



Digitalisierung pushen, Gesundheitsversorgung verbessern und Cybersicherheit stärken

Die Finanzsituation im deutschen Sozialwesen – insbesondere im Gesundheits- und Pflegebereich – ist stark angespannt: Nachhaltig wirkende Strukturreformen sind aus Sicht von BITMARCK unerlässlich, um diese Bereiche auf zukunftsste FüÙe zu stellen. Die Digitalisierung stellt in diesem Kontext eine eminent wichtige Möglichkeit dar, Prozesse zu optimieren, Synergien zu heben und letztlich auch die Versichertenversorgung zu verbessern.

Basis hierfür ist der konsequente Fokus auf **Cybersicherheit**. Vor dem Hintergrund „des Gesetzentwurfes der Bundesregierung für ein Gesetz zur Befugnisserweiterung und Entbürokratisierung in der Pflege“ sollte der Deutsche Bundestag analog zum Bereich der Datentransparenz den Bereich der Cybersicherheit als existenziell berücksichtigen. Daher unterbreiten wir den folgenden Vorschlag:

„0. § 4 Absatz 5 wird durch den folgenden Absatz 5 ersetzt: „(5) Im Jahr 2026 dürfen sich die sächlichen Verwaltungsausgaben einer Krankenkasse nicht um mehr als 8 Prozent gegenüber dem Jahr 2024 erhöhen. Die Begrenzung nach Satz 1 gilt nicht für Aufwendungen für Datentransparenz nach den §§ 303a bis 303e. Ferner gilt die Begrenzung nach Satz 1 nicht für Aufwendungen der IT-Sicherheit der gesetzlichen Krankenkassen nach § 392 SGB V und für Cloud-Anwendungen im Gesundheitswesen nach § 393 SGB V im Kontext der Cybersicherheit.“

Zur Begründung:

- Die **Bedrohungslage im Cyberraum** hat sich in den vergangenen Jahren erheblich verschärft. Staatlich gesteuerte und hybride Angriffe – also die Kombination aus Cyberangriffen, Desinformationskampagnen und wirtschaftlicher

Einflussnahme – nehmen zu. Gerade der Gesundheitssektor gilt als ein äußerst stark gefährdetes Ziel, da hier besonders sensible und schützenswerte Daten verarbeitet werden. Die Angriffe zielen zunehmend auf den Diebstahl von Gesundheitsdaten, Spionage, Sabotage und die Lahmlegung kritischer Infrastrukturen.

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stuft die Bedrohungslage konstant als „besorgniserregend“ an. Die Zahl der gemeldeten Sicherheitsvorfälle und Ransomware-Angriffe auf medizinische Einrichtungen, Rechenzentren und IT-Dienstleister ist in den letzten Jahren deutlich gestiegen. Diese Angriffe werden häufig von professionellen, teils staatlich unterstützten Gruppen aus dem Ausland durchgeführt, die gezielt auf Schwachstellen in vernetzten IT-Systemen und Cloud-Infrastrukturen abzielen.
- BITMARCK steht als zentraler IT-Dienstleister der gesetzlichen Krankenversicherung besonders im Fokus. Die Verantwortung umfasst kritische Plattformen wie die elektronische Patientenakte (ePA) und weitere Gesundheitsdienste, die für Millionen Versicherte betrieben werden.

Aufgrund dieser Rolle stellen Angriffe auf BITMARCK faktisch Angriffe auf die gesamte gesetzliche Krankenversicherungslandschaft dar. Ein erfolgreicher Angriff hätte nicht nur finanzielle Schäden, sondern auch gravierende Auswirkungen auf die Versorgungssicherheit und das Vertrauen der Bevölkerung in die digitale Gesundheitsinfrastruktur.

Die **Kosten für die IT-Sicherheit** steigen angesichts dieser Entwicklungen stetig – getrieben durch alternativlose Investitionen in präventive Schutzmaßnahmen, Systemhärtung, Forensik, Monitoring und Compliance mit regulatorischen Vorgaben (zum Beispiel NIS2, BSI-Gesetz, B3S GKV/PV). Gleichzeitig sind die Verwaltungsausgaben der Krankenkassen gesetzlich gedeckelt, wodurch dringend benötigte Investitionen in Sicherheit oft nicht in vollem Umfang realisierbar sind.

Eine Entkoppelung der IT-Kosten von den Verwaltungskosten ist daher zwingend erforderlich. Um sicherzustellen, dass IT-Systeme den aktuellen und zukünftigen

Anforderungen an Cybersicherheit und Gefahrenabwehr standhalten können. Unterbleiben diese Investitionen, führt dies unweigerlich zu einer wachsenden Verwundbarkeit gegenüber Cyberangriffen. Die möglichen Folgekosten – etwa durch Betriebsunterbrechungen, Datenverlust, Bußgelder oder Reputationsschäden – übersteigen die präventiven Investitionen bei weitem.

Cybersicherheit ist eine systemrelevante Voraussetzung für den sicheren Betrieb des Gesundheitswesens. Nur durch die Entkoppelung der IT-Kosten kann sichergestellt werden, dass die digitale Gesundheitsversorgung resilient, vertrauenswürdig und dauerhaft funktionsfähig bleibt.

Kontakt:
BITMARCK
Kruppstraße 64
45145 Essen
presse@bitmarck.de