



Das Gesundheitswesen steht besonders jetzt – im Zeitalter der Digitalisierung – vor großen Herausforderungen. Zu den aktuellen Informationssicherheitsvorfällen zählen häufig:

- Angriffe von Hackern mit Verschlüsselungstrojanern, die zum Teil zu längeren Betriebsstillständen und hohen Schäden geführt haben.
- **Besonders dramatisch:** Auch Menschenleben waren zu beklagen, weil die Notfallvorkehrungen in einigen Fällen nicht wirksam waren.

Das zeigt:

Informationssicherheit ist nur wirksam als ganzheitlich eingesetztes Informations-Sicherheits-Management-System („ISMS“)

Ein ISMS besteht aus:

- Einer dedizierten Security-Organisation
- Richtlinien und Anweisungen
- Sicherheitsbewusstsein bei den EDV-Benutzern
- Security-Prozessen
- Unterstützenden technischen Einrichtungen
- Security Reporting
- Kontinuierlicher Verbesserungsprozess

Seit 2015 schreibt der Gesetzgeber mit dem **Informationssicherheitsgesetz für kritische Infrastrukturbetreiber und dem Gesundheitssektor** vor:

- „Angemessene“,
- Organisatorische und
- Technische Vorkehrungen zur Vermeidung von:
⇒ Störungen der VERFÜGBARKEIT, INTEGRITÄT, AUTHENTIZITÄT und VERTRAULICHKEIT ihrer informationstechnischen Systeme, Komponenten oder Prozesse sicherzustellen.

Daraus hat sich der **branchenspezifische Sicherheitsstandard für das Gesundheitswesen „B3S“** entwickelt, welcher die Implementierung eines an der ISO 27001 angelehnten ISMS zum Inhalt hat.

Was bedeutet das jetzt für Ihre IT-Abteilung, die die informationsverarbeitenden Systeme zur Erhebung, Speicherung und Verarbeitung der Informationen einrichtet und betreibt?

Zu beachten sind bei der Umsetzung:

- Die neuen Herausforderungen im Rahmen der Digitalisierungs-Initiative des BMG und
- die Auflagen des Krankenhauszukunftsgesetzes für die Digitalisierung von Krankenhäusern.

Was bedeutet Digitalisierung eigentlich?

Digitalisierung bedeutet im Kern nichts anderes, als bisher manuell und analog unterstützte Gesundheitsprozesse durch digitale Services und Informationstechnologie abzulösen. Dabei steigt die **Abhängigkeit der Gesundheitsleistungen von Informationstechnologie** und die Anforderungen an Informationssicherheit und Datenschutz signifikant. D.h., nur „reife“ IT-Abteilungen können **Informationssicherheit** gewährleisten. Dabei gibt es international anerkannte Best Practices und Normen. IT Services sollten sicher gemäß **ISO 27001/B3S** und prozessorientiert gemäß **ISO 20000-1** sowie qualitätsgesichert gemäß **ISO 9001** produziert werden.



Was benötigt Ihre IT-Abteilung für eine Digitalisierung im Security-Bereich?

- IT Security Officer und Betriebsverantwortlichen für die technische Security Technologie
- Leitlinien und Richtlinien
- Moderne und integrierte Service- und Security-Management-Systeme
- Genügend Personalressourcen
- Ausreichendes Wissen
- Technische Einrichtungen

Das sollten Sie wissen:

Mit dem **Krankenhaus-Zukunfts-Gesetz (KHZG)** will der Bund die Digitalisierung im Gesundheitswesen vorantreiben. Den Trägern werden mit dem Krankenhauszukunftsfonds (KHZF) Fördermittel in Höhe von über **3 Mrd. Euro** zur Verfügung gestellt.

Um der steigenden Abhängigkeit von digitalisierten Prozessen von informationsverarbeitenden Systemen und Informationssicherheit entgegenzuwirken, unterstützt der Bund Maßnahmen zur Verbesserung der Informationssicherheit mit entsprechenden Förderbeiträgen.

Wichtig für den Antrag: Berücksichtigt werden muss die Sicherheit des IT-Bereichs und ein Teil-Projekt für die Implementierung eines Information-Security-Management-Systems **gemäß der ISO 27001 / B3S**. Außerdem müssen ergänzende technische Sicherheitseinrichtungen in der IT-Abteilung beantragt werden.

**Förderanträge können an das Land gestellt werden.
Die Fristen sind von Bundesland zu Bundesland unterschiedlich. Handeln Sie jetzt!**

Das zeichnet die DSP Unternehmensberatung bei der Projekterfahrung im Gesundheitswesen aus:

- Professionalisierung des Service-Management-Systems gemäß ITIL, ISO 9001 u. ISO 20000-1 wie auch der Lieferung und Implementierung von integrierten Service-Management-Lösungen.
- Professionalisierung und Zertifizierung von IT-Security-Management-Systemen gemäß ISO 27001, dem **Branchenstandard B3S** als auch der Lieferung und Implementierung von integrierten Security-Management-Lösungen.
- Ausbildung und Zertifizierung von Sicherheitsfachpersonal, wie Information Security Officer und IT-Informationssicherheits-Beauftragenden.

Die DSP begleitet seit vielen Jahren Krankenhäuser und große Arztpraxen auf dem Weg der Digitalisierung, die:

- Nun wieder ruhig schlafen können, weil das Service-Management professionalisiert, ein Informations-Sicherheits-Management-System implementiert und unterstützende Systeme der Matrix42 implementiert wurden.
- Die durch ein ISO-Zertifikat nachweisen können, dass nachhaltige, sichere, verfügbare IT-Services für die Patienten und die Gesundheitsorganisation produziert werden.
- Jetzt im Rahmen der Digitalisierungs-Projekte gut aufgestellt und ein geschätzter In-House-Serviceprovider sind.

Wenn Ihr Krankenhaus oder Ärzteverbund von der Expertise der DSP und dem Krankenhauszukunftsfonds profitieren möchte, dann rufen Sie uns zeitnah unter der Telefonnummer 06172-679460 an oder senden Sie uns eine Mailanfrage an: info@dsp-consulting.expert

Unsere Consultants sind vom Bundesamt für Soziale Sicherung für die Beratung beim Antrag von Fördermitteln nach § 19 Absatz 1 Satz 1 Nummer 2 bis 6, 8 und 10 KHSFV und dem Krankenhausfinanzierungsgesetzes zertifiziert.

Weitere Informationen und unsere Leistungen finden Sie unter: www.dsp-consulting.expert

Ihre DSP Unternehmensberatung

*Besuchen Sie auch die [DSP IT Service GmbH](http://www.dsp-consulting.expert) (Teil der DSP-Gruppe).

DSP Unternehmensberatung GmbH

Weinbergsweg 68a
61348 Bad Homburg

Tel.: (06172) 679 460
Fax: (06172) 679 469

E-Mail: info@dsp-consulting.expert
<https://www.dsp-consulting.expert>