Bibliografie	
Titel	Sozialgesetzbuch (SGB) Fünftes Buch (V) Gesetzliche Krankenversicherung
Amtliche Abkürzung	SGB V
Normtyp	Gesetz
Normgeber	Bund
Gliederungs-Nr.	860-5

§ 392 SGB V - IT-Sicherheit der gesetzlichen Krankenkassen

(1) Krankenkassen sind verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der jeweiligen Krankenkasse und die Sicherheit der verarbeiteten Versicherteninformationen maßgeblich sind.

(2) Organisatorische und technische Vorkehrungen nach Absatz 1 sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der Arbeitsprozesse der Krankenkasse oder der Sicherheit der verarbeiteten Versicherteninformationen steht.

(3) Die Krankenkassen erfüllen die Verpflichtungen nach Absatz 1 insbesondere, indem sie den branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Krankenkassen in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

(4) [1]Die Krankenkassen sind verpflichtet, repräsentiert durch ihre Verbände und den Spitzenverband Bund der Krankenkassen, in einem gemeinsamen bestehenden oder zu schaffenden Branchenarbeitskreis an der Entwicklung des branchenspezifischen Sicherheitsstandards für die informationstechnische Sicherheit der Krankenkassen im Sinne des Absatzes 3 mitzuwirken. [2]Die Krankenkassen, repräsentiert durch ihre Verbände und den Spitzenverband Bund der Krankenkassen, haben darauf hinzuwirken, dass der branchenspezifische Sicherheitsstandard auch Vorgaben enthält zu

1. geeigneten Maßnahmen zur Erhöhung der Cybersecurity-Awareness,

2. dem Einsatz von Systemen zur Angriffserkennung, die geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten, wobei diese dazu in der Lage sein sollten, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen (Maßnahmen zur Aufrechterhaltung der Betriebskontinuität) und

3. an IT-Dienstleister zu stellende Sicherheitsanforderungen gemäß Absatz 6, sofern diese Leistungen für die Krankenkassen zur Wahrnehmung ihrer gesetzlichen Aufgaben erbringen.

(5) Die Verpflichtung nach Absatz 1 gilt für alle Krankenkassen, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene organisatorische und technische Vorkehrungen zu treffen haben.

(6) Sofern eine Krankenkasse im Rahmen ihrer Aufgabenerfüllung IT-Dienstleistungen eines Dritten in Anspruch nimmt und eine Störung der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse des Dritten zu einer Beeinträchtigung der Funktionsfähigkeit der jeweiligen Krankenkasse oder der Sicherheit der verarbeiteten Versicherteninformationen führen kann, muss die Krankenkasse durch geeignete vertragliche Vereinbarungen sicherstellen, dass die Einhaltung des branchenspezifischen Sicherheitsstandards im Sinne des Absatzes 3 durch den Dritten gewährleistet wird.