

Informationssicherheit im Krankenhaus Neuerungen im B3S „Medizinische Versorgung“ sowie Anforderungen nach § 75c SGB V

verinice.XP 2022 – Digital!

Videokonferenz | Berlin, 23. Februar 2022 | Mario Beck | Referent IT, Datenaustausch und eHealth

Die Deutsche Krankenhausgesellschaft (DKG)

Dachverband der Krankenhausträger in Deutschland



- Arbeiterwohlfahrt Bundesverband e. V.
- Bundesverband Deutscher Privatkliniken e. V.
- Deutscher Caritasverband e. V.
- Deutscher Landkreistag
- Deutscher Paritätischer Wohlfahrtsverband Gesamtverband e. V.
- Deutscher Städte- und Gemeindebund
- Deutscher Städtetag
- Deutsches Rotes Kreuz e. V.
- Deutsche Rentenversicherung Bund
- Diakonie Deutschland
- Verband der Universitätsklinika Deutschlands e. V.
- Zentralwohlfahrtsstelle der Juden in Deutschland e. V.

Branchenspezifischer Sicherheitsstandard für Krankenhäuser (B3S) - Ein Blick zurück

Grundlage BSI-Gesetz

ca. März 2019

„§ 8a
Sicherheit in der
Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundes-

amt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt

1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.

(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln verlangen:

1. die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel.

2

„B3S“ – Auftragsinhalte

- Primär: „Entwicklungshelfer“ für Ausarbeitung von Positionen und Beiträgen zum B3S
- Ideen zur Gestaltung entwickeln
- Prüfung von Ideen des BAK und der DKG
- Lösungsideen für praktikable, nachweislich umsetzbare Sicherheitsanforderungen
- Abgleich der besonderen Rahmenbedingungen der KH mit dem Wissen aus anderen Branchen
- Hinweise zu besonderen Risiken und Fallen im Rahmen des Aufstellen eines Sicherheitsstandards

Rolle und Entwicklung des B3S hin zum Standard für Informationssicherheit im Krankenhaus



EN PRESSE · KONTAKT · LOGIN  

 **DKG**  Themen  Service **FA+R**

DEUTSCHE KRANKENHAUS GESELLSCHAFT 

DIGITALISIERUNG & DATEN

Digitalisierung und IT-Strategie »
Informationstechnik im Krankenhaus »
Elektronische Datenübermittlung »
Informationssicherheit und technischer Datenschutz »
Informationssicherheit im Krankenhaus »
Technischer Datenschutz »
Telematik-Infrastruktur »
Datenschutz und ärztliche Schweigepflicht »

INFORMATIONSSICHERHEIT UND TECHNISCHER DATENSCHUTZ

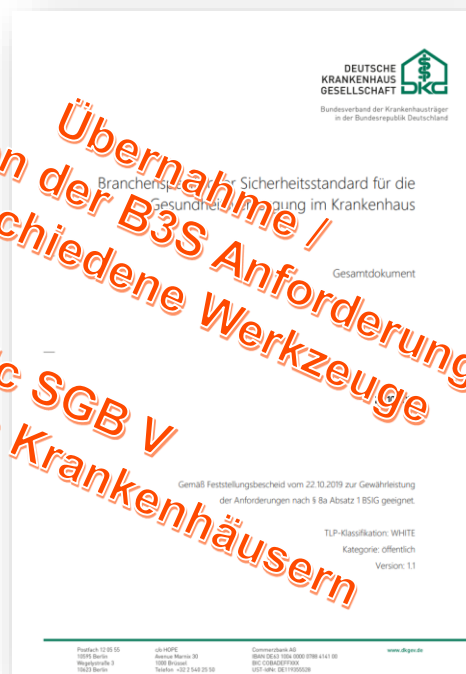
Informationssicherheit im Krankenhaus Branchenspezifischer Sicherheitsstandard (B3S)


Mit dem IT-Sicherheitsgesetz will der Gesetzgeber wirksame Schutzmechanismen für die sogenannten kritischen Infrastrukturen in Deutschland festschreiben. Die Deutsche Krankenhausgesellschaft ist sich aktiv u. a. mit der Definition eines branchenspezifischen Sicherheitsstandards [B3S] für die Verbesserung der IT-Sicherheit in den deutschen Krankenhäusern ein. Die Sicherheit der informationstechnischen Systeme in den Krankenhäusern dient in letzter Konsequenz auch der Patientensicherheit.

Die Deutsche Krankenhausgesellschaft hat den im Dezember 2018 veröffentlichten Entwurf eines Branchenspezifischen Sicherheitsstandards [B3S] entsprechend den Hinweisen des Bundesamtes für Sicherheit in der Informationstechnik überarbeitet und nach Abstimmung und Freigabe durch den Branchenarbeitskreis „Medizinische Versorgung“ des UP KRITIS sowie der hierfür zuständigen Gremien der Deutschen Krankenhausgesellschaft dem BSI die Fassung (Version 1.0) zur abschließenden Prüfung der Eignung des B3S für die Umsetzung der Anforderungen nach § 8a BSIg zugeleitet. Aus der Prüfung ergaben sich minimale Anpassungen, die zu einer Fassung 1.1 führten. Diese wurde seitens des BSI am 22.10.2019 als geeignet im Sinne des BSI-Gesetzes festgestellt.

Nachfolgend wird die als geeignet im Sinne des BSI-Gesetzes festgestellte Fassung des B3S (Version 1.1) vom 22.10.2019 zur Verfügung gestellt.

**Übernahme /
Integration der B3S Anforderungen
in verschiedene Werkzeuge
§ 75c SGB V
IT-Sicherheit in Krankenhäusern**



DEUTSCHE KRANKENHAUS GESELLSCHAFT 
Bundesverband der Krankenhausträger
in der Bundesrepublik Deutschland

Branchenspezifischer Sicherheitsstandard für die Informationssicherheit im Krankenhaus

Gesamtdokument

Gemäß Feststellungsbescheid vom 22.10.2019 zur Gewährleistung
der Anforderungen nach § 8a Absatz 1 BSIg geeignet.

TLP-Klassifikation: WHITE
Kategorie: öffentlich
Version: 1.1

Postfach 3201 55
10270 Berlin
Weyersberg 3
10243 Berlin

DKG-DE
Bismarckstrasse 30
10825 Berlin
Telefon: +49 30 244 25 50

Commerzbank AG
BIC: COBADE33HAN
IBAN: DE44 2512 0510 0007 0001 0141 00
BIC: COBADE33HAN
IBAN: DE 44 2512 0510 0007 0001 0141 00

www.dkg.de

§ 75c SGB V IT-Sicherheit in Krankenhäusern

- (1) Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.
- (2) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.
- (3) Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

B3S-Überarbeitung - Präzisierung, Klarstellungen, Verbesserung der Lesbarkeit

Kapitel 1

- Präzisierung, Klarstellungen in der Einleitung
- Streichung der Darstellung zu:
 - UP KRITIS
 - IT-Sicherheitsgesetz allgemein
 - Entstehung des B3S

Kapitel 2

- Zielsetzung, Adressaten und Anwendungsbereich des B3S klarer herausgearbeitet
- Umsortierung einzelner Unterkapitel (u.a. „Festlegung spezifische Ziele und Anforderungen“)

B3S-Überarbeitung - Präzisierung, Klarstellungen, Verbesserung der Lesbarkeit

Kapitel 1

- Präzisierung, Klarstellungen in der Einleitung
- Streichung der Darstellung zu:
 - UP KRITIS
 - IT-Sicherheitsgesetz allgemein
 - Entstehung des B3S

Kapitel 2

- Zielsetzung, Adressaten und Anwendungsbereich des B3S klarer herausgearbeitet
- Umsortierung einzelner Unterkapitel (u.a. „Festlegung spezifische Ziele und Anforderungen“)

Kapitel 3 + 4

- Hinweise zum Geltungsbereich überarbeitet und zusammengefasst
- Verschiebung der Hinweise zur Leitlinie Informationssicherheit in die Anforderungen (Kap. 6)
- Geringfügige redaktionelle Überarbeitung

B3S-Überarbeitung - Erweiterung des Betrachtungsbereichs auf 4 Säulen der KDL

Kapitel 5

- Standard-Risikomanagement-Prozess hierher verschoben
- Erweiterung des Betrachtungsbereichs zur Kritikalität von ausschließlich IT-Systemen auf alle 4 Säulen:
 - **Informationstechnik,**
 - **Medizintechnik,**
 - **Kommunikationstechnik und**
 - **Versorgungstechnik**

B3S-Überarbeitung - Neue und geänderte Anforderungen

Kapitel 6

- Ergänzung neuer Anforderungen:
 - Leitlinie Informationssicherheit (vorher nicht formal als Anforderung definiert)
 - Trennung der Logging-Anforderungen für IT und Medizintechnik
 - Neues Kapitel zu branchenspezifischer Technik / MPG Anforderungen (6.13.20)
 - Datensicherung, Datenwiederherstellung und Archivierung
 - Intrusion Detection / Prevention (IDS, IPS am Perimeter) - SOLL (ab 2023 MUSS -> ITSG)
- Klarstellung / Ergänzung bestehender Anforderungen:
 - Betriebliches Kontinuitätsmanagement (BCM)
 - Priorisierung bei mehreren Sicherheitsvorfällen / Behandlungsmaßnahmen

B3S-Überarbeitung - Präzisierung, Klarstellungen, Verbesserung der Lesbarkeit

Kapitel 7

- Enthält die vormals in Kapitel 3 enthaltenen Umsetzungsempfehlungen (Schrittfolge)

Kapitel 8

- unverändert

Kapitel 9

- unverändert

B3S-Überarbeitung – Zusammenfassung

- Version 1.2 baut auf Version 1.1 auf, Überarbeitung eher moderat,
- Grundstruktur bleibt, Verbesserung der Lesbarkeit durch Straffung und Umsortierung einiger Kapitel
- Anforderungen von MUSS <-> SOLL < 10
- Neue Anforderungen (Backup, Fernzugriff, IPS / IDS) < 10
- Neue Nummerierung der Anforderung (!)
- Entwurf V1.2 aktuell in der fachlichen Vor-Prüfung des BSI → Ergebnis Mitte/Ende März erwartet
- Übernahme evtl. Änderungsbedarfe und Einreichung zur formalen Eignungsfeststellung → Gleichzeitig Veröffentlichung auf der DKG-Website

Umsetzungshinweise nach § 75c SGB V

Informationssicherheit in Krankenhäusern

Stand: 07.12.2021

Kategorie: öffentlich

Status: Freigegeben

Version: 0.98

Kürzel: GF-Info-75c

GF-Info zum Starter-Paket - Umsetzungshinweise nach § 75c SGB V

Kapitel der Umsetzungshinweise:

[...]

3. Verstehen, worum es geht
4. Gefährdungen: Wodurch ist die Informationssicherheit in Krankenhäusern bedroht?
5. Grundlegendes zum Starter-Paket und seiner Anwendung
6. Gesetzliche Grundlagen
7. Gap-Analyse
8. Notfall- und Business-Continuity-Management

Weiteres Vorgehen / Roadmap

- Weiterentwicklung „Starter Paket Plus“
 - Anforderungen Dienstleister u. Logistik
 - Scope u Prozesse
 - Asset Management
 - weitere Vorlagen, u. a. Risikomanagement

Paket unter:

<https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/>

Herzlichen Dank

Für weitere Informationen kontaktieren Sie bitte

Mario Beck

Deutsche Krankenhausgesellschaft e.V.
Dezernat III - IT, Datenaustausch und eHealth

Anschrift: Wegelystraße 3 | 10623 Berlin
Telefon: +49 (30) 39801-1320
Telefax: +49 (30) 39801-3310
E-Mail: m.beck@dkgev.de
Website: www.dkgev.de