Universität Bremen

✉ Universität Bremen · **Fachbereich 06** · Postfach 33 04 40 · 28334 Bremen

Bundesministerium des Innern, für Bau
und Heimat

nachrichtlich per E-Mail

Fachbereich 06
Rechtswissenschaft

Dr. Dennis-Kenji Kipker

Universitätsallee(gegenüber
Universum)
GW 1, Raum 2010
28359 Bremen

Telefon (0421) 218 – 66049
Fax (0421) 218 – 66052
eMail kipker@uni-bremen.de

Ihr Zeichen:	Ihre Nachricht vom:	Unser Zeichen:	Datum: 02.12.20

Dr. Dennis-Kenji Kipker

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

Das IT-SiG 2.0 hat es sich zum Ziel gesetzt, die Cyber- und Informationssicherheit als ein Schlüsselthema für Staat, Wirtschaft und Gesellschaft im Besonderen zu fördern. Der aktuelle Referentenentwurf basiert auf der vorliegenden dritten Entwurfsfassung (Stand Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat vom 01.12.2020, „Diskussionsentwurf“), die am 19.11.2020 veröffentlicht wurde. Inhaltlich greift das IT-SiG 2.0 die inhaltlichen Regelungen auf, die schon 2015 mit dem ersten IT-SiG getroffen wurden, und versucht insbesondere auch die Erfahrung bei der Umsetzung dieser Regelungen zu berücksichtigen. Überdies fließen neue technologische und gesellschaftspolitische Dimensionen der Nutzung und Vernetzung von IT-Systemen in die Erwägungen ein. Das bisherige Gesetzgebungsverfahren war von erheblicher öffentlicher Wahrnehmung und einem umfassenden Diskurs geprägt, der seit der Veröffentlichung des ersten Referentenentwurfes im April 2019 fortdauert. Aufgrund der Kürze der zur Verfügung stehenden Zeit wird in dieser Stellungnahme nur auf zentrale Auffälligkeiten und Kritikpunkte Bezug genommen.

- **„Unternehmen im besonderen öffentlichen Interesse“:** Schon kurz nach Inkrafttreten des IT-SiG aus 2015 wurden rechtspolitische Forderungen laut, auch solche Unternehmen in den Regelungsbereich einzubeziehen, die zwar keine Kritischen Infrastrukturen als solche sind, bei denen ein Ausfall jedoch erhebliche volkswirtschaftliche Beeinträchtigungen zur Folge haben kann. Auch in der gegenwärtigen Entwurfsfassung findet sich ein solcher Regelungsvorschlag wieder. Die Aufnahme einer neuen Kategorie von „Unternehmen im besonderen öffentlichen Interesse“ ist jedoch abzulehnen. Zuvorderst stellt sich schon per Definition die Frage, worin die genauen Messbarkeitskriterien bestehen sollen, an die man die „erhebliche volkswirtschaftliche Bedeutung“ anknüpft. Zwar ist es begrüßenswert, dass der dritte Entwurf gegenüber der zweiten Entwurfsfassung deutlich konkreter geworden ist, und nicht mehr nur abstrakt von einer Rechtsverordnung zur Bestimmung die Rede ist, gleichwohl sind die Maßstäbe nach wie vor zu unbestimmt. Gerade auch im Vergleich zu den Kritischen Infrastrukturen, die durch ihre Sektoren und Branchen deutlich konkreter umgrenzt sind, ist der Kreis von Unternehmen mit erheblicher volkswirtschaftlicher Bedeutung deutlich schwacher umrissen. Überdies suggeriert ein derartiger Vorschlag, dass derlei Unternehmen bis dato keinerlei rechtlichen Pflichten zur Cybersecurity unterliegen, was rechtlich nicht der Fall ist. Nicht zuletzt sollte überlegt werden, ob tatsächlich eine Notwendigkeit besteht, sämtliche Maßnahmen über das BSI zu koordinieren, oder es nicht teils inhaltlich näherliegt, eine entsprechende Koordinierung über Fachbehörden durchzuführen, um den inhaltlichen Zuschnitt der KRITIS-Regelungen nicht zu verwässern.

- **Tätigkeit des BSI als nationale Cybersicherheitszertifizierungsbehörde/Abgrenzung zum freiwilligen IT-Sicherheitskennzeichen:** Richtigerweise sollen mit dem IT-SiG 2.0 die Aufgaben und Befugnisse gem. EU Cybersecurity Act (VO EU 2019/881) an das BSI übertragen werden, indem dieses als nationale Cybersicherheitszertifizierungsbehörde fungiert. Völlig unklar ist jedoch, warum darüber hinausgehend für kongruente europäische Regelungen zusätzliche nationale Alleingänge erforderlich sind. Dies betrifft zum einen die eigene Entwicklung und Veröffentlichung eines Stands der Technik für sicherheitstechnische Anforderungen an IT-Produkte, mehr noch aber das „freiwillige IT-Sicherheitskennzeichen“. Hier ist nicht erkennbar, welchen Mehrwert dieses Gütesiegel gegenüber einer EU-Cybersicherheitszertifizierung der niedrigsten Stufe bringen soll, die gerade auch für das B2C-Segment einschlägig sein dürfte. Ganz im Gegenteil, durch derlei nationale Alleingänge wird der Wirkkraft europäischer Bestimmungen geschadet, es werden Mehraufwände für Unternehmen geschaffen, und der Verbraucher sieht sich einer immer größer werdenden Zahl an Gütesiegeln ausgesetzt, womit das einzelne Siegel an Wert verliert. Daher wird empfohlen, das freiwillige IT-Sicherheitskennzeichen ersatzlos aus dem Entwurf zu streichen.

- **Verarbeitung von Protokolldaten und Bestandsdatenauskunft:** Festgesetzt werden umfassende Speichermöglichkeiten für Protokoll- und Bestandsdaten inkl. IP-Adressen. Generell sollte in diesem Zusammenhang überdacht werden, die Datenverarbeitungsbefugnisse nicht mehr als unbedingt notwendig auszudehnen und

informationelle Freiheit und Interessen öffentlicher Sicherheit in einen angemessenen Ausgleich zu bringen. Die gegenwärtigen Regelungsvorschläge rücken von einem derartigen angemessenen Interessenausgleich zunehmend zugunsten der IT-Sicherheit ab. Auch ist allgemein anzuregen, die Regelungen zur Abbedingung von datenschutzrechtlichen Betroffenenrechten aus der EU DS-GVO, die 2019 im Zuge des 2. DSAnpUG-EU Eingang in das BSIG fanden, im Sinne des Datenschutzes zu revidieren.

- **Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden:** Auch der sog. „Hackerparagraph" ist in der jüngsten Entwurfsfassung erhalten geblieben, demgemäß nach wie vor aktive Detektionsmaßnahmen zu den ausgebauten Befugnissen des BSI gehören sollen. Die Maßnahmen, die sich auf die IT des Bundes oder von Kritischen Infrastrukturen, digitalen Diensten oder Unternehmen im besonderen öffentlichen Interesse beziehen können, müssen sich auf das Notwendige beschränken. Eingegriffen werden kann in ungeschützte IT-Systeme. Dies sind solche, auf denen öffentlich bekannte Sicherheitslücken bestehen oder bei denen aufgrund sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf das System zugegriffen werden kann. Schon im Vorfeld wurde diese Vorschrift verschiedentlich erheblich kritisiert, da die aktiven Detektionsmaßnahmen des BSI ohne Vorankündigung stattfinden können und sich dadurch (weitergehende) Schäden an IT-Systemen nicht ausschließen lassen. Soweit eine solche aktive Detektionsmöglichkeit vorgesehen wird, sollte daher unbedingt eine Vorankündigung der Detektionsmaßnahmen Eingang in das Gesetz finden.

- **Untersagung des Einsatzes kritischer Komponenten:** Eine zentrale Regelung des neuen Entwurfs betrifft den Einsatz der kritischen Komponenten. Der Einsatz solcher Komponenten, für die aufgrund einer gesetzlichen Regelung eine Zertifizierungspflicht besteht, sind durch den Betreiber einer Kritischen Infrastruktur gegenüber dem BMI vor dem Einsatz anzuzeigen. Die schon aus den anderen Entwurfsfassungen bekannte Garantieerklärung inkl. des Lieferkettennachweises des Herstellers von kritischen Komponenten wurde auch im dritten RefE beibehalten. Das BMI legt federführend die Mindestanforderungen an die Garantieerklärung durch Allgemeinverfügung fest. Außerdem soll das BMI nach wie vor die Befugnis erhalten, den Einsatz einer kritischen Komponente gegenüber dem Betreiber einer Kritischen Infrastruktur zu untersagen, wenn dem überwiegende öffentliche Interessen – insbesondere sicherheitspolitische Interessen – entgegenstehen. Die Untersagungsbefugnis betrifft nicht nur die Entscheidung über den Einsatz, sondern auch über den weiteren Betrieb der kritischen Komponente. Genannt werden in diesem Zusammenhang verschiedene alternative Anforderungen, wann der Hersteller einer kritischen Komponente nicht vertrauenswürdig ist. Die vorliegende Regelung ist ersatzlos zu streichen. Nicht nur, dass es höchst fraglich ist, ob Hersteller diese Anforderungen tatsächlich erfüllen können, auch stellt sich die Frage, ob damit nicht vornehmlich den landeseigenen Herstellern kaum erfüllbare Nachweise auferlegt werden. Durch den Regelungsvorschlag der Garantieerklärung wird die bisher vielfach fruchtlose

politische Debatte um „digitale Souveränität“ mit konkreten, aber nicht wirklich zu erfüllenden Pflichten in ein Gesetz verlagert. Damit ist niemandem ein Gefallen getan.

- **Bußgeldvorschriften:** Der zweite RefE sah für die Bußgeldvorschriften einen Gleichlauf mit der EU DS-GVO vor, der jedoch für die dritte Entwurfsfassung nicht mehr gegeben ist – gleichwohl sind die vorgeschlagenen Sanktionen erheblich und gehen über das bisherige Maß deutlich hinaus, so sind für bestimmte Fälle Geldbußen bis zu 2 Millionen Euro möglich. Weitere Abstufungen sind 1 Million Euro und 100.000 Euro. Über den Verweis auf § 30 OWiG ist überdies eine maximale Geldbuße von bis zu 20 Millionen Euro möglich. Aufgrund dieser Unübersichtlichkeit sollte der Bußgeldkatalog wieder in die Fassung des zweiten Referentenentwurfs gebracht werden. Auf diese Weise wäre auch der Gleichklang mit den datenschutzrechtlichen Regelungen aus der EU DS-GVO wieder hergestellt.

Bremen, den 2. Dezember 2020

Dr. Dennis-Kenji Kipker