Recht der IT-Sicherheit in Arztpraxis und Krankenhaus

24. Frühjahrstagung der Arbeitsgemeinschaft Medizinrecht des Deutschen Anwaltvereins e.V.

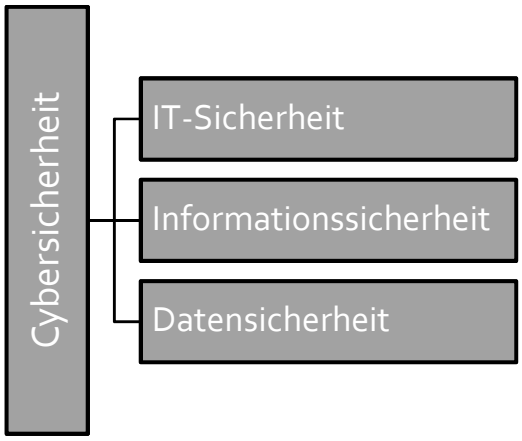
am 20.04.2024 in Erfurt

Dr. Carsten Dochow

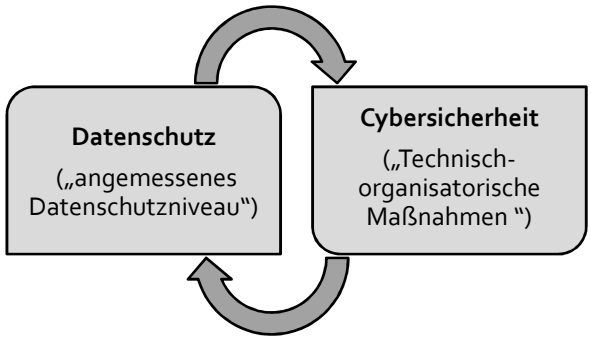
Leiter Personal, Organisation, Datenschutz in der Bundesärztekammer, Berlin Zertifizierter Datenschutzbeauftragter (TÜV)

im Vortrag persönliche Auffassung des Referenten

Einführung // Begriffe



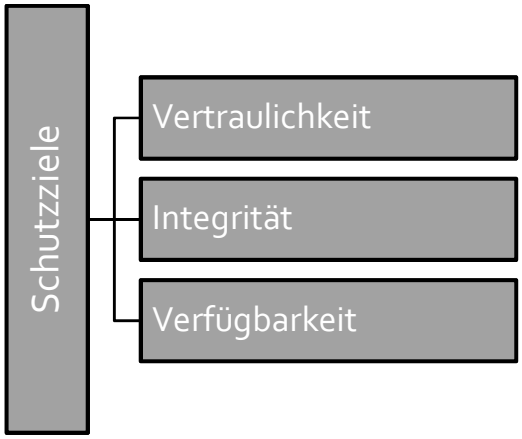
Einführung
//
Cybersicherheit
und Datenschutz



Einführung
//
Bedeutung von
Cybersicherheit

Ziel von „TOMs" → Gewährleistung von **Schutzzielen**

Einführung
//
Bedeutung von Cybersicherheit



Gesundheitswesen

Einführung // Angriffsziel Gesundheitswesen

Lage

- Die **Zahl von Cyberangriffen** auf Krankenhäuser und andere medizinische Einrichtungen **steigt** (BSI 2024)
- **rapide wachsendes Bedrohungspotenzial** durch zunehmend zielgerichtete, technologisch ausgereiftere und komplexere Angriffe

Ursachen

- wachsender Grad der **Digitalisierung** und Vernetzung
- → wachsende Angriffsflächen
- → Abhängigkeit von IT-Systemen
- Angreifbarkeit/ „Erpressbarkeit" steigt
- lukrative „Geschäftsmodelle" für Cyberkriminelle
- erhöhte Cybergefahren schon während Corona-Pandemie
- neue Cybergefahren aufgrund des Ukraine-Krieges

Einführung // Bedeutung von Cybersicherheit

Bedeutung

- **Cybersicherheit** = zielt nicht nur auf den Schutz von personenbezogenen Daten
- Funktionsfähigkeit von IT-Systemen der Einrichtungen
- Sicherheit und Vertrauenswürdigkeit bei allen Informationsverarbeitungsprozessen
- zunehmend an Bedeutung aufgrund der großen **Abhängigkeit** von verlässlichen Informations- und Kommunikationsstrukturen im Gesundheitsbereich

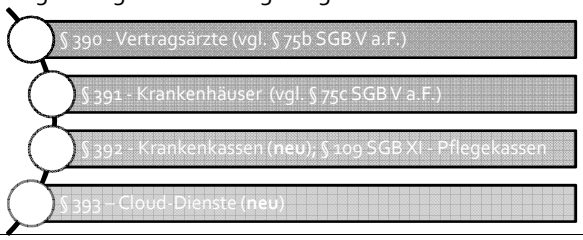
Mögliche Folgen

- Gefährdung der Patientenversorgung
- Gefährdung der Vertraulichkeit von Patientengeheimnissen
- Risiken für die wirtschaftliche Situation der Einrichtungen

Einführung
//
Gesetzgebung

Reaktionen des Gesetzgebers im SGB V

- seit 2019 mit dem DVG und PDSG
- zuletzt durch Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz - **DigiG**) v. 22.03.2024 (BGBl. 2024 I Nr. 101, 101a):
- **12. Kapitel**: „Interoperabilität und **Cybersicherheit im Gesundheitswesen**; Nationales Gesundheitsportal"
- Bündelung verschiedener Vorschriften zur Cybersicherheit (IT-Sicherheit) im SGB V und Ergänzung durch Neuregelungen



Arztpraxen

Arztpraxen
//
Lage der Cybersicherheit

Bedrohungslage im ambulanten Sektor

- IT-Sicherheitslage für Arztpraxen in Deutschland bisher kaum erfasst

> Arztpraxen von Datenleaks betroffen (BSI 2020)

- Keine KRITIS-Einrichtungen → **keine Meldepflichten** nach BSIG → keine Auswertung anhand Lageberichte des BSI möglich
- Meldepflichten nur bei Datenschutzvorfällen (Art. 33 DSGVO) → Auswertung anhand TB der LfDI:

> Cyberangriffe = „Platz 2 der Top 7-Liste" der häufigsten Ursachen gemeldeter Datenpannen
> (TB LfDI BW, 2019, S. 20)

- s.a. **(Fach-)Presseberichte**
- auch Vorfälle oder **Sicherheitslücken bei Software** für Arztpraxen

Arztpraxen
//
Lage der Cybersicherheit

Ursachen u.a.

- Hackerangriffe
- Sicherheitslücken in Software/IT-Systemen infolge von Programmierfehlern
- unterbliebene Updates
- Fehlkonfigurationen
- Fehlverhalten, Unachtsamkeit und Bedienungsfehler des Personals

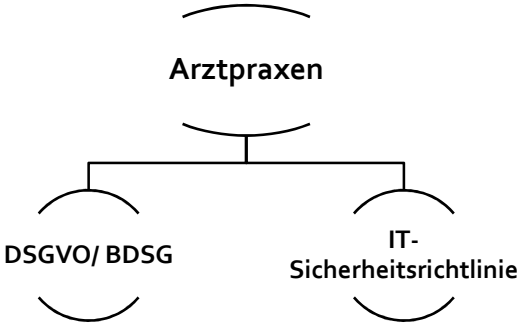
Fazit

- **unklares Bild der Bedrohungslage** im ambulanten Sektor
- viele **Einzelheiten** zu Vorfällen (v.a. bei Software-Anbietern) **blieben im Dunkeln**

Arztpraxen
//
Rechtliche Grundlagen

- DSGVO
- BDSG
- SGB V
- Untergesetzliche Vorschriften (Anl. BMV-Ä)
- ggf. weitere bereichsspezifische Regelungen
- Berufsrecht
- Strafrecht

Arztpraxen
//
Rechtliche Grundlagen



Arztpraxen
//
Rechtliche Grundlagen

Allgemeine Anforderungen // Datenschutzrecht

- **Art. 5 Abs. 1 lit. f DSGVO** (Grundsatz der „Integrität und Vertraulichkeit")
- **Art. 24 Abs. 1 DSGVO** (allgemeine Pflicht TOM umzusetzen + Nachweispflicht)
- **Art. 32 DSGVO** (Sicherheit der Verarbeitung)
- **Art. 25 Abs. 1 DSGVO** (Datenschutz durch Technikgestaltung auch bzgl. der Sicherheit der Datenverarbeitung)
- **Art. 33, 34 DSGVO** (Meldepflicht bei Datenpannen)
- **§ 22 Abs. 2 BDSG** (angemessene und spezifische Maßnahmen)

→ jeweils **Bezugspunkt**: Verarbeitung personenbezogener Daten

Arztpraxen
//
Anforderungen

Allgemeine Anforderungen // Datenschutzrecht

Art. 24 Abs. 1 DSGVO

*„Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der **Risiken** für die Rechte und Freiheiten natürlicher Personen geeignete **technische und organisatorische Maßnahmen** um, um sicherzustellen und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.*"

→ allgemeine Pflicht, dem jeweiligen Risiko angemessene und geeignete technisch-organisatorische Maßnahmen umzusetzen

Arztpraxen
//
Anforderungen

Allgemeine Anforderungen // Datenschutzrecht

Art. 32 Abs. 1 DSGVO

*„Unter **Berücksichtigung des Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um **ein dem Risiko angemessenes Schutzniveau** zu gewährleisten"*

→ Zumeist Verweis auf unbestimmten Rechtsbegriff „**Stand der Technik**" → Einfallstor für technische Standards (z.B. ISO/IEC 2700x)

Arztpraxen
//
Anforderungen

Allgemeine Anforderungen // Datenschutzrecht

Maßnahmen gem. Art. 32 Abs. 1 DSGVO u.a.

- **Pseudonymisierung und Verschlüsselung** personenbezogener Daten;
- Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme** und Dienste im Zusammenhang mit der Verarbeitung auf Dauer **sicherzustellen**;
- Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**;
- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Arztpraxen
//
Rechtliche Grundlagen

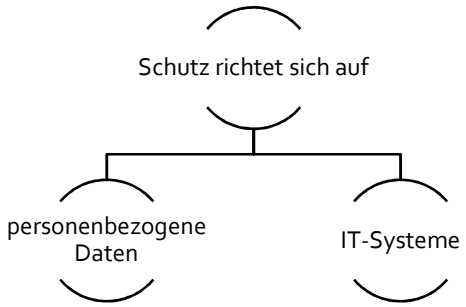
IT-Sicherheitsrichtlinie der K(Z)BV

- **§ 390 SGB V** – Richtlinien regeln Voraussetzungen für die IT-Sicherheit in Praxen
- **Aufgabe der K(Z)BV** die IT-Sicherheitsanforderungen in der vertrags(zahn)ärztlichen Versorgung in einer Richtlinie festzulegen
- eingeführt als § 75b SGB V a.F. mit dem DVG 2019
- Hintergrund: Arzt-und Zahnarztpraxen sind i.d.R. KMU, die keine kritischen Infrastrukturen i.S.d. BSIG sind und der BSI-KRITIS-Verordnung nicht unterfallen
- dennoch besteht ein großes Bedrohungspotenzial für die in Arztpraxen eingesetzten IT-Systeme

Arztpraxen
//
Rechtliche Grundlagen

IT-Sicherheitsrichtlinie der K(Z)BV

- erstmals vom 16.12.2020 und 2021 veröffentlicht
- Richtlinie ist alle zwei Jahre zu aktualisieren
- gilt unabhängig von Verarbeitung personenbezogener Daten



Arztpraxen
//
Rechtliche Grundlagen

IT-Sicherheitsrichtlinie der K(Z)BV

Adressaten

- die an der vertrags(zahn)ärztlichen Versorgung teilnehmenden Leistungserbringer
- **Ausnahme**: vertrags(zahn)ärztliche Versorgung im Krankenhaus, soweit dort bereits angemessene Vorkehrungen gem. § 391 SGB V getroffen werden

→ **verbindlich** für Vertrags/zahn)ärzte

- Privatärzte?
  - ggf. als **Teil des berufsrechtlichen Pflichtenprogramms** (§ 2 Abs. 5, § 9, § 10 Abs. 5 MBO–Ä i.V.m. Empfehlungen der Ärztekammern), und/oder
  - über das **Datenschutzrecht** (§ 22 Abs. 2 BDSG), soweit Datenverarbeitung erfolgt

Arztpraxen
//
Rechtliche Grundlagen

Privatärzte

BUNDESÄRZTEKAMMER
KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntmachungen

Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis[1]

3.11. Technische und organisatorische Maßnahmen

Die DSGVO verpflichtet den Praxisinhaber, technische und organisatorische Maßnahmen nach dem Stand der Technik zur Gewährleistung des Datenschutzes zu treffen.[161] Sie müssen unter Berücksichtigung der bezweckten Verarbeitung von Gesundheitsdaten und der möglichen Risiken für die Rechte von Patienten geeignet sein, den Datenschutz gemäß der DSGVO und eine hinreichende Informationssicherheit zu gewährleisten.[162]

Empfehlung: Auf Basis des Verzeichnisses der Verarbeitungstätigkeiten lässt sich eine Bewertung der Risiken vornehmen.

Zu berücksichtigende Schutzziele der Informations- und IT-Sicherheit werden in Art. 32 DSGVO benannt: Dazu zählt z. B. die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Eine Konkretisierung erfolgt durch die IT-Sicherheitsrichtline gem. § 75b SGB V[163], die auch für den privatärztlichen Bereich eine gute Orientierung bietet.

Arztpraxen
//
Rechtliche Grundlagen

IT-Sicherheitsrichtlinie der K(Z)BV

Mögliche Folgen bei Nichtbeachtung:

- **Disziplinarmaßnahmen** gem. Art. 81 Abs. 5 SGB V

...im Übrigen

- **Bußgelder** gem. Art. 83 DSGVO
- **Schadensersatz- und Unterlassungsansprüche** (Art. 82 DSGVO, §§ 280 ff. §§ 823 ff., 1004 BGB)
- Strafbarkeit gem. **§ 203 StGB**

Arztpraxen
//
Anforderungen

IT-Sicherheitsrichtlinie der K(Z)BV

Grundsystematik

Kleine Artpraxen
- < 5 mit Datenverarbeitung betraute Personen
- es gilt: Anlage 1 und 5

Mittlere Arztpraxen
- 6-20 mit Datenverarbeitung betraute Personen
- es gilt: Anlage 1, 2 und 5

Große Arztpraxen
- > 20 ständig mit Datenverarbeitung betraute Personen oder Datenverarbeitung über „normalem" Umfang (Groß-MVZ mit krankenhausähnlichen Strukturen, Labore)
- es gilt: Anlage 1, 2, 3 und 5

Arztpraxen
//
Anforderungen

IT-Sicherheitsrichtlinie der K(Z)BV

Grundsystematik


Anlage 1: Anforderungen für Praxen


Anlage 2: zusätzliche Anforderungen für mittlere Praxen


Anlage 3: zusätzliche Anforderungen für Großpraxen


Anlage 4: zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte


Anlage 5: Dezentrale Komponenten der Telematikinfrastruktur

Arztpraxen
//
Anforderungen

IT-Sicherheitsrichtlinie der K(Z)BV

Inhalte: Anforderungen für die IT-Sicherheit

- differenziert nach Kategorien: „**Software**" und „**Hardware**"
- für einzelne **Zielobjekte** (Apps, Internetanwednungen, Office-Produkte etc.)
- z.B.
  - konsequente **Verschlüsselung** der Kommunikation und Aufbewahrung
  - **Updates**
  - Datensicherungen/ **Backups**
  - **Virenscanner**
  - etc.

Arztpraxen
//
Anforderungen

IT-Sicherheitsrichtlinie der K(Z)BV

Umsetzung

- Seite der KBV mit zusätzlicher Spalte für „weitere Hinweise"

  https://hub.kbv.de/site/its
- **Praxis-Check** = Selbsttest für Niedergelassene und Praxisteams von der KBV

  https://praxischeck.kbv.de/mpc/courses/list.xhtml
- von 2018: **Technische Anlage** zu *KBV/BÄK*, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis

  http://daebl.de/MA27
- weitergehend: *BSI*, **Leitfaden zur Basis-Absicherung nach IT-Grundschutz**: In drei Schritten zur Informationssicherheit

  https://www.bsi.bund.de/

Arztpraxen
//
Anforderungen

IT-Sicherheitsrichtlinie der K(Z)BV

Inhalte/Anforderungen

- umfasst auch Anforderungen für medizinische Großgeräte wie z.B. Computertomograph oder Magnetresonanztomograph (Anlage 4)
- umfasst auch Anforderungen an die sichere **Installation und Wartung von Komponenten und Diensten der TI**, die in der vertragsärztlichen Versorgung genutzt werden (Anlage 5)
- NEU seit DigiG: soll jetzt auch Maßnahmen zur Erhöhung von **Awareness** („Sicherheitsbewusstsein") umfassen, z.B. Informationsmaterialien über Schulungen bis zu simulierten beziehungsweise demonstrativen „Angriffen".

Arztpraxen
//
Bewertung

BSG (zunächst) zufrieden

*Der Gesetzgeber sei „seiner **Beobachtungs- und Nachbesserungspflicht** nachgekommen, indem er etwa auf die in der Praxis zu Tage getretenen datenschutzrechtlichen Defizite und Sicherheitslücken […] reagiert und entsprechende Gegenmaßnahmen ergriffen hat. […] Soweit die Kl. auf Schwachstellen in den IT-Systemen einzelner Arztpraxen hinweist, hat der Gesetzgeber darauf mit der bereits durch das DVG eingefügten und mit dem PDSG nochmals nachgebesserten **Neuregelung des § 75b SGB V** reagiert. Danach ist die Kassenärztliche Bundesvereinigung verpflichtet, in einer für die Leistungserbringer verbindlichen **Richtlinie** die – mit dem BSI abzustimmenden – **Anforderungen zur Gewährleistung von IT-Sicherheit in der vertragsärztlichen Versorgung festzulegen** und jährlich anzupassen (vgl. die Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit vom 16.12.2020, abrufbar unter https://www.kbv.de/"* (BSG, Urt. v. 20.01.2021 - B 1 KR 7/20 R)

Arztpraxen
//
Bewertung

BSI eher unzufrieden

- jüngere **Studien des BSI** mit Umfrage unter 12.000 Arztpraxen (Rückmeldung von 1.600) im Jahr 2023
- **Ziel**: Umsetzungsgrad der IT-Sicherheitsrichtlinie zu identifizieren
  - nur 1/3 der Befragten setz vorgegebene Schutzmaßnahmen um
  - 10% waren mindestens einmal von einem IT-Sicherheitsvorfall betroffen
  - unzureichender Schutz vor Schadsoftware, mangelndes Patchmanagement und fehlende Back-ups festgestellt.
  - sensible Patientendaten werden nicht durch Festplattenverschlüsselung geschützt
  - Anschluss an die Telematikinfrastruktur (TI) mit Parallelschaltung statt mit von der gematik empfohlenen Reihenschaltung
- Fazit: **dringender Handlungsbedarf**

Arztpraxen
//
Bewertung

BSI Projekt CyberPraxMed

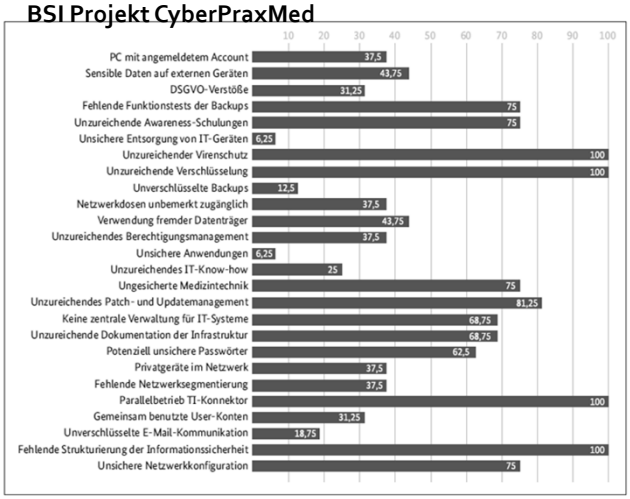


Abbildung 1 – Häufigkeit der Schwachstellen in Prozent

Quelle: BSI, Tätigkeitsbericht Gesundheit 2023, April 2024, S. 14 (beachte: sehr kleine Datenbasis mit 16 befragten Arztpraxen in dem Projekt CyberPraxMed!)

Arztpraxen
//
Bewertung

Kritik an der IT-Sicherheitsrichtlinie

- 55 Prozent der Befragten der o.g. BSI-Studie (2024) gaben an, dass die Angaben in der IT-Sicherheitsrichtlinie zu **wenig verständlich** seien
- **Bedarf nach konkreten Hilfestellungen** bei der Umsetzung der Anforderungen
- Es wird andererseits kritisiert, die Vorgaben seien gerade einmal auf **Heimanwender-Niveau**:

> *„Die Autoren stellen mit Erstaunen fest, dass die Hinweise dieser Richtlinie für kleine Praxen den BSI-Empfehlungen für Privatnutzer bzw. Heimanwender ähneln […] wie zB der Hinweis, den Browser zu aktualisieren. Die Maßnahmen sind so allgemeingültig und gleichzeitig alt […] Auch sind die Vorschläge technisch teils unausgegoren […]. Die Richtlinie bleibt insgesamt weit hinter dem Stand der Technik zurück, ist unstrukturiert und damit wertlos"* (*Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechtshandbuch, 2023)

Arztpraxen // Bewertung

Kritik an der IT-Sicherheitsrichtlinie

- Letztlich fasst die Richtlinie – zumindest, aber auch nicht mehr als – ein **Mindestmaß** an zu ergreifenden Maßnahmen für Arztpraxen (**Basisschutzkonzept**) zusammen
- **zu stark auf die IT-Sicherheit fokussiert** und deckt andere wichtige Aspekte der Cybersicherheit, wie eine physische, organisatorische und personelle Sicherheit, nicht genügend ab
- → Technische Anlage zu Hinweisen der KBV/BÄK zu Datenschutz und Schweigepflicht bereits seit 2008 umfassten teilweise diese Aspekte
- viele Maßnahmen dürften mit Blick auf Art. 32 DSGVO schon vorher Standard gewesen sein
- **Orientierung an Personenzahl** in Arztpraxen vernachlässigt risikobasierten Ansatz, weil bei automatisierter Verarbeitung durch wenige Personen gleichwohl hohe Risiken denkbar sind

Arztpraxen // Verbesserungen

Lösungsansätze

- **Verbesserung des Lagebildes**
  - Einführung einer Meldepflicht wie im KRITIS-Sektor → strukturierte Erfassung
  - Einführung von Transparenzregeln nach Vorfällen → „Ursachenforschung"
- **Verständlichkeit** erhöhen bei Erhöhung des Niveaus
- **Awareness** verbessern
  - siehe jetzt **neu** in § 390 SGB V
  - Umsetzung durch kostengünstige Angebote zugeschnitten auf die ambulante Versorgung (vgl. BSI-Studie 2023)
- **Cloud-Lösungen** (SaaS mit entsprechender Sicherheitsverantwortung für Dienstleister)

Krankenhäuser

Krankenhäuser // Lage der Cybersicherheit

- **BSI**: Die **Zahl von Cyberangriffen** auf Krankenhäuser und andere medizinische Einrichtungen **steigt** (BSI 2024)
- → Bedrohungslage nach Einschätzung so hoch wie noch nie
- s.a. **(Fach-)Presseberichte und Medienberichte** von zahlreichen Krankenhäusern, die Opfer von Cyberangriffen wurden, z.B.
  - Lukas-Krankenhaus Neuss (2016)
  - Universitätsklinikum Düsseldorf (2020)
  - Universitätsklinikum Frankfurt (2023)
  - Klinikverbund Soest (2024)
- **Bundesregierung** im April 2024: weist auf **zurückgehende Zahlen von Cyberangriffen** hin:

Krankenhäuser // Lage der Cybersicherheit

Bundesregierung teilt Meldestatistik mit:

- 2018 – 17 Vorfälle
- 2019 – 61 Vorfälle
- 2020 – 55 Vorfälle
- 2021 – 35 Vorfälle
- 2022 – 35 Vorfälle
- 2023 – 21 Vorfälle
- 2024 – 3 Vorfälle (bis 18. März 2024)

→ erfasst sind nur Meldungen der KRITIS-Krankenhäuser (§ 8b Abs. 4 BSIG) und nur „informationstechnische Angriffe" (BReg, BT-Drs. 20/10907)

Krankenhäuser // Rechtliche Grundlagen

- **DSGVO**
- BDSG
- LDSG
- KDG / DSG-EKD
- **BSIG + KRITIS-VO**
- **SGB V**
- Untergesetzliche Vorschriften (Anl. BMV-Ä)
- ggf. weitere bereichsspezifische Regelungen
- Berufsrecht
- Strafrecht

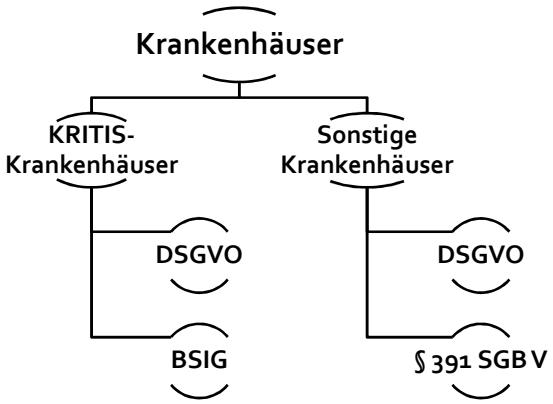
Krankenhäuser
//
Rechtliche Grundlagen

Allgemeine Anforderungen // Datenschutzrecht

- **Art. 5 Abs. 1 lit. f DSGVO** (Grundsatz der „Integrität und Vertraulichkeit")
- **Art. 24 Abs. 1 DSGVO** (allgemeine Pflicht TOM umzusetzen + Nachweispflicht)
- **Art. 32 DSGVO** (Sicherheit der Verarbeitung)
- **Art. 25 Abs. 1 DSGVO** (Datenschutz durch Technikgestaltung auch bzgl. der Sicherheit der Datenverarbeitung)
- **Art. 33, 34 DSGVO** (Meldepflicht bei Datenpannen)
- ggf. **§ 22 Abs. 2 BDSG** (angemessene und spezifische Maßnahmen) *oder* Regelungen in **LDSG**

→ jeweils **Bezugspunkt**: Verarbeitung personenbezogener Daten

Krankenhäuser
//
Rechtliche Grundlagen



Krankenhäuser // Rechtliche Grundlagen

Spezifische Anforderungen // BSIG

Adressaten

- **Betreiber Kritischer Infrastrukturen**

Kritische Infrastrukturen sind **Einrichtungen** oder Anlagen u.a. aus dem Sektor Gesundheit **mit hoher Bedeutung für das Funktionieren des Gemeinwesens**, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (vgl. § 2 Abs. 10 BSIG)

Krankenhäuser // Rechtliche Grundlagen

Spezifische Anforderungen // BSIG

Kritische Infrastrukturen

- § 2 Abs. 10 BSIG i.V.m. **§ 6 Abs. 1 Nr. 1 BSI-KritisV** (Sektor Gesundheit) i.V.m. Anhang 5, Teil 3

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Stationäre medizinische Versorgung**		
1.1	Krankenhaus	Vollstationäre Fallzahl/Jahr	30 000

- nur zugelassenes Krankenhaus gem. § 108 SGB V
- Bemessungskriterium/Schwellwert: **30.000 vollstationäre Behandlungsfälle/ pro Jahr**

→ v.a. **Großkrankenhäuser**

- nach Schätzungen 5-10% der Krankenhäuser

Krankenhäuser
//
Anforderungen

Spezifische Anforderungen // BSIG

Anforderungen: Pflichten gem. § 8a, § 8b BSIG

- § 8a Abs. 1 BSIG: „***angemessene organisatorische und technische Vorkehrungen*** *zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten oder Prozesse zu treffen*" (S. 1) → Verpflichtung zu angemessenen OTV (auch TOV; entspricht TOM)
- **Angemessenheit**, „*wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht*" (S. 3)
- Maßstab: es „**soll**" der **Stand der Technik** eingehalten werden (S. 2)
- **Stand der Technik**: ISO2700-Reihe, IT-Grundschutz, BSI-Richtlinien, B3S

Krankenhäuser
//
Anforderungen

Spezifische Anforderungen // BSIG

Anforderungen: Pflichten gem. § 8a, § 8b BSIG

- § 8a Abs. 2 BSIG: es genügen **branchenspezifische Sicherheitsstandards → „B3S Medizinische Versorgung"** v. 10.01.2023; abrufbar bei der DKG
- § 8a Abs. 1a BSIG: OTV umfasst auch **Einsatz von Systemen zur Angriffserkennung** als gesetzlich vorgeschriebene OTV

Krankenhäuser
//
Anforderungen

Spezifische Anforderungen // BSIG

Anforderungen: Pflichten gem. § 8a, § 8b BSIG

- § 8a Abs. 3 BSIG: **Nachweispflichten**
- § 8a Abs. 4BSIG: **Überprüfungsrecht des BSI** mit Betretungsrecht und umfassender Auskunftsanspruch
- § 8b Abs. 3 BSIG: **Registrierungspflicht** von KRITIS beim BSI + **Kontaktstelle benennen**
- § 8b Abs. 4 BSIG: **Meldepflichten bei Störungen**
  - Störungen, die zu Ausfall oder erheblichen Beeinträchtigung der KRITIS geführt haben
  - erhebliche Störungen, die zu Ausfall oder erheblichen Beeinträchtigung der KRITIS führen können

Krankenhäuser
//
Anforderungen

Spezifische Anforderungen // BSIG

Mögliche Folgen bei Nichtbeachtung

- **Bußgelder gem. § 14 BSIG**

...im Übrigen:

- **Bußgelder** gem. Art. 83 DSGVO
- **Schadensersatz- und Unterlassungsansprüche** (Art. 82 DSGVO, §§ 280 ff. §§ 823 ff., 1004 BGB)

Krankenhäuser
//
Rechtliche Grundlagen

Spezifische Anforderungen // SGB V

- **§ 391 SGB V - IT-Sicherheit in Krankenhäusern**
- eingeführt als § 75c SGB V a.F. mit dem PDSG 2020
- *„das Bedrohungspotenzial wächst durch zunehmend zielgerichtete, technologisch ausgereiftere und komplexere Angriffe. Solche Cyberangriffe richten sich nicht nur gegen große Krankenhäuser mit über 30 000 vollstationären Fällen pro Jahr. Auch in Krankenhäusern mit geringeren Fallzahlen besteht ein großes Bedrohungspotenzial für die dort eingesetzten informationstechnischen Systeme, welches es einzudämmen gilt.*" (BT-Drucks. 19/20708 , 167 zu § 75c SGB V aus Juli 2020)
- Anlehnung an § 8a Abs. 1 BSIG erkennbar
- Ziel: Mindestsicherheitsniveau für **alle Krankenhäuser**

Krankenhäuser
//
Rechtliche Grundlagen

Spezifische Anforderungen // SGB V

Adressaten

- gilt für alle Krankenhäuser
- **Ausnahme**: Krankenhäuser als Betreiber Kritischer Infrastrukturen, die gemäß § 8a des BSI-Gesetzes angemessene organisatorische und technische Vorkehrungen zu treffen haben.

Mögliche Folgen bei Nichtbeachtung

- im SGB V sind **keine Bußgelder** vorgesehen

im Übrigen aber:

- **Bußgelder** gem. Art. 83 DSGVO
- **Schadensersatz- und Unterlassungsansprüche** (Art. 82 DSGVO, §§ 280 ff. §§ 823 ff., 1004 BGB)

Krankenhäuser
//
Anforderungen

Spezifische Anforderungen // SGB V

§ 391 SGB V - IT-Sicherheit in Krankenhäusern

- *„Krankenhäuser 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 des jeweiligen Krankenhauses und den Schutzbedarf der verarbeiteten Patienteninformationen maßgeblich sind.*" (Abs. 1)
- **Angemessenheit**: *„wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder dem Schutzbedarf der verarbeiteten Patienteninformationen steht.*" (Abs. 3)

Krankenhäuser
//
Anforderungen

Spezifische Anforderungen // SGB V

§ 391 SGB V - IT-Sicherheit in Krankenhäusern

- **Stand der Technik** → unbestimmter Rechtsbegriff → Verweis auf technische Normen
- **Orientierungshilfe**: Erfüllung der Anforderungen durch Anwendung des „**branchenspezifischen Sicherheitsstandard** für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung" (Abs. 4; → sog. **B3S „Medizinische Versorgung"**, auch sog. „B3S Krankenhaus" Version 1.2. Stand: 08.12.2022)

- Keine Nachweispflichten
- Keine Meldepflichten!

Krankenhäuser
//
Anforderungen

Spezifische Anforderungen // SGB V

§ 391 SGB V - IT-Sicherheit in Krankenhäusern

- NEU seit DigiG: *„verpflichtende Maßnahmen zur Steigerung der **Security-Awareness** von Mitarbeiterinnen und Mitarbeitern."* (Abs. 2)

Cloud-Dienste

Cloud-Dienste // Neuregelung

- **§ 393 SGB V** - Regelung zum Einsatz von cloudbasierten Systemen im Gesundheitswesen
- **Ziel**: Erfüllung von **Mindestanforderungen** beim Einsatz von Cloud-Diensten
- Zulässig wenn Dienst im **Inland, EU** oder Staat mit **Angemessenheitsbeschluss** (gem. Art. 45 DSGVO) erfolgt + **Niederlassung im Inland** (Abs. 2)
- angemessene **TOM** nach **dem Stand der Technik** (Abs. 3, Nr. 1)
- aktuelles **C5-Testat** für Einsatz von **Cloud-Diensten** im Gesundheitswesen durch Leistungserbringer (Abs. 3, Nr. 2) → Basiskriterien für Cloud-Dienste oder vergleichbare Testate oder Zertifikate (Abs. 5 S. 2)
- Umsetzung der korrespondierenden Kriterien für Endkunden (**Endnutzerkontrollen**) aus dem Testat (Abs. 3, Nr. 3) → Mitwirkungspflicht des Leistungserbringer

Cloud-Dienste // Neuregelung

- aktuelles **C5-Testat**: *„das positive Prüfergebnis über einen sicheren Cloud-Computing-Dienst anhand des Kriterienkatalogs C5 (Cloud Computing Compliance Criteria Catalogue) des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils gültigen Fassung" (§ 384 Nr. 6 SGB V)*
- **C5-Testat: Cloud Computing Compliance Criteria Catalogue** → definiert die Mindestanforderungen für sicheres Cloud-Computing in Deutschland
- § 393 SGB V gilt **ab dem 1.7.2024,** um eine ausreichende Übergangsfrist zur Testat-Erlangung einzuräumen

Weiterführende Informationen

- *Dochow/Herpers/Raptis*, Kapitel 16. Gesundheit und Soziales, in: Kipker (Hrsg.), Cybersecurity, Rechtshandbuch, 2. Aufl. 2023
- *Dittrich*, Muss die vertragsärztliche Versorgung Kritische Infrastruktur werden? - ein Plädoyer für eine Anpassung von § 75b SGB V, GesR 2023, 360
- *Dittrich/ Dochow* Cybersicherheitsrecht in der Telematikinfrastruktur mit Blick auf Arztpraxen, GesR 2022, 414
- *Nadeborn/Dittrich* Cybersicherheit in Krankenhäusern – Teil 1: IT-Compliance als Leitungsaufgabe, ICLR 1/2022, 147 und Teil 2: vom Normalfall zum Notfall, ICLR 2/2022, 273
- *Dochow*, Cybersicherheitsrecht im Gesundheitswesen, MedR 2022, 100
- *Grzesiek*, Neue Anforderungen an die IT-Sicherheit in der Arztpraxis, GuP 2021, 171
- *Dittrich/Ippach* IT-Sicherheit betrifft nicht nur Großkrankenhäuser – die Regulierung der IT-Sicherheit im ambulanten und stationären Bereich, GesR 2021, 285
- *Dittrich/Dochow/Ippach* Auswirkungen der neuen EU-Cybersicherheitsstrategie auf das Gesundheitswesen – der Entwurf der NIS-2-Richtlinie und der „Resilienz"-Richtlinie, GesR 2021, 613
- *Dittrich*, Die Verankerung der IT-Sicherheit von Krankenhäusern im Sozialrecht – worin liegt der Nutzen des § 75 c SGB V?, GuP 2021, 165
- *Becker/Gärtner*, Der neue § 75c SGB V, KH 4/2021, 292

Weiterführende Informationen

Themen

- Krankenhäuser
- Medizinprodukte und Arzneimittel
- Telematikinfrastruktur
- Ambulante Gesundheitsversorgung
- Digitale Gesundheitsanwendungen
- Telemedizin.

Berücksichtigt

- NIS-2-Richtlinie und Entwurf eines Umsetzungsgesetzes
- Digitalgesetz für den Gesundheitsbereich (DigiG)
- CER-Richtlinie und Entwurf des KRITIS-Dachgesetzes.

Erscheint Juni 2024

ISBN 978-3-8114-8928-8

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:

https://www.dochows.de/