



BKK Dachverband e.V.
Mauerstraße 85
10117 Berlin

TEL (030) 2700403-200
FAX (030) 2700400-191
politik@bkk-dv.de
www.bkk-dachverband.de

STELLUNGNAHME BKK DACHVERBAND E.V.

vom 24.01.2024

Referentenentwurf

**Entwurf eines Gesetzes zur Umsetzung der
Richtlinie (EU) 2022/2557 und zur Stärkung
der Resilienz von Betreibern kritischer Anla-
gen**

(KRITIS-Dachgesetz – KRITIS-DachG)

I. DETAILKOMMENTIERUNG

Artikel 1

Zu § 4 Abs. 2 KRITIS DachG:

Mit der vierten Verordnung zur Änderung der BSI-KRITIS-Verordnung (4. KRITISÄndVO) wurde der Schwellenwert für die Einstufung im Sektor Finanzen und Versicherungen der Anlagenkategorie Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung von 3.000.000 auf 500.000 Versicherte abgesenkt. In der Begründung des Verordnungsentwurfes wurde die Absenkung des Schwellenwertes unter anderem mit zunehmenden Cyberangriffen auf IT-Dienstleister der gesetzlichen Kranken- und Pflegekassen erklärt. Durch diesen Schritt wurde im Ergebnis eine Registrierung von insgesamt einem Drittel aller gesetzlichen Kranken- und Pflegekassen als Betreiber Kritischer Infrastruktur erreicht.

Kleinere Kassen werden überdies künftig ergänzend im Rahmen des Gesetzentwurfes der Bundesregierung für ein Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) vorgenommenen Neuregelung in § 217f Absatz 4c SGB V erfasst, wonach der GKV-Spitzenverband bis zum 30. Juni 2024 in einer Richtlinie zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme Komponenten oder Prozesse der Krankenkassen für diese verbindlich festlegt.

Es gibt jedoch Kranken- und Pflegekassen, die zwar unter dem o.g. Schwellenwert liegen und zugleich, aufgrund eines regionalen Schwerpunktes in ihrer Versichertenpopulation, für die Gesundheitsversorgung in einer oder mehreren Regionen von herausgehobener Bedeutung sind. Diese werden auch in der Neufassung der KRITIS-Verordnung nicht berücksichtigt.

Zudem lagern einige Gesetzliche Kranken- und Pflegeversicherungen Teilprozesse der durch sie für das Gesundheitswesen erbrachten Dienstleistungen sowie den Betrieb von dafür nötigen IT-Infrastrukturen an Dienstleister aus. Unter den Kassen, auf die dies zutrifft, finden sich viele kleinere Gesetzliche Kranken- und Pflegeversicherungen, die unter dem Regelschwellenwert für die Kritikalität einer Anlage von 500.000 zu versorgenden Einwohnern (§ 4 Abs. 1 KRITIS DachG) liegen. Einige der für sie tätigen IT-Dienstleister werden jedoch von mehreren Kassen zugleich beauftragt und sind durch

die Gesamtzahl der Versicherten ihrer Kunden selbst von essenzieller Bedeutung für die Erbringung kritischer Dienstleistungen für eine deutlich über dem Regelschwellenwert liegende Anzahl von Einwohnern – ohne dass diese Dienstleister bisher eine kritische Infrastruktur im Sinne des KRITIS-DachG darstellen.

Weiterhin ist auch festzuhalten, dass der Gesetzgeber der Gesetzlichen Krankenversicherung zukünftig über die Richtlinie des GKV-Spitzenverbands nach § 217f Absatz 4c SGB V einheitliche Vorgaben zur Vermeidung von Störungen ihrer IT-Systeme vorgeben lässt. Die Ausprägung des Stands der Technik bei den Kassen – und dementsprechend der informationstechnischen Systeme, Komponenten und Prozesse – gestaltet sich jedoch in der Realität häufig sehr individuell, zumal wenn man die o.g. IT-Dienstleister im Gesamtbild berücksichtigt. Eine einheitliche und sinnvolle Anwendbarkeit zentraler Vorgaben ist hierdurch nicht automatisch gegeben.

Aus all diesen Gründen begrüßen die Betriebskrankenkassen die nun mit dem KRITIS-DachG geplante Flexibilisierung bei der Identifizierung von Betreibern kritischer Infrastrukturen in § 4 Abs. 2 KRITIS DachG. Wir sehen die unbedingte Notwendigkeit, zumindest jene IT-Dienstleister der Krankenkassen mit starker, systemrelevanter Marktposition, wie bspw. BITMARCK, als Betreiber einer kritischen Infrastruktur zu erfassen. Diese Einordnung würde sicherstellen, dass es nicht zu erheblichen Versorgungslücken der Bevölkerung oder zu Gefährdungen der Sicherheit kommt.

II. WEITERGEHENDER ÄNDERUNGSBEDARF

- Die Erfüllung der Anforderungen an KRITIS-relevante IT-Dienstleistungen der Kassen sollte, soweit inhaltlich und fachlich sinnvoll, auf deren IT-Dienstleister verantwortlich übertragen werden dürfen, sofern diese ihrerseits selbst als Betreiber einer kritischen Infrastruktur erfasst sind.
- Vor dem Hintergrund regelmäßiger Sicherheitsaudits für KRITIS-Betreiber gilt es zugleich eine inadäquate Mehrfachbelastung von solchen KRITIS-betreibenden IT-Dienstleistern zu vermeiden, die im Regelfall von mehreren Krankenkassen beauftragt werden. Hier sollte die einfache Nachweiserbringung genügen.