahl ausgegebener Zertifikate als alleiniges Kriterium sind nicht geeignet um einer Kritische Infrastruktur zuverlässig zu identifizieren: Andernfalls würden beispielsweise auch Produkthersteller, die ihre Produkte zur Erstkonfiguration mit selbsterstellten Zertifikaten ausliefern, von der Rechtsverordnung erfasst. Aus Bitkom-Sicht ist also dringend sicherzustellen, dass hier als Voraussetzung auch die Anlagenbezeichnung „Trust-Center“ zutreffend ist.
Es gilt zu verhindern, dass aufgrund der qualitativen Kriterien (Anzahl der ausgegebenen Zertifikate) ein Betreiber einer Infrastruktur, der nicht als kritisch im Sinne der Rechtsverordnung gelten kann (wie zum Beispiel Produkthersteller im Consumer-Markt, Verlagshäuser und zivilgesellschaftliche Organisationen), durch die Verordnung zum Trust-Center erhoben wird.

Erfüllungsaufwand für die Wirtschaft

Die Berechnungsgrundlage für den Erfüllungsaufwand für die Wirtschaft fehlt. Die Schätzung erscheint sehr subjektiv. Insbesondere bei dem Bearbeitungsaufwand von 660 Euro pro Meldung fehlt die Grundlage. Fixkosten, die sich durch die Sicherstellung der Meldefähigkeit ergeben, werden nicht berücksichtigt. Die hier durchgeführte Kalkulation könnte den Eindruck erwecken, dass keine Meldung keine Kosten verursachen. Das Gegenteil wäre richtig. Entscheidende Kostenfaktoren sind erfahrungsgemäß stets die Festlegung und Aufrechterhaltung eines Prozesses, weniger die Bearbeitung eines einzelnen Vorkommnisses.