3.2023 I TÜV Media I www.mt-medizintechnik.de I G 8770F I ISSN 0344-9416

mt|medizintechnik

Schwerpunktthema:

Künstliche Intelligenz

Entwicklung und Zertifizierung klinischer KI-Software

Was kann ChatGPT im Gesundheitswesen?

Künstliche Intelligenz auf dem Weg in die Pflege

Organ für: fbmt – Fachverband Biomedizinische Technik e.V. · BSM – Bundesverband der Sachverständigen für Medizinprodukte e.V.
VDI-Gesellschaft Technologies of Life Sciences

Best Practice für zwei Standards

DIN EN 80001-1:2023 und *B3S in der Umsetzung*

Autoren: K. Herwig, F. Korth u. D. Schehl

Einordnung der geänderten Vorgaben

Bestand bisher nur für KRITIS-Krankenhäuser eine Verpflichtung zur Implementierung von Maßnahmen zur Informationssicherheit nach dem Stand der Technik, betrifft dies seit der Novellierung des SGB V im Januar 2022 alle Krankenhäuser in Deutschland (**Bild 1**) [3; 4]. Der hier geforderte B3S besteht aus 222 Anforderungen, wovon ein bedeutender Anteil die vernetzten Medizingeräte betrifft. Angesichts zunehmender Digitalisierung und einhergehender Erhöhung der Risiken von vernetzten Geräten [5, S. 6, Abschnitt 1] empfiehlt der B3S, sich an einem Risikomanagement nach DIN EN 80001-1 zu orientieren [5, S. 42]. Demnach sollten beide Standards parallel angewendet werden. Jedoch unterscheiden sie sich in ihrer Herangehensweise und ihren Schwerpunkten.

Während der B3S primär Bedrohungen betrachtet, die von außen auf das System einwirken können, analysiert die DIN EN 80001-1 hauptsächlich, welche Bedrohungen von dem System selbst ausgehen können [5, S. 6; 2, S.19, Kapitel 6.1.2.1]. Entsprechend fordert der B3S ein System zur Angriffserkennung wie auch eine Methodik zur Einschätzung von Risiken [5, S. 71, Kapitel 6.13.5]. In dieser Methodik des B3S werden neben den Schwachstellen auch explizit Bedrohungen ermittelt und gelistet [5, S. 32, Kapitel 4.1 ff.]. In der DIN EN 80001-1 hingegen wird auf die Schwachstellen und Bedrohungen mit ihrer Eintrittswahrscheinlichkeit lediglich in einem einzigen Nebensatz verwiesen [2, S. 21, Kapitel 6.1.2.3]. Ein weiter Unterschied der Schwerpunkte dieser beiden Standards besteht in den definierten Schutzzielen, die in **Bild 2** gegenübergestellt sind. Die drei Schutzziele der DIN EN 80001-1 sind die Sicherheit, die Effektivität sowie die Daten- und Systemsicherheit mit Blick auf die Verfügbarkeit, Vertraulichkeit und Integrität der Daten [2]. Beim Vergleich mit dem B3S lässt sich feststellen, dass seine Informationssicherheitsschutzziele identisch mit jenen zur Daten- und Systemsicherheit der DIN EN 80001-1 sind. Der B3S fordert darüber hinaus aber noch die Betrachtung der Authentizität [5].

> >> Für eilige Leser
> Mit dem Jahreswechsel hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Eignung des B3S in der Version 1.2 festgestellt [1]. Fast zeitgleich wurde die deutsche Fassung der DIN EN 80001-1:2023 veröffentlicht [2]. Aus den geltenden rechtlichen Anforderungen (BSI-Gesetz § 8a, SGB V § 75c) resultiert hinsichtlich der Sicherheit in der Informationstechnik die Einhaltung des aktuellen Stands der Technik sowie die Empfehlung zur Umsetzung des Branchenspezifischen Sicherheitsstandards B3S [3; 4]. Dieser Artikel soll einen ersten Ansatz zur praktischen Umsetzung der beiden Standards aus Sicht der Medizintechnik liefern.

Zusätzlich stellt dieser auch den Bezug zur Patientensicherheit und Behandlungseffektivität her, welche als KRITIS-Schutzziele bezeichnet werden [5]. Voraussetzung zur Aufrechterhaltung der KRITIS-Schutzziele sind wiederum die Informationssicherheitsschutzziele (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) [5, S. 9, Kapitel 2.2.2]. Die KRITIS-Schutzziele ähneln also den Schutzzielen der DIN EN 80001-1 (Sicherheit und Effektivität), wobei diese in der Norm eigenständig betrachtet werden [2, S. 10].

Ein Beispiel

Der folgende Fall soll die Problematik der verschiedenen Anforderungen und ihrer vollumfänglichen Berücksichtigung verdeutlichen: Ein Anwender stolpert an einem Bettplatz auf einer Intensivstation über ein ungünstig verlegtes Ethernet-Kabel und trennt damit einen Vitalzeichenmonitor vom bestehenden Netzwerk. Hierdurch entstehen mindestens zwei technische Probleme: Es werden einerseits keine Daten mehr in das nachgelagerte Patientendatenmanagementsystem (PDMS) automatisch übertragen und dokumentiert, andererseits wird die Alarmweiterleitung zur zentralen Überwachung unterbrochen. Ergänzend ist hinzuzufügen, dass eventuell auch die Netzwerkdose und/oder die geräteseitige Schnittstelle einen Schaden genommen haben könnten.

Durch diese Unterbrechung der Datenübertragung kann das Schutzziel „Verfügbarkeit" beider Standards nicht (mehr) eingehalten werden. Weiterhin kann dies zu einer Patientengefährdung führen, da primäre Alarme am Bettplatz überhört werden können, auch wenn an der zentralen Überwachung eine

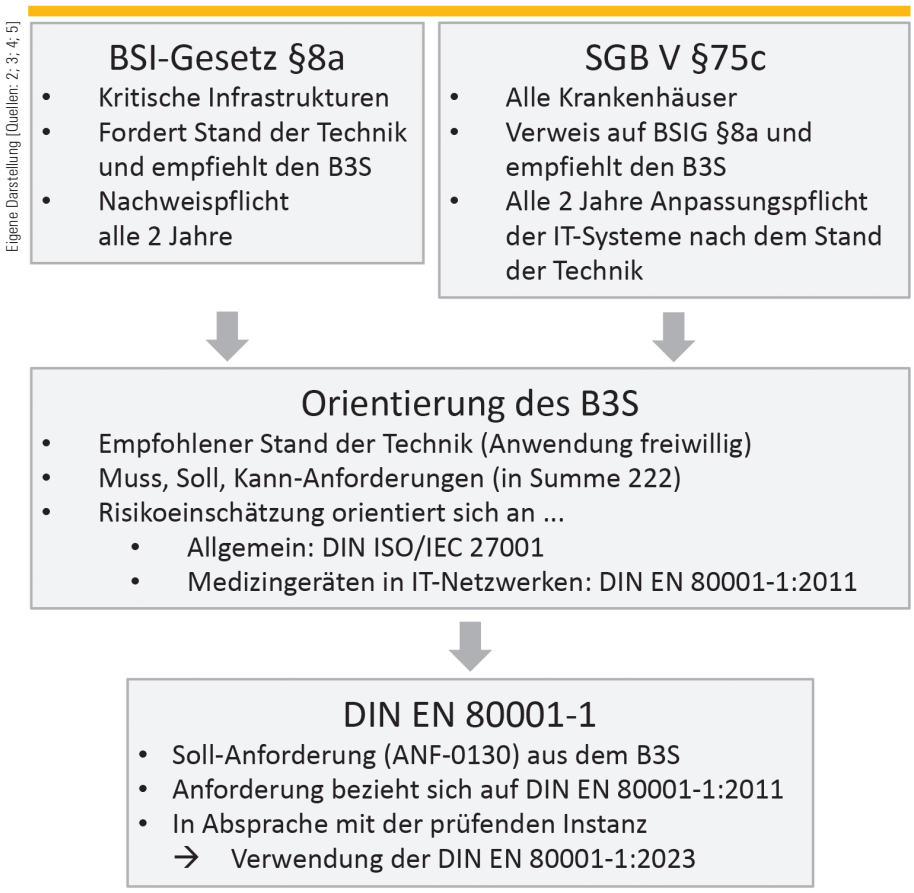

Bild 1: Änderung der Gesetze mit Empfehlung des B3S und dessen Ausrichtung auf die DIN EN 80001-1.

entsprechende Fehlermeldung entsteht (Bezug zu KRITIS-Schutzziel Patientensicherheit).

Darüber hinaus kann das Schutzziel der DIN EN 80001-1 in Bezug auf Sicherheit nicht mehr erreicht werden. Im genannten Beispiel könnte sich der Anwender durch das Stolpern eine Verletzung zuziehen, möglicherweise sogar eine Platzwunde bei einem Sturz auf den Boden.

Vor diesem Hintergrund stellt sich somit die Frage: Wie können die Anforderungen der Standards gleichermaßen praktisch umgesetzt werden?

Ein Vorschlag zur Vorgehensweise

In einem ersten Schritt empfiehlt es sich, eine sog. „Mapping-Tabelle" zu erstellen (**Tabelle 1**). Die Tabelle kann je nach Krankenhaus individuell abgestimmt werden. Um einen ersten Überblick zu bekommen, welche Anforderungen überhaupt gefordert sind, ist es ratsam, sich die Standards zu beschaffen und sich mit diesen vertraut zu machen. Auf der Internetseite der Deutschen Krankenhausgesellschaft (DKG) wird eine vorgefertigte „Mapping-Tabelle" [7] angeboten. Auch die DIN EN 80001-1:2023 stellt im Anhang A eine Zuordnungstabelle zur Verfügung, die ebenfalls genutzt werden kann [2, S. 30ff.].

Aus medizintechnischer Sicht ist es zunächst zu vernachlässigen, welcher Standard als Leitdokument verwendet wird. Um alle Anforderungen bedienen zu können, ist es empfehlenswert, einen Abgleich der Dokumente durchzuführen. So findet sich der Abschnitt 5.4.3 „Verständnis der Organisation und des soziotechnischen Ökosystems" der DIN EN 80001-1:2023 unter anderem in ähnlicher Form im B3S Kapitel 6.5 (ANF-0051) „Asset Management" wieder [2; 5]. In der vorherigen Version der DIN EN 80001 von 2011 war dies im Kapitel 4.3.2 „Beschreibung der Risikorelevanten Elemente" abgebildet [6].

Nachdem die Anforderungen identifiziert wurden, ist es hilfreich, diese zu kategorisieren, da die Anforderungen je nach Gesundheitseinrichtung unterschiedlich priorisiert werden können. Hierbei kann der B3S mit den „Muss, Soll und Kann"-Anforderungen unterstützen [5, S. 10, Kapitel 2.2.3]. Die Priorisierung kann durch eine farbliche Markierung erfolgen, beispielsweise in Rot, Orange und Gelb.

Aus der Erfahrung der praktischen Umsetzung empfiehlt sich die Ergänzung einer Spalte für Bemerkungen. Beispielsweise kann zu Kapitel 5.4.3 der DIN EN 80001-1 angemerkt werden (**Tabelle 1, Spalte 1** und **Spalte 5**), ob es vorhandene Richtlinien oder Prozesse in der Gesundheitseinrichtung gibt und/oder ob bereits eine Umsetzung des jeweiligen Aspekts bekannt ist.

Wurden entsprechende Fragen geklärt, können konkrete Aufgaben aus den Bemerkungen abgeleitet werden (**Tabelle 1, Spalte 6**). Eine sinnvolle Aufgabe ist in diesem Zusammenhang die Dokumentation der Eigenschaft des Medizinproduktes im Medizinproduktebuch. Ein mögliches Merkmal kann die Gesundheitsdatenspeicherung sein.

Eine Zuordnung, welcher jeweilige Fachbereich für die Umsetzung eines Prozesses zuständig ist, kann in den nachfolgenden Spalten hinterlegt werden (**Tabelle 1, Spalte 7 bis 10**). In Abhängigkeit von der Gesundheitseinrichtung kann dies unter anderem die Medizintechnik, die Betriebstechnik, ein Arbeitskreis zum Thema DIN EN 80001-1, die IT-Abteilung oder der Informationssicherheitsbeauftrage (ISB) sein. Im Kontext der Medizinprodukte wird die Zuständigkeit dem Bereich Medizintechnik zugeordnet (wie im beispielhaften Auszug der **Tabelle 1**).

Um fortlaufend einen Überblick über die Fortschritte zu den einzelnen Anforderungen zu bewahren, ist es nützlich, einen Umsetzungsstatus einzufügen (**Tabelle 1, Spalte 11**). Der Status kann individuell gewählt werden. Eine mögliche Statusdarstellung kann wie folgt aussehen: <25% (Rot), <50% (Orange), >50% (Gelb), >75% (Weiß).

Im Zuge der weiteren praktischen Umsetzung ist es zunächst sinnvoll, eine Liste mit

Medizingeräten (Vermögenswerten) zu erstellen, um eine Clusterung nach Gerätearten bzw. -gruppen vorzunehmen. Hierbei können Vorgaben und Vorschläge von Informationsportalen, wie z. B. von emtec weiterhelfen.

Für die folgende Risikobetrachtung bieten sich im ersten Schritt Medizingeräte an, welche essentiell für die Aufrechterhaltung der kritischen Dienstleistung sind. Dabei ist eine Orientierung an der Klassifizierung des B3S hilfreich [5, S. 51]. Konkret aus Sicht der DIN EN 80001-1 können zunächst Medizingeräte zur Lebenserhaltung (z. B. Beatmungs- und Narkosegeräte, Infusionstechnik oder Systeme zur Vitalzeichenüberwachung) betrachtet werden, da hierbei von einer hohen Kritikalität ausgegangen werden kann.

Nach der Klassifizierung der Medizingeräte ist eine Risikoanalyse der einzelnen Geräte bzw.- gruppen vorzunehmen. Die überarbeitete VDI 5707 „Wiederholungsprüfungen an aktiven Medizinprodukten im medizinischen Einsatz – Prüfgrundlagen", veröffentlicht im Februar 2023, bietet im Anhang B ein Schema zur exemplarischen Risikobewertung als Grundlage an [8].

Eigene Darstellung [Quellen: 2, S. 10 & S. 45; 5, S. 9]

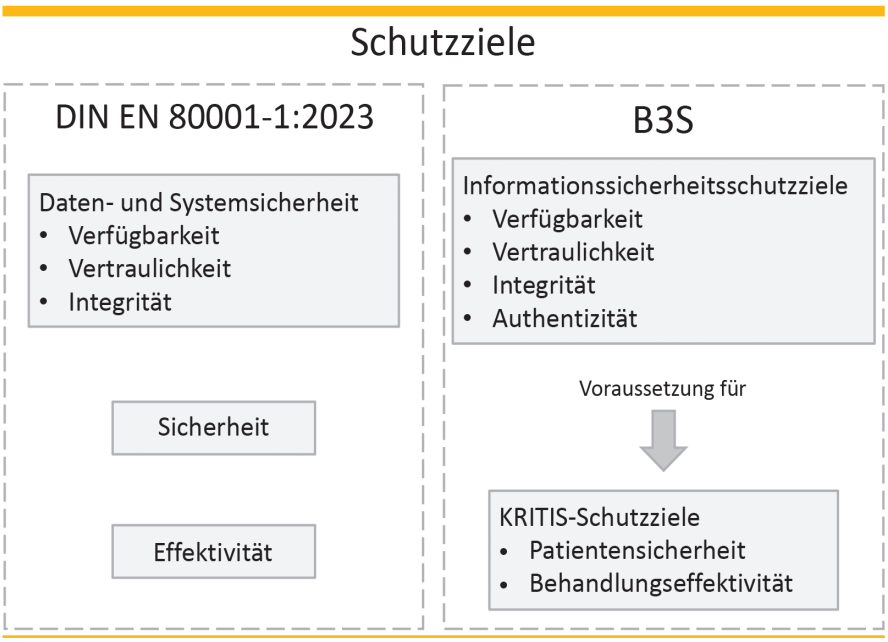

Bild 2: Gegenüberstellung der Schutzziele der DIN EN 80001-1 und des B3S.

Tabelle 1: Individualisierte „Mapping-Tabelle". Eigene Darstellung [Quellen: 2; 5; 6]

Abschnitt DIN EN 80001-1:2023	Anforderungen nach DIN EN 80001-1 oder B3S	Abgleich mit den ANF des B3S	Abgleich mit 80001:2011	Bemerkung	Aufgaben	MT	BT	80001	ISB / IT	Status
5.4.3 Verständnis der Organisation und des soziotechnischen Ökosystems	• Welche Anforderungen stellt die DIN EN 80001-1? • Welche Anforderungen stellt der B3S?	Beispiel: Kapitel 6.5 (ANF-0051)	Beispiel: Kapitel 4.3.2	• Gibt es vorhandene Richtlinien oder Prozesse? • Wird die Anforderung bereits nachgehalten?	Beispiel: • Im Medizinproduktebuch jedem Medizinprodukt, welches Gesundheitsdaten speichern kann, ein Merkmal geben.	x				> 50 % umgesetzt

Fazit

Die beiden aktuellen Standards setzen unterschiedliche Schwerpunkte, sodass eine gemeinsame Betrachtung beider Dokumente notwendig ist. Mit einer „Mapping-Tabelle" kann hierfür eine gute, auf die Gesundheitseinrichtung angepasste Ausgangsbasis geschaffen werden. Fortlaufend können die priorisierten Anforderungen an die zugeordneten Fachbereiche verteilt werden, um Schritt für Schritt eine Umsetzung der Standards durchzuführen.

Da der Zusammenhang zwischen der DIN EN 80001-1 und dem B3S komplex ist, erfordert eine Erarbeitung und Umsetzung der Thematik in der Gesundheitseinrichtung den Einsatz entsprechender Ressourcen. Die dargestellte Vorgehensweise mag als erster Vorschlag zur praktischen Umsetzung der beiden Standards aus medizintechnischer Sicht dienen.

Literatur

[1] Deutsche Krankenhausgesellschaft e.V. (12.01.2023), Rundschreiben Nr. 25/2023

[2] DIN EN IEC 80001-1 (VDE 0756-1):2023-02 (02.2023), Kommentar zur Norm: Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten – Teil 1: Sicherheit, Effektivität, Daten- und Systemsicherheit bei Implementierung und Gebrauch von eingebundenen Medizinprodukten oder eingebundener Gesundheitssoftware, (Herausgeber: VDE Verlag GmbH, Berlin & Beuth Verlag GmbH, Berlin)

[3] Bundesministerium der Justiz (20.08.2009). BSI-Gesetz § 8a, Kommentar zum Gesetz: Sicherheit in der Informationstechnik Kritischer Infrastrukturen

[4] Bundesministerium der Justiz (20.12.1988). SGB V § 75c, Kommentar zur Webseite: Sozialgesetzbuch (Fünftes Buch) § 75c IT-Sicherheit in Krankenhäusern

[5] Deutsche Krankenhausgesellschaft e.V. (08.12.2022), Branchenspezifischer Sicherheitsstandard „Medizinische Versorgung" Version 1.2

[6] DIN EN IEC 80001-1:2011 (11. 2011). DIN EN 80001-1:2011, Kommentar zur Norm: Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten – Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten (IEC 80001-1:2010). (Herausgeber: VDE Verlag GmbH, Berlin & Beuth Verlag GmbH, Berlin)

[7] Deutsche Krankenhausgesellschaft e.V. (o. D.)

[8] VDI 5707 (02.2023), Kommentar zur Richtlinie: Wiederholungsprüfungen an aktiven Medizinprodukten im medizinischen Einsatz – Prüfgrundlagen (Herausgeber: Beuth Verlag GmbH, Berlin)

Dokumentation: K. Herwig, F. Korth u. D. Schehl. DIN EN 80001-1:2023 und B3S in der Umsetzung. mt | medizintechnik 143 (2023), Nr. 3, S. 9, 2 Bilder, 1 Tabelle, 8 Lit.-Ang.

Schlagwörter: Informationssicherheit, Risikomanagement, DIN EN 80001-1:2023, Branchenspezifischer Sicherheitsstandard (B3S)

Autoren

Kai Herwig, B. Sc.

Fachbereich: Medizinische Informationstechnik, Themengebiete: Risikomanagement nach DIN EN 80001-1, Ausweitung des Informationssicherheitsmanagementsystems

Uniklinik Köln
medfacilities Betrieb GmbH
Gleueler Straße 66, 50931 Köln
E-Mail: kai.herwig@medfacilities.de
Web: www.medfacilities.de

Felix Korth, M. Sc.

medfacilities Betrieb GmbH, Stv. Abteilungsleiter Medizintechnik, Fachbereich: Projektleitung Medizintechnik, Themengebiete: Projektmanagement und Großgeräte
E-Mail: felix.korth@medfacilities.de

Denis Schehl, M. Sc.

medfacilities Betrieb GmbH, Fachbereich: Medizintechnische Fachplanung/Risikomanagement, Themengebiete: Fachplanung, Investitionsmanagement, Gerätekombinationen
E-Mail: denis.schehl@medfacilities.de

Anzeige

Medizintechnik und Informationstechnologie digital

MIT – Konzepte, Technologien, Anforderungen

- Überblick über Technik, Organisation, rechtliche Grundlagen
- Konkrete Lösungen für den Betrieb von medizinischen Anlagen und IT-Systemen im Krankenhaus
- Immer auf dem Stand der Technik und der Vorschriften

Jörg Schönfeld
Medizintechnik und Informationstechnologie digital
MIT – Konzepte, Technologien, Anforderungen
Browserbasiertes Onlineprodukt
Jahreslizenz: 333,64 EUR (netto)/ 357,- EUR (brutto)

Testen Sie jetzt 4 Wochen lang kostenlos:
www.tuev-media.de/mit-digital

TÜV Media GmbH · Tel. +49 221 806 3521
www.tuev-media.de

TÜVRheinland®
Genau. Richtig.