Stellungnahme
des GKV-Spitzenverbandes vom 04.07.2025

---

zum Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

GKV-Spitzenverband
Reinhardtstraße 28
10117 Berlin
Telefon 030 206288-0
politik@gkv-spitzenverband.de
www.gkv-spitzenverband.de

Inhaltsverzeichnis

I. Vorbemerkung 3

II. Stellungnahme 4

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen 4

§ 32 Meldepflichten 5

§ 33 Registrierungspflicht 6

§ 35 Unterrichtungspflichten 7

§ 39 Nachweispflichten 9

§ 41 Untersagung des Einsatzes kritischer Komponenten 11

§ 64 Zuwiderhandlungen durch Institutionen der sozialen Sicherung 13

Nr. 3 – § 7 Sektor Finanzwesen 14

Nr. 5 – § 8 Sektor Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende 15

I. Vorbemerkung

Der Referentenentwurf des Bundesinnenministeriums zur Umsetzung der EU-Richtlinie NIS-2 zielt auf eine umfassende Stärkung der Cybersicherheit in Deutschland ab. Er erweitert das IT-Sicherheitsgesetz deutlich und führt neue Kategorien wie „kritische Anlagen“, „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ ein. Diese betreffen künftig viele Unternehmen und Institutionen. Dazu gehören auch gesetzliche Krankenkassen, die bisher nicht unter das KRITIS-Regime fielen.

Für die betroffenen Einrichtungen sollen verbindliche Anforderungen an das Risikomanagement, die Meldepflichten, die Registrierung und Nachweise gelten. Dazu zählen u.a. die Durchführung von Risikobewertungen, die Implementierung von Firewalls, Intrusion Detection Systemen, Verschlüsselungstechnologien, Notfallplänen oder regelmäßige Sicherheitsüberprüfungen. Ein dreistufiges Meldeverfahren soll schnelle Reaktionen auf Sicherheitsvorfälle ermöglichen. Die Bundesverwaltung muss Informationssicherheitsbeauftragte benennen und ein zentrales Sicherheitsmanagement etablieren. Das Bundesamt für Sicherheit in der Informationstechnik erhält erweiterte Befugnisse zur Aufsicht und Beratung.

Finanziell entstehen bis 2029 erhebliche Kosten: rund 1,38 Milliarden Euro jährlich für die Bundesverwaltung und 2,2 Milliarden Euro jährlich für die Wirtschaft. Dem steht laut dem vorliegenden Entwurf ein potenziell verhinderter Schaden von 3,6 Milliarden Euro gegenüber. Der Entwurf konkretisiert bestehende Gesetze und integriert europäische Vorgaben, um ein kohärentes Sicherheitsregime zu schaffen.

Kritisch betrachtet der GKV-Spitzenverband die vorgesehenen Regelungen bezüglich etwaiger Zuwiderhandlungen durch Institutionen der sozialen Sicherung. Die Institutionen der sozialen Sicherung sollten von Sanktionen und Bußgeldern explizit ausgenommen werden und es sollte ein eigenständiges, sektorspezifisches Verfahren entwickelt werden, das die Besonderheiten der sozialen Selbstverwaltung und der Beitragsfinanzierung angemessen berücksichtigt.

II. Stellungnahme

Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)
Teil 3 (Sicherheit in der Informationstechnik von Einrichtungen)
Kapitel 2 (Risikomanagement, Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten)

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

A) Beabsichtigte Neuregelung

Die Regelung in Absatz 6 setzt Artikel 24 der NIS-2-Richtlinie um und ermächtigt das Bundesinnenministerium, durch eine Rechtsverordnung den verpflichtenden Einsatz zertifizierter IT-Produkte, -Dienste oder -Prozesse vorzuschreiben. EU-delegierte Rechtsakte haben dabei Vorrang. Vor Erlass einer solchen Verordnung muss sichergestellt werden, dass entsprechende Zertifizierungen existieren und zertifizierte Produkte ausreichend verfügbar sind, um Lieferengpässe zu vermeiden.

B) Stellungnahme

Der GKV-Spitzenverband unterstützt die Regelung in Absatz 6, die den verpflichtenden Einsatz von nach europäischen Schemata zertifizierten IT-Produkten, -Diensten oder -Prozessen ermöglicht. Gleichzeitig weisen wir darauf hin, dass vor Erlass entsprechender Verordnungen sichergestellt sein sollte, dass ausreichend viele zertifizierte Lösungen am Markt verfügbar sind, um Versorgungsengpässe und Umsetzungsprobleme zu vermeiden.

C) Änderungsvorschlag

Keiner.

Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)
Teil 3 (Sicherheit in der Informationstechnik von Einrichtungen)
Kapitel 2 (Risikomanagement, Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten)

§ 32 Meldepflichten

A) Beabsichtigte Neuregelung

Das mehrstufige Meldeverfahren gemäß § 32 zur Umsetzung der NIS-2-Richtlinie sieht ein dreistufiges Melderegime für erhebliche Sicherheitsvorfälle vor. Es ersetzt die bisherige einstufige Meldepflicht und dient der Bürokratieentlastung sowie der besseren Koordination mit anderen Meldepflichten (z. B. im Rahmen des KRITIS-Dachgesetzes).

B) Stellungnahme

Der GKV-Spitzenverband begrüßt die in § 32 Absatz 1 BSIG-E vorgesehene Konkretisierung der Meldepflicht bei erheblichen Sicherheitsvorfällen als wichtigen Beitrag zur Stärkung der Cybersicherheit in kritischen Infrastrukturen und besonders wichtigen Einrichtungen.

Die Klarstellung, dass die Meldefrist mit der Kenntniserlangung durch eine Mitarbeiterin oder einen Mitarbeiter während der Arbeitszeit beginnt, schafft Rechtssicherheit für die betroffenen Einrichtungen.

Besonders begrüßt wird die Möglichkeit, bei konzerninternen Vorfällen eine zentrale Meldung an eine einheitliche Kontaktstelle abzugeben. Dies trägt zur Vermeidung von Doppelmeldungen und damit zur Bürokratieentlastung bei. Voraussetzung hierfür muss jedoch sein, dass die benannte Kontaktstelle auch in der Lage ist, einrichtungs- oder anlagenspezifische Rückfragen des Bundesamts für Sicherheit in der Informationstechnik (BSI) qualifiziert zu beantworten oder entsprechende Ansprechpartner zu benennen.

Der GKV-Spitzenverband unterstützt zudem die Perspektive, die zentrale Meldestelle künftig auch für weitere Meldepflichten – etwa nach der Verordnung (EU) 2022/2554 – zu nutzen. Dies ist ein sinnvoller Schritt in Richtung einer integrierten und effizienten Meldeinfrastruktur.

C) Änderungsvorschlag

Keiner.

Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)
Teil 3 (Sicherheit in der Informationstechnik von Einrichtungen)
Kapitel 2 (Risikomanagement, Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten)

§ 33 Registrierungspflicht

A) Beabsichtigte Neuregelung

§ 33 zur Umsetzung der NIS-2-Richtlinie regelt die Registrierungspflichten für besonders wichtige Einrichtungen, wichtige Einrichtungen sowie Betreiber kritischer Anlagen. Ein zentraler Aspekt dabei ist die Übermittlung öffentlicher IP-Adressen.

B) Stellungnahme

Die vorgesehene Pflicht zur Übermittlung öffentlicher IP-Adressbereiche durch besonders wichtige Einrichtungen, wichtige Einrichtungen und Betreiber kritischer Anlagen ist aus Sicht des GKV-Spitzenverbandes aus mehreren Gründen kritisch zu bewerten:

Unnötiger Administrativer Mehraufwand

Die Registrierungspflicht von IP-Adressen kommt zu den bereits bestehenden Meldepflichten bei Sicherheitsvorfällen nach § 32 des Entwurfs hinzu. Die betroffenen Organisationen müssen zusätzlich zu ihren etablierten Sicherheitsmaßnahmen nun eine weitere Compliance-Schicht bedienen. Die Zugehörigkeit von IP-Adressen zu bestimmten Organisationen ist durch mehrere bereits vorhandene Register feststellbar. Der Nutzen einer weiteren Registratur ist nicht belegbar. Der bürokratische Aufwand ist jedoch erheblich.

Unklare Zweckbindung und Verhältnismäßigkeit

Die Regelung lässt offen, zu welchen konkreten Zwecken die IP-Adressen verwendet werden dürfen. Ohne klare Zweckbindung und technische sowie organisatorische Schutzmaßnahmen besteht die Gefahr einer Zweckentfremdung.

C) Änderungsvorschlag

Die Regelung in § 33 Absatz 2 ist zu streichen.

Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)
Teil 3 (Sicherheit in der Informationstechnik von Einrichtungen)
Kapitel 2 (Risikomanagement, Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten)

§ 35 Unterrichtungspflichten

A) Beabsichtigte Neuregelung

Die vorgesehene Neuregelung zielt darauf ab, die Transparenz und Reaktionsfähigkeit bei erheblichen Sicherheitsvorfällen und Cyberbedrohungen zu verbessern. Besonders wichtige und wichtige Einrichtungen sollen künftig verpflichtet werden, ihre Dienstempfänger unverzüglich zu unterrichten, wenn ein erheblicher Sicherheitsvorfall die Erbringung ihrer Dienste beeinträchtigen könnte. Diese Unterrichtung kann auch durch eine Veröffentlichung auf der Website der Einrichtung erfolgen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kann eine solche Unterrichtung anordnen und informiert in diesem Fall auch die zuständige Aufsichtsbehörde.

B) Stellungnahme

Der GKV-Spitzenverband begrüßt grundsätzlich die geplanten Regelungen zur Verbesserung der IT-Sicherheit im Gesundheitswesen. Insbesondere die Möglichkeit des Bundesamts für Sicherheit in der Informationstechnik (BSI), betroffene Einrichtungen zur unverzüglichen Information ihrer Dienstempfänger zu verpflichten, wird als sachgerecht und notwendig erachtet. In einer zunehmend digitalisierten Versorgungslandschaft ist es essenziell, dass Patientinnen und Patienten sowie andere betroffene Nutzendengruppen frühzeitig über sicherheitsrelevante Vorfälle informiert werden, um eigene Schutzmaßnahmen ergreifen zu können und das Vertrauen in digitale Gesundheitsdienste zu stärken.

Kritisch bewertet der GKV-Spitzenverband hingegen die vorgesehene Pflicht zur proaktiven Information über potenzielle Cyberbedrohungen und entsprechende Gegenmaßnahmen. Zwar kann eine frühzeitige Sensibilisierung zur Erhöhung der Resilienz beitragen, jedoch bestehen Bedenken hinsichtlich der praktischen Umsetzbarkeit und der Verhältnismäßigkeit der Informationspflichten. Die Einschätzung, welche Bedrohungen als erheblich gelten und welche Maßnahmen empfohlen werden sollten, erfordert eine differenzierte Bewertung, die nicht immer eindeutig möglich ist. Zudem besteht die Gefahr, dass durch vorschnelle oder unklare Informationen Unsicherheit bei den Empfängern entsteht. Zudem ist der Begriff einer erheblichen Cyberbedrohung nicht definiert und bedarf einer Schärfung.

Die vorgesehene Interessenabwägung zwischen Einrichtung und Empfänger ist ein wichtiger Schritt, um die Informationspflichten angemessen auszugestalten. Dennoch sieht der GKV-Spitzenverband hier auch den größten Klärungsbedarf, um eine ausgewogene und praktikable Regelung sicherzustellen.

Insgesamt wird die Neuregelung als ein bedeutender Beitrag zur Erhöhung der Transparenz und zur Stärkung der Patientensicherheit gewertet – unter der Voraussetzung, dass die Informationspflichten klar definiert werden und die Informationspflicht nicht auf potenzielle Cyberbedrohungen ausgeweitet wird.

C) Änderungsvorschlag

§35 Absatz 2 wird wie folgt geändert:

„(2) Einrichtungen nach Absatz 1 Satz 1 aus den Sektoren Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, digitale Infrastruktur, Verwaltung von IKT-Diensten und Digitale Dienste teilen den von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste und dem Bundesamt unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Pflichten nach Satz 1 oder 2 gelten nur dann, wenn in Abwägung der Interessen der Einrichtung und des Empfängers die Interessen des Empfängers überwiegen.“

Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)
Teil 3 (Sicherheit in der Informationstechnik von Einrichtungen)
Kapitel 2 (Risikomanagement, Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten)

§ 39 Nachweispflichten

A) Beabsichtigte Neuregelung

§ 39 regelt die Nachweispflichten für Betreiber kritischer Anlagen. Diese Betreiber müssen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) alle drei Jahre nachweisen, dass sie die vorgeschriebenen Sicherheitsmaßnahmen gemäß § 30 Absatz 1 Satz 1 in Verbindung mit § 31 Absatz 1 und 2 umgesetzt haben. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Dabei sind auch aufgedeckte Sicherheitsmängel zu dokumentieren und dem BSI zu melden. Das BSI kann zusätzlich die zugrunde liegende Dokumentation einfordern, die Vorlage eines Mängelbeseitigungsplans verlangen und die Beseitigung der Mängel sowie deren Nachweis einfordern.

Zur Ausgestaltung des Nachweisverfahrens kann das BSI Anforderungen an die Durchführung, die Eignung der Nachweise sowie an die prüfenden Stellen festlegen. Diese Anforderungen werden nach Anhörung der betroffenen Betreiber und Wirtschaftsverbände im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe öffentlich bekannt gemacht.

Für Betreiber, die bereits vor Inkrafttreten des Gesetzes als Betreiber kritischer Infrastrukturen galten, wird der Zeitpunkt der Nachweiserbringung so festgelegt, dass ein kontinuierlicher Dreijahresrhythmus gewahrt bleibt.

B) Stellungnahme

Der GKV-Spitzenverband begrüßt ausdrücklich die im Referentenentwurf vorgesehene Regelung zur Nachweisfrequenz für Betreiber kritischer Anlagen gemäß § 39 BSIG-E. Die Festlegung eines dreijährigen Rhythmus für die Erbringung von Sicherheitsaudits, Prüfungen oder Zertifizierungen stellt eine ausgewogene und praxisgerechte Lösung dar.

Die Verlängerung der Nachweisfrequenz gegenüber früheren Regelungen trägt wesentlich zur Entlastung der betroffenen Einrichtungen bei, ohne dabei die Sicherheit zu gefährden. Sie ermöglicht eine effizientere Ressourcenplanung und schafft Raum für eine nachhaltige Umsetzung von Sicherheitsmaßnahmen. Gleichzeitig bleibt die regelmäßige Kontrolle gewährleistet, sodass weiterhin ein hohes Schutzniveau für kritische Infrastrukturen sichergestellt ist.

Besonders positiv hervorzuheben ist, dass die Regelung eine Differenzierung zwischen neuen und bereits regulierten Betreibern vorsieht und Übergangsfristen berücksichtigt. Dies schafft Rechtssicherheit und verhindert unnötige Doppelbelastungen.

Aus Sicht des GKV-Spitzenverbandes ist die dreijährige Nachweisfrequenz ein sinnvoller Beitrag zur Stärkung der Cybersicherheit bei gleichzeitiger Wahrung der Verhältnismäßigkeit. Sie fördert die Akzeptanz der neuen Anforderungen und unterstützt die Betreiber dabei, ihre Sicherheitsstrategien langfristig und wirksam zu gestalten. Sie ist – insbesondere im Vergleich zu alternativen, weniger

eingriffsintensiven Mitteln wie freiwilliger Registrierung oder pseudonymisierter technischer Erfassung – verhältnismäßig.

C) Änderungsvorschlag

Keiner.

Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)
Teil 3 (Sicherheit in der Informationstechnik von Einrichtungen)
Kapitel 2 (Risikomanagement, Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten)

§ 41 Untersagung des Einsatzes kritischer Komponenten

A) Beabsichtigte Neuregelung

Kritische Komponenten sind laut § 2 Nr. 23 IKT-Produkte, die in kritischen Anlagen eingesetzt werden, bei denen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift als kritische Komponenten bestimmt werden oder eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.

Ein Betreiber hat den geplanten erstmaligen Einsatz einer kritischen Komponente und die geplante Art ihres Einsatzes dem Bundesministerium des Innern anzuzeigen (Absatz 1). Das Bundesministerium kann den erstmaligen Einsatz gegenüber dem Betreiber bis zum Ablauf von zwei Monaten nach Eingang der Anzeige untersagen oder hierzu Anordnungen erlassen. Vor Ablauf der Frist von zwei Monaten ist der Einsatz nicht gestattet. Die Frist kann um weitere zwei Monate verlängert werden, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist (Absatz 2).

Kritische Komponenten dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der kritischen Anlage abgegeben hat. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zweck von Sabotage, Spionage oder Terrorismus, auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einwirken zu können (Absatz 3).

Das Bundesministerium kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen untersagen oder hierzu Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist (Absatz 4).

Wurde der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen (Absatz 6). Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit kann das Bundesministerium den Einsatz aller kritischen Komponenten des Herstellers untersagen (Absatz 7).

B) Stellungnahme

Die Regelung war bisher in § 9b BSIG gefasst und greift stark in den Auswahl- und Vergabeprozess für IKT-Produkte („Gruppe von Elementen eines Netz- oder Informationssystems“ vgl. Art. 2 Nr. 12

Verordnung (EU) 2019/881)) bei kritischen Anlagen ein. Die EU-NIS-2-Richtlinie sieht eine derartige Regelung nicht vor.

Einerseits wird der Auswahl- und Vergabeprozess unter Berücksichtigung der maximalen Frist von vier Monaten (vgl. Absatz 2) stark verlangsamt. Andererseits sind erhebliche zusätzliche Aufwände und bürokratisch induzierte Beschaffungsengpässe bei den deutschen Betreibern kritischer Anlagen zu befürchten. Das bisherige Verfahren hat sich offenbar weder in den Sektoren Telekommunikation noch Energie als geeignetes Mittel bewährt, um die technologische Abhängigkeit bei Schlüsseltechnologien bzw. kritischen IT-Komponenten spürbar und nachhaltig zu verringen (vgl. Positionspapier NIS2UmsuCG, UP KRITIS, Oktober 2023). Das Verfahren im Absatz 1 sollte daher stark vereinfacht und entbürokratisiert werden.

C) Änderungsvorschlag

Der Absatz 1 wird durch folgende Formulierung ersetzt:

„Ein Betreiber kritischer Anlagen hat den geplanten Einsatz einer kritischen Komponente gemäß § 2 Nummer 23 gegen die vom Bundesministerium des Innern zur Verfügung gestellte Negativliste zu prüfen. Sofern zu Beginn des Auswahl- und Vergabeprozesses die kritische Komponente in dieser Liste aufgeführt ist, hat der Betreiber das zugrundeliegende IKT-Produkt mit Verweis auf dieses Gesetz vom Vergabeprozess ausschließen."

Artikel 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)
Teil 7 (Aufsicht)

§ 64 Zuwiderhandlungen durch Institutionen der sozialen Sicherung

A) Beabsichtigte Neuregelung

§ 64 zur Umsetzung der NIS-2-Richtlinie regelt, wie bei Verstößen gegen IT-Sicherheitsvorgaben durch Institutionen der sozialen Sicherung vorzugehen ist. Bei Einrichtungen in Bundeshand oder bundesunmittelbaren Körperschaften mit Selbstverwaltung stimmt sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der zuständigen Aufsichtsbehörde über geeignete Maßnahmen ab. Bei Einrichtungen in Landesträgerschaft oder landesunmittelbaren Körperschaften mit Selbstverwaltung informiert das BSI die jeweilige Landesaufsicht und schlägt Maßnahmen vor. Die Durchsetzung obliegt dann der zuständigen Aufsichtsbehörde, die das BSI über eingeleitete Schritte unterrichtet. Ziel ist eine abgestimmte und wirksame Aufsicht, ohne dass das BSI direkt durchgreift.

B) Stellungnahme

Der GKV-Spitzenverband lehnt die im Zusammenhang mit § 64 vorgesehene Regelung zur Behandlung von Zuwiderhandlungen durch Institutionen der sozialen Sicherung in der vorliegenden Form ab. Einerseits könnte eine mit Bußgeldern belegte Körperschaft bereits durch einen Verstoß gegen die Vorgaben zur Informationssicherheit bei voller Ausschöpfung des Bußgeldrahmens in ihrer wirtschaftlichen Existenz und letztlich in der Wahrnehmung ihrer gesetzlichen Aufgaben bedroht sein. Das Handeln der Verwaltung ist ohnehin an Gesetz und Recht gebunden (Art. 20 Abs. 3 GG), diese darf nach dem Grundsatz der Gesetzmäßigkeit der Verwaltung nicht ohne gesetzliche Ermächtigung und nicht im Widerspruch zu bestehenden gesetzlichen Regelungen handeln. Andererseits würden damit öffentliche Gelder nur von einer Körperschaft auf eine Behörde verlagert, was nicht vom Sinn und Zweck dieses Gesetzes erfasst werden kann.

C) Änderungsvorschlag

§ 64 wird analog zu § 85 a SGB X um folgenden Satz 5 ergänzt:

„Gegen Institutionen der sozialen Sicherung werden keine Bußgelder verhängt.“

Artikel 8 (Änderung der Änderung der BSI-Kritisverordnung)

Nr. 3 – § 7 Sektor Finanzwesen

A) Beabsichtigte Neuregelung

Um die unterbrechungsfreie Identifizierung von KRITIS-Betreibern zu gewährleisten, sollen die sich aus der Novelle des BSI-Gesetzes (Artikel 1) ergebenden Folgeänderungen in der BSI-KritisV umgesetzt werden.

B) Stellungnahme

Die Fassung des Gesetzentwurfes sieht vor, lediglich die Wörter „Versicherungsdienstleistungen und“ in Nummer 5 zu streichen. Damit würden weiterhin „Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitssuchende“ unter den Kritis-Sektor Finanzen fallen und unter Nummer 5 aufgeführt werden. Dabei sieht der Gesetzentwurf vor mit einem neuen „§ 8 Sektor Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende“ einen eigenen Kritis-Sektor für den Bereich der Sozialversicherung zu schaffen. Leider enthält der Entwurf keine Gesetzesbegründung für dieses Vorgehen. Wir gehen davon aus, dass ein Anliegen des Gesetzgebers ist, Rechtsklarheit darüber zu schaffen, welcher Kritis-Sektor für den Bereich der Sozialversicherung Anwendung finden soll. Um sicherzustellen, dass die Sozialversicherungen künftig unter einen Kritis-Sektor fallen, wird eine Streichung vorgeschlagen.

C) Änderungsvorschlag

Streichung von § 7 Abs. 1 Nummer 5 BSI-Kritis-Verordnung.

Artikel 8 (Änderung der Änderung der BSI-Kritisverordnung)

Nr. 5 – § 8 Sektor Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende

A) Beabsichtigte Neuregelung

Die Regelungen in Anlage 6 der Kritis- Verordnung zu Schwellenwerten im Sektor „Finanz- und Versicherungswesen“ werden in einen neuen Sektor „Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende“ übertragen.

B) Stellungnahme

Im vorliegenden Referentenentwurf fehlt die referenzierte Anlage 9. Eine Bewertung zu Auswirkungen auf die Kranken- und Pflegekassen kann daher nicht vorgenommen werden.

C) Änderungsvorschlag

Der Referentenentwurf wird um die fehlende Anlage 9 ergänzt und die Schwellenwerte aus Anlage 6 der BSI-Kritisverordnung werden übertragen.