Anlage

Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Absatz 1 NKRG

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (NKR-Nr. 4792, BMI)

Der Nationale Normenkontrollrat hat den Entwurf des oben genannten Regelungsvorhabens geprüft.

I. Zusammenfassung

Bürgerinnen und Bürger	Keine Auswirkungen
Wirtschaft	
Jährlicher Erfüllungsaufwand:	rund 21,6 Mio. Euro
davon aus Informationspflichten:	*rund 350.000 Euro*
Einmaliger Erfüllungsaufwand:	rund 40.000 Euro
Verwaltung	
Bund	
Jährlicher Erfüllungsaufwand:	rund 202 Mio. Euro
Einmaliger Erfüllungsaufwand:	rund 32 Mio. Euro
'One in one out'-Regel	Im Sinne der ‚One in one out'-Regel der Bundesregierung stellt der jährliche Erfüllungsaufwand der Wirtschaft in diesem Regelungsvorhaben ein „In" von 21,6 Mio. Euro dar.
Evaluierung	Das Regelungsvorhaben wird vier Jahre nach der Verkündung unter Einbeziehung wissenschaftlicher Expertise evaluiert.
Ziele:	Verbesserung des Schutzes der IT der Bundesverwaltung, der kritischen Infrastrukturen, der Unternehmen im besonderen öffentlichen Interesse und der Verbraucher.
Kriterien/Indikatoren:	z.B. abgewehrte Schadprogramm-Angriffe auf die Bundesverwaltung, Anzahl der von KRITIS-Betreibern gemeldeten (abgewehrten) Angriffe und Verbreitung des IT-Sicherheitskennzeichens, Entwicklung der Gesamtzahlen zu Cybercrime sowie die Anzahl der dem BSI bekannt gewordenen Cyberangriffe. Die detaillierten Kriterien und das Untersuchungsdesign werden unter Einbezie-

	hung wissenschaftlicher Expertise frühzeitig, d.h. mit Beginn des Personalaufbaus, erarbeitet und festgelegt.
Datengrundlage:	Daten des BSI, der Bundesverwaltung, der Interessenverbände der KRITIS-Betreiber, des Statistischen Bundesamtes sowie die Kriminalstatistik. Zudem wird durch das Regelungsvorhaben die ursprünglich für Juni 2021 vorgesehene Evaluation des IT-Sicherheitsgesetzes von 2015 verschoben (vgl. II.3.).

Bei der Vorbereitung dieses Regelungsvorhabens wurde in **mehrfacher Hinsicht gegen die Grundsätze Besserer Rechtsetzung verstoßen.** Derartige Verstöße haben - trotz wiederholter Beanstandungen durch den Nationalen Normenkontrollrat (NKR) - in den letzten Monaten in bedenklicher Weise zugenommen. Im Rahmen seines Mandats erhebt der NKR ein Mal mehr Bedenken gegen die bewusst in Kauf genommene Nichtbeachtung der Regeln der Gemeinsamen Geschäftsordnung der Bundesministerien.

Die Ressorts haben einen erheblichen Stellenmehrbedarf angemeldet und diesen den entsprechenden Vorgaben des Gesetzes – gesondert nach Laufbahnen – zugeordnet. Inwieweit die angemeldeten Stellenbedarfe dem nur durch das vorliegende Regelungsvorhaben hervorgerufenem Erfüllungsaufwand entsprechen, ist für den NKR im Einzelnen nicht nachvollziehbar. Hinzu kommt, dass nicht alle Ressorts Rückmeldungen zum Erfüllungsaufwand gegeben haben. Insgesamt muss daher von einer **erheblichen Unsicherheit** bei der Schätzung ausgegangen werden.

Der erste Entwurf des Regelungsvorhabens lag bereits im März 2019 vor, jedoch ist **die Schlussabstimmung unter großer Eile und enger Fristsetzung** erfolgt. Zugleich sah die formale Länder- und Verbändebeteiligung eine Rückmeldefrist von nur einem Tag vor. Auch unter Hinzunahme des zugänglich gemachten vorläufigen Diskussionsentwurfes ergibt sich lediglich eine Rückmeldefrist von etwa sechs Werktagen. Aus Sicht des NKR lässt ein so enger Zeitplan eine wirksame Einbeziehung der Länder und Verbände sowie die Prüfung der eingegangenen Stellungnahmen durch das Ressort nicht zu. Auskömmliche Rückmeldefristen sind für die Gestaltung adressatenorientierten Rechts aus Sicht des NKR unabdingbar. **Anderenfalls sind Beteiligungen eine reine Formalie.**

Der NKR stellt ferner fest, dass die im Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme von 2015 **vorgeschriebene, wissenschaftlich begleitete Evaluation, die für Sommer 2021 vorgesehen war, durch das vorliegende Regelungsvorhaben verschoben wird.** Das Ressort führt dazu aus, dass die zu evaluierenden Vorgaben mit dem vorliegenden Regelungsvorhaben basierend auf Rückmeldungen aus der Praxis teilweise angepasst würden. Dem Grundsatz der Besseren Rechtsetzung, Regelungen zunächst zu evaluieren und erst anschließend zu überarbeiten ('evaluate first' principle), wird damit nicht entsprochen.

II. Im Einzelnen

Gemäß dem Koalitionsvertrag für die 19. Legislaturperiode wird das IT-Sicherheitsgesetz fortgeschrieben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) soll als

nationale Cybersicherheitsbehörde ausgebaut und in seiner Rolle als Beratungsstelle für Fragen der IT-Sicherheit gestärkt werden.

Folgende Änderungen sind vorgesehen:

- Einführung weiterer Prüf- und Kontrollbefugnisse für das BSI. Neben den Stellen des Bundes gelten die durch das BSI festgelegten Mindeststandards künftig auch für IT-Dienstleister, die Dienstleistungen für die Kommunikationstechnik des Bundes erbringen.
- Erlaubnis für das BSI zur Detektion von Schadprogrammen zum Schutz der Regierungsnetze. Damit kann das BSI nach Sicherheitslücken suchen und die Betroffenen informieren. Darüber hinaus darf das BSI künftig Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden einsetzen.
- Das BSI kann künftig Auskunft über Bestandsdaten von Telekommunikationsdienstleistungen verlangen, um Betreiber Kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und Anbieter digitaler Dienste über Sicherheitslücken und Angriffe informieren zu können.
- Schaffung einer Anordnungsbefugnis des BSI gegenüber Telekommunikations- und Telemedienanbietern zur Abwehr spezifischer Gefahren für die Informationssicherheit. Diese müssen die erforderlichen technischen und organisatorischen Maßnahmen ergreifen, um einen ordnungsgemäßen Zustand ihrer Angebote wiederherzustellen, wenn diese Angebote unzureichend gesichert sind.
- Ausweitung der bestehenden Meldepflichten und verpflichtenden Mindeststandards für Betreiber Kritischer Infrastrukturen auf Unternehmen im besonderen öffentlichen Interesse, u.a. Unternehmen der Rüstungsindustrie und Unternehmen mit besonderer volkswirtschaftlicher Bedeutung.
- Schaffung von Eingriffsbefugnissen (umfassende Prüfmöglichkeit) für den Einsatz und Betrieb kritischer Komponenten.
- Etablierung von Verbraucherschutz im Bereich der Informationssicherheit als zusätzliche Aufgabe des BSI.
- Schaffung der Voraussetzungen für ein einheitliches freiwilliges IT-Sicherheitskennzeichen, das die IT-Sicherheit von Produkten sichtbar machen soll.
- Überarbeitung des Bußgeldregimes.

II.1. Erfüllungsaufwand

Das Ressort hat den Erfüllungsaufwand in Kooperation mit dem Statistischen Bundesamt geschätzt und dargestellt.

Bürgerinnen und Bürgern entsteht durch das Regelungsvorhaben kein Erfüllungsaufwand.

Wirtschaft

Der Wirtschaft entsteht geschätzt **laufender** Erfüllungsaufwand in Höhe von 21,6 Millionen Euro. Der **einmalige** Erfüllungsaufwand wird auf rund 40.000 Euro beziffert. Die Schätzung basiert mangels empirischer Daten in erheblichem Maße auf Annahmen. Die vom Ressort genannten Werte sind daher als Mindestwerte zu verstehen.

Der Aufwand wird im Wesentlichen durch die folgenden zwei Vorgaben verursacht:

§ 8a Absatz 1a BSIG-E: Verpflichtender Einsatz von Systemen zur Angriffserkennung bei Betreibern Kritischer Infrastruktur

Betreiber Kritischer Infrastrukturen werden verpflichtet, Systeme zur Angriffserkennung einzusetzen und bestimmte Daten für mindestens vier Jahre zu speichern. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollen dazu in der Lage sein, Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dafür wird ein personeller Aufwand von **jährlich** rund einer Million Euro geschätzt. Hinzu kommen **jährliche** Sachkosten von 11,8 Millionen Euro.

§ 109 Absatz 2 TKG-E: Zertifizierung kritischer Komponenten im Bereich der Telekommunikationsnetze

Kritische Komponenten im Bereich der Telekommunikationsnetze und –dienste dürfen nur eingesetzt werden, wenn Sie ein Zertifizierungsverfahren durchlaufen haben. Das Zertifizierungsverfahren muss hierbei eng durch die Hersteller begleitet werden. Der Wirtschaft entsteht geschätzt **jährlicher** Personalaufwand in Höhe von rund 2,3 Millionen Euro. Hinzu treten **jährliche** Sachkosten von geschätzt rund sechs Millionen Euro. Es wird von 100.000 Euro Sachkosten pro Fall bei 60 Fällen jährlich ausgegangen. Der Zeitaufwand pro Fall wird auf 18 Stunden geschätzt.

Der übrige Erfüllungsaufwand wird im Wesentlichen durch kleinteilige Antragsverfahren sowie Datenspeicher-, Melde- und Informationspflichten verursacht, die das Ressort in der Begründung des Regelungsvorhabens aufschlüsselt.

Verwaltung (Bund)

Die Schätzung des Erfüllungsaufwandes der Verwaltung beruht auf Rückmeldungen der Ressorts zu den für die jeweiligen Aufgaben benötigten Stellen. Der angemeldete Stellenbedarf wurde zur Darstellung des Erfüllungsaufwandes in Personenjahre (entspricht acht Stunden pro Tag und 200 Arbeitstagen pro Jahr) umgerechnet.

Die Ressorts haben einen erheblichen Stellenmehrbedarf angemeldet und diesen den entsprechenden Vorgaben des Gesetzes – gesondert nach Laufbahnen – zugeordnet (vgl. Tabelle 1). Die einzelnen Darstellungen finden sich detailliert im Begründungsteil des Regelungsvorhabens.

Insgesamt wird ein Aufwand von rund 1.584 Stellen (714 höherer Dienst; 774 gehobener Dienst; 96 mittlerer Dienst) mit einem jährlichen Erfüllungsaufwand in Höhe von rund 202 Millionen Euro ausgewiesen. Davon entfallen rund 133 Millionen Euro auf jährliche Personalkosten und rund 69 Millionen Euro auf jährliche Sachkosten. Der einmalige Erfüllungsaufwand beträgt geschätzt rund 32 Millionen Euro.

Tabelle 1: Überblick zum gemeldeten Stellenmehrbedarf

Ressort einschließlich Geschäftsbereich	**Stellen**	**Davon:**		
		Höherer Dienst	**Gehobener Dienst**	**Mittlerer Dienst**
Bundesministerium des Innern, für Bau und Heimat (BMI)	873	561	309	3
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)	15	9	6	-
Auswärtiges Amt (AA)	51	14	29	8
Bundesministerium für Arbeit und Soziales (BMAS)	15	4	11	-
Bundesministerium der Finanzen (BMF)	278	20	247	11
Bundesministerium für Gesundheit (BMG)	5	3	2	-
Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)	9,3	0,5	8	1
Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU)	32	4	28	-
Bundesministerium für Verkehr und digitale Infrastruktur (BMVI)	254,5	85,5	109	60
Bundesministeriums für Wirtschaft und Energie (BMWi)	34	3,5	18,5	12
Bundeskanzleramt (BKAmt)	17	9	7	1

Die drei größten Aufwände betreffen im Wesentlichen:

Geschäftsbereich des BMI - Bundesamt für Sicherheit in der Informationstechnik

Angemeldet wurden 799 Stellen (533 hD, 266 gD). Es entstehen jährlicher Personalaufwand von rund 74 Millionen Euro sowie jährliche Sachkosten von rund 50 Millionen Euro. Hinzu kommen einmalige Sachkosten von 28 Millionen Euro. Ursächlich sind die vielfältigen neuen Aufgaben des BSI, u.a. die Förderung des Verbraucherschutzes und der Verbraucherinformation im Bereich der Informationssicherheit oder die Begleitung von Digitalisierungsvorhaben der Bundesverwaltung.

Geschäftsbereich des BMF

- Informationstechnikzentrum Bund: Angemeldet wurden 184 Stellen (16 hD, 168 gD). Dies entspricht einem jährlichen Personalaufwand von rund 13 Millionen Euro sowie jährlichen Sachkosten von rund fünf Millionen Euro. Der Bedarf wird im Regelungsentwurf nicht näher begründet.
- Zollverwaltung: Es wurden 83 Stellen angemeldet (3 hD, 72 gD, 8 mD). Dies entspricht einem jährlichen Personalaufwand von rund sechs Millionen Euro sowie jährlichen Sachkosten von rund zwei Millionen Euro. Der Bedarf wird nicht näher begründet.

Geschäftsbereich des BMVI - Wasserstraßen- und Schifffahrtsverwaltung des Bundes

Zur Erfüllung der durch das Gesetz verursachten Verpflichtungen werden 130 Stellen geltend gemacht (41 hD, 60 gD, 30 mD). Dies entspricht einem jährlichen Personalaufwand von rund zehn Millionen Euro sowie jährlichen Sachkosten von rund drei Millionen Euro. Der Aufwand wird laut Entwurf im Wesentlich durch die Verarbeitung behördeninterner Protokollierungsdaten hervorgerufen. Das BSI erhält die Befugnis, zur Abwehr von Gefahren für die Kommunikationstechnik behördeninterne Protokollierungsdaten auszuwerten. Der Wasserstraßen- und Schifffahrtsverwaltung des Bundes entsteht Aufwand durch die Speicherung der Daten, die für die Verarbeitung notwendige Pseudonymisierung sowie sonstige Zuarbeiten.

Inwieweit die angemeldeten Stellenbedarfe dem nur durch das vorliegende Regelungsvorhaben hervorgerufenem Erfüllungsaufwand entsprechen, ist für den NKR im Einzelnen nicht nachvollziehbar. Hinzu kommt, dass nicht alle Ressorts Rückmeldungen zum Erfüllungsaufwand gegeben haben. Insgesamt muss daher von einer erheblichen Unsicherheit bei der Schätzung ausgegangen werden.

II.2. ‚One in one out'-Regel

Im Sinne der ‚One in one out'-Regel der Bundesregierung stellt der jährliche Erfüllungsaufwand der Wirtschaft in diesem Regelungsvorhaben ein „In" von rund 21,6 Millionen Euro dar.

II.3. Evaluierung

Vier Jahre nach der Verkündung soll das Regelungsvorhaben - mit Ausnahme der bereits nach zwei Jahren zu überprüfenden Regelungen zur Kritischen Infrastruktur (§§ 2 Absatz 10, 8a bis 8c und § 8e sowie § 10 BSIG) - unter Einbeziehung wissenschaftlicher Expertise evaluiert werden. Dabei soll im Wesentlichen überprüft werden, ob die mit den Neurege-

lungen verfolgten **Ziele**, die Verbesserung des Schutzes der IT der Bundesverwaltung, der Kritischen Infrastrukturen, der Unternehmen im besonderen öffentlichen Interesse und der Verbraucher, erreicht wurden. **Indikatoren** zur Messung der Zielerreichung können z.B. abgewehrte Schadprogramm-Angriffe auf die Bundesverwaltung, die Anzahl der von KRITIS-Betreibern gemeldeten (abgewehrten) Angriffe, die Verbreitung des IT-Sicherheitskennzeichens, die Entwicklung der Gesamtzahlen zu Cybercrime sowie die Anzahl der BSI bekannt gewordenen Cyberangriffe sein. Die detaillierten Kriterien und das Untersuchungsdesign werden unter Einbeziehung wissenschaftlicher Expertise frühzeitig, d.h. mit Beginn des Personalaufbaus, erarbeitet und festgelegt. **Datengrundlage** sind Daten des BSI, der Bundesverwaltung, der Interessenverbände der KRITIS-Betreiber, des Statistischen Bundesamtes sowie die Kriminalstatistik.

Zudem sollen bereits zwei Jahre nach Verkündung des vorliegenden Regelungsvorhabens die Vorgaben mit Bezug zur Kritischen Infrastruktur (§§ 2 Absatz 10, 8a bis 8c und § 8e sowie § 10 BSIG) unter Einbeziehung von wissenschaftlichem Sachverstand **evaluiert** werden. Diese Evaluation war bereits im IT-Sicherheitsgesetz vom 17. Juli 2015 festgelegt worden und ursprünglich im Juni 2021 vorgesehen, d.h. vier Jahre nach Inkrafttreten der Verordnung zur Bestimmung Kritischer Infrastrukturen. Laut Ressort haben Erfahrungen aus der Praxis mittlerweile einen umfangreichen Änderungsbedarf am BSIG aufgezeigt, der sich teilweise auch direkt auf die zu evaluierenden Vorschriften beziehe. Dieser Änderungsbedarf werde ferner mit dem vorliegenden Regelungsvorhaben teilweise umgesetzt. Die Evaluation werde verschoben, um die durch das vorliegende Regelungsvorhaben erfolgten Anpassungen einbeziehen zu können. Bei der Evaluation soll überprüft werden, ob das Ziel des IT-Sicherheitsgesetzes, die Verbesserung des Schutzes Kritischer Infrastrukturen, erreicht worden ist. Die Evaluierung erfolgt auf der Grundlage von Daten des BSI, der Bundesverwaltung, der Interessenverbänden der Betreiber Kritischer Infrastrukturen sowie des Statistischen Bundesamts.

III. Ergebnis

Bei der Vorbereitung dieses Regelungsvorhabens wurde in **mehrfacher Hinsicht gegen die Grundsätze Besserer Rechtsetzung verstoßen**. Derartige Verstöße haben - trotz wiederholter Beanstandungen durch den Nationalen Normenkontrollrat (NKR) - in den letzten Monaten in bedenklicher Weise zugenommen. Im Rahmen seines Mandats erhebt der NKR ein Mal mehr Bedenken gegen die bewusst in Kauf genommene Nichtbeachtung der Regeln der Gemeinsamen Geschäftsordnung der Bundesministerien.

Die Ressorts haben einen erheblichen Stellenmehrbedarf angemeldet und diesen den entsprechenden Vorgaben des Gesetzes – gesondert nach Laufbahnen – zugeordnet. Inwieweit die angemeldeten Stellenbedarfe dem nur durch das vorliegende Regelungsvorhaben hervorgerufenem Erfüllungsaufwand entsprechen, ist für den NKR im Einzelnen nicht nachvollziehbar. Hinzu kommt, dass nicht alle Ressorts Rückmeldungen zum Erfüllungsaufwand gegeben haben. Insgesamt muss daher von einer **erheblichen Unsicherheit** bei der Schätzung ausgegangen werden.

Der erste Entwurf des Regelungsvorhabens lag bereits im März 2019 vor, jedoch ist **die Schlussabstimmung unter großer Eile und enger Fristsetzung** erfolgt. Zugleich sah die formale Länder- und Verbändebeteiligung eine Rückmeldefrist von nur einem Tag vor. Auch unter Hinzunahme des zugänglich gemachten vorläufigen Diskussionsentwurfes ergibt sich lediglich eine Rückmeldefrist von etwa sechs Werktagen. Aus Sicht des NKR lässt ein so enger Zeitplan eine wirksame Einbeziehung der Länder und Verbände sowie die Prüfung der eingegangenen Stellungnahmen durch das Ressort nicht zu. Auskömmliche Rückmeldefristen sind für die Gestaltung adressatenorientierten Rechts aus Sicht des NKR unabdingbar. **Anderenfalls sind Beteiligungen eine reine Formalie.**

Der NKR stellt ferner fest, dass die im Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme von 2015 **vorgeschriebene, wissenschaftlich begleitete Evaluation, die für Sommer 2021 vorgesehen war, durch das vorliegende Regelungsvorhaben verschoben wird.** Das Ressort führt dazu aus, dass die zu evaluierenden Vorgaben mit dem vorliegenden Regelungsvorhaben basierend auf Rückmeldungen aus der Praxis teilweise angepasst würden. Dem Grundsatz der Besseren Rechtsetzung, Regelungen zunächst zu evaluieren und erst anschließend zu überarbeiten ('evaluate first' principle), wird damit nicht entsprochen.

Dr. Ludewig
Vorsitzender

Prof. Dr. Kuhlmann
Berichterstatterin