Stellungnahme des KH-IT Bundesverbandes zum geplanten „Sofortprogramm Cybersicherheit im Gesundheitswesen"

Der KH-IT Bundesverband begrüßt das vom Bundesministerium für Gesundheit geplante Sofortprogramm Cybersicherheit ausdrücklich. Aus Sicht der Krankenhaus-IT-Verantwortlichen handelt es sich um eine absolut notwendige und längst überfällige Maßnahme. Sie kommt nicht zu früh – im Gegenteil: Die Bedrohungslage für Kliniken hat sich in den vergangenen Jahren dramatisch verschärft. Ransomware-Angriffe, hybride Bedrohungen und gezielte Attacken auf versorgungskritische Infrastruktur sind keine Ausnahmefälle mehr, sondern Alltag. Wenn IT-Systeme in Krankenhäusern ausfallen, steht unmittelbar die Patientenversorgung auf dem Spiel.

Mit dem KRITIS-Dachgesetz und der Umsetzung der NIS-2-Richtlinie kommen auf die Einrichtungen des Gesundheitswesens erhebliche und verpflichtende Anforderungen an das Informationssicherheitsmanagement zu. Diese Pflichten sind fachlich richtig und notwendig – aber sie sind ohne substanzielle finanzielle Unterstützung von den Häusern nicht zu stemmen. Genau hier setzt das Sofortprogramm an, und genau deshalb ist es unverzichtbar.

Entscheidend ist aus unserer Sicht der Zusammenhang mit der Vergangenheit: Die neuen Sicherheitsanforderungen treffen auf einen Sektor, der über Jahre strukturell unterfinanziert war. Die Mittel des Krankenhauszukunftsgesetzes (KHZG) haben zwar erste Impulse gesetzt, den tatsächlichen Bedarf an Cybersicherheit jedoch nicht flächendeckend abgedeckt – insbesondere nicht die laufenden Betriebs-, Personal- und Wartungskosten, die moderne IT-Sicherheit dauerhaft, auch über den Förderzeitraum des KHZG hinaus, verursacht. Der über Jahre aufgelaufene Investitionsstau lässt sich nicht durch Vorgaben allein auflösen. Es braucht die Mittel, die das Sofortprogramm nun in Aussicht stellt.

Besonders begrüßt der KH-IT Bundesverband, dass das Ministerium den Dialog mit der Praxis sucht – mit den Fachleuten aus den Reihen der Leistungserbringer zu sprechen und nicht über sie, ist der richtige Ansatz. Und er entscheidet über den Erfolg des Programms: Fördermittel wirken nur, wenn Förderrichtlinie, Antragslogik und Nachweispflichten im realen Klinikbetrieb funktionieren. Genau an dieser Schnittstelle – zwischen förderpolitischer Zielsetzung und betrieblicher Umsetzbarkeit in den Häusern – ist der KH-IT Bundesverband verortet. Es sind unsere Mitglieder, die IT-Sicherheit in den Kliniken täglich verantworten, umsetzen und aufrechterhalten. Diese Perspektive frühzeitig einzubinden, verhindert, dass gut gemeinte Vorgaben in der Fläche an der Machbarkeit vorbeigehen – und erhöht die Wirksamkeit jedes eingesetzten Euros.

Der KH-IT Bundesverband bietet dem Ministerium und dem künftigen Projektträger diese Fachexpertise konkret an. In den folgenden Themenfeldern können wir besonders zum Erfolg beitragen:

- **Praxis-Review der Förderinstrumente**: fachliche Rückmeldung zu Förderrichtlinie, Antragsverfahren und Reifegradmodell aus Sicht der umsetzenden IT-Leitungen – idealerweise vor dem breiten Roll-out.

- **Review-Panel der Krankenhaus-IT**: ein strukturierter Kreis von IT-Verantwortlichen aus Häusern unterschiedlicher Größe und Trägerschaft als Resonanzraum für den geplanten „Cybersicherheitshub".

- **Erprobung der Antragslogik**: ein realitätsnaher Test der Antrags- und Nachweisprozesse an konkreten Häusern, bevor sie bundesweit verbindlich werden.

Transfer in die Fläche: Aufbereitung und Kommunikation des Programms in die Krankenhäuser hinein, damit die Mittel tatsächlich abgerufen werden.

Damit die Wirkung nicht verpufft, verbindet der KH-IT Bundesverband seine Zustimmung mit vier Erwartungen an die Ausgestaltung:

Unbürokratischer Zugang: Antrags- und Nachweisverfahren müssen praxistauglich und für IT-Abteilungen mit begrenzten Ressourcen tatsächlich leistbar sein.

Breite Einbeziehung: Nicht nur formal als KRITIS eingestufte Häuser sind gefährdet – auch kleinere und mittlere Einrichtungen leisten einen unverzichtbaren Beitrag zur Gesundheitsversorgung und brauchen daher ebenfalls Zugang zur Förderung.

Verstetigung statt Strohfeuer: Cybersicherheit ist eine Daueraufgabe. Einmalige Investitionszuschüsse reichen nicht; es braucht eine planbare, mehrjährige Perspektive über 2029 hinaus, die auch Betriebskosten trägt.

Fachliche Anschlussfähigkeit: Reifegradmessungen und Nachweispflichten sollten auf etablierten Standards aufsetzen und den realen Klinikbetrieb abbilden.

Der KH-IT Bundesverband steht bereit, diese Angebote unmittelbar in die weitere Ausgestaltung des Sofortprogramms einzubringen, und lädt das Bundesministerium für Gesundheit zu einem direkten fachlichen Austausch ein.

Bundesverband der Krankenhaus IT-Leiterinnen/Leiter KH-IT e.V.

Der KH-IT bietet als Berufsverband den Führungskräften aus der Krankenhaus-IT eine Plattform zum Austausch von Erfahrungen und Wissen, sowie zahlreiche Möglichkeiten zur Fort- und Weiterbildung.

Die Mitglieder des Verbandes begleiten und gestalten in verschiedenen Gremien die Entwicklung der Rahmenbedingungen für die Digitalisierung im Gesundheitswesen. Der Verband unterstützt seine Mitglieder in der Entwicklung vom Techniker zum Wegbereiter der digitalen Transformation und IT-Strategen.

Kontakt:
Geschäftsstelle des Bundesverband KH-IT e.V.
z.Hd. Michael Kalmbacher

Plauener Str. 21
44139 Dortmund

Tel.: +49-15679-000063

geschaeftsstelle@kh-it.de
www.kh-it.de
Vereinsregister: VR 8125
Amtsgericht Dortmund

Pressereferent: Jürgen Flemming

Tel.: +49-170-926 9836
flemming@kh-it.de