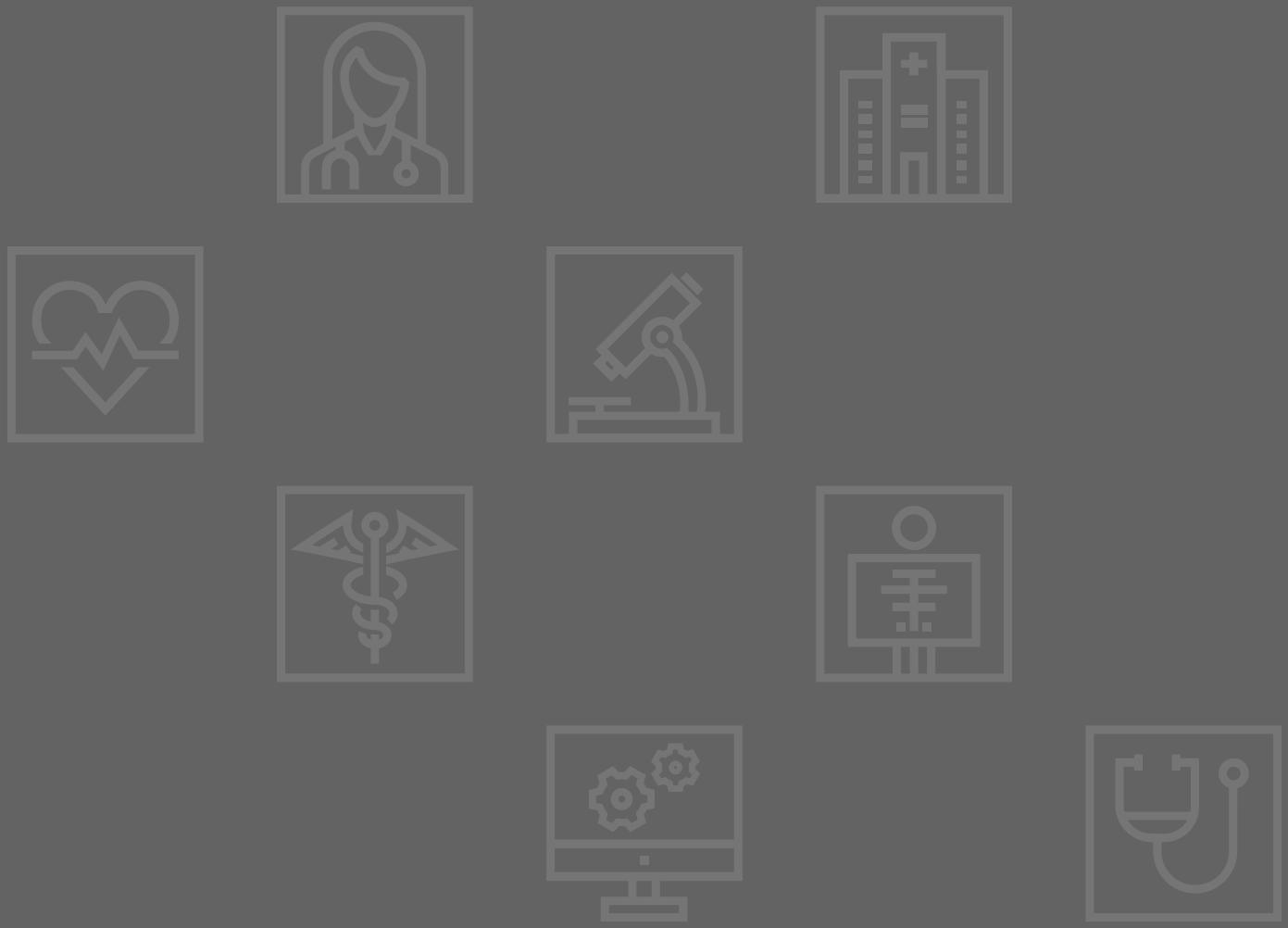
www.pwc.de/digitaleskrankenhaus

Digitalisierung im Krankenhaus? Aber sicher!

Wie Informationssicherheit im Krankenhaus umgesetzt werden kann und warum Abwarten keine gute Idee ist

pwc



Inhaltsverzeichnis

IT-Betrieb gegen Lösegeld – ein unwiderstehliches Angebot

Keine IT – keine Patientenbehandlung
Im Krankenhaus sind sämtliche IT-Systeme ausgefallen, es herrscht Chaos. Personal in weißen Kitteln eilt durch die Gänge und versucht, die schlimmsten Folgen abzuwenden und den Betrieb aufrechtzuerhalten. Wichtige Daten zu den Patient:innen werden hastig auf Papier notiert, Laboraufträge und Röntgentermine per Laufzettel angefordert. Währenddessen ist bei der Krankenhausdirektion eine Lösegeldforderung eingetroffen. Die Angreifer sind routiniert und wissen um den Wert ihrer Geisel. Sie unterbreiten ein unwiderstehliches Angebot: die Wiederherstellung des Normalbetriebs gegen einen Betrag in Millionenhöhe.

Solche Szenarien sind harte Realität, täglich fallen Unternehmen Cyberkriminellen zum Opfer und immer häufiger trifft es auch Krankenhäuser in Deutschland. Die digitale Transformation bietet enorme Chancen für unser Gesundheitssystem, doch sie schafft auch neue Risiken und offene Flanken für Angreifer. Krankenhäuser jeder Größe sind für Cyberkriminelle äußerst lukrative Angriffsziele und sie sind nicht zuletzt während der Covid-19-Pandemie noch stärker in deren Fokus geraten. Es gibt wenige Organisationen, in denen Cyberangriffe so fatale Folgen haben können – bis hin zu Patientenschäden und zum Ausfall kritischer Versorgungsstrukturen. Entsprechend groß ist der Druck, die von den Angreifern verursachte Zwangslage schnell zu beenden oder besser noch, es gar nicht erst so weit kommen zu lassen.

Die Regulierung zieht an
Der Gesetzgeber hat die Gefahr bereits erkannt. Die gesetzlichen Anforderungen an die IT-Sicherheit in Krankenhäusern werden immer weiter verschärft. Ab dem Jahr 2022 sind umfangreiche IT-Sicherheitsmaßnahmen für ausnahmslos alle Krankenhäuser verpflichtend – nicht mehr nur für Häuser, die als Kritische Infrastrukturen (KRITIS) eingestuft werden. Die Referenz für die Maßnahmen ist der Branchenspezifische Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus, den die Deutsche Krankenhausgesellschaft (DKG) in Absprache mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt hat und regelmäßig aktualisiert. Gefordert sind organisatorische und technische Maßnahmen, um die „kritische Dienstleistung“ eines Krankenhauses abzusichern. Dafür bedarf es der Einführung eines Informationssicherheitssystems (ISMS) und eines Business-Continuity-Managementsystems (BCM) sowie des aktiven Managements von Risiken, die sich aus dem Ausfall der digitalen Systeme ergeben. Das Ziel aller Maßnahmen ist, die im jeweiligen Krankenhaus etablierten Versorgungsniveaus aufrechtzuerhalten.

Die Anforderungen in der Praxis umzusetzen ist keine leichte Aufgabe. Die Handlungsfelder sind vielfältig und die implementierten Managementsysteme müssen auch tatsächlich im klinischen Alltag und in der Technik Anwendung finden. Allein das kann ein Mammutprojekt sein. Darüber hinaus sind Cyberkriminelle sehr kreativ und schnell, wenn es darum geht, neue Schwachstellen zu finden. Die Bedrohungsszenarien verändern sich dadurch ständig; oft schneller, als traditionelle IT-Abteilungen und Sicherheitsteams reagieren können. Nichtstun ist keine Option, wenn Betriebsunterbrechungen und Schaden an Patienten drohen.

Es herrscht Handlungsdruck
Zudem drohen auch den Führungskräften und Entscheider:innen im Ernstfall massive rechtliche Folgen, wenn die Frage im Raum steht, ob sie ihre Systeme nach dem Stand der Technik abgesichert haben. Dazu können vertragsärztliche Folgen, Schadensersatzforderungen, Bußgelder, die Rückforderung von Fördergeldern und – im äußersten Fall – strafrechtliche Konsequenzen gehören.

Die Krankenhausleitung steht unter Zugzwang: Prozesse und Abläufe müssen digitalisiert werden – das erfordern die Wettbewerbssituation, der Personalmangel und nicht zuletzt die drohenden Abschläge, die durch das Krankenhauszukunftsgesetz (KHZG) im Krankenhausentgeltgesetz (KHEntG) eingeführt wurden (§ 5 Abs. 3h KHEntgG). Gleichzeitig bestehen strenge Pflichten zur Absicherung digitaler Systeme, ganz allgemein aufgrund der Verantwortung von Ärzt:innen und Betreibern für die Vermeidung von Schäden und auch sehr konkret für KRITIS-Häuser (§ 8a BSIG), ebenso für Nicht-KRITIS-Häuser (§ 75c SGB V), aus Datenschutzperspektive (Art. 32 DSGVO) sowie aufgrund von Anforderungen an die Nutzung der Telematikinfrastruktur.

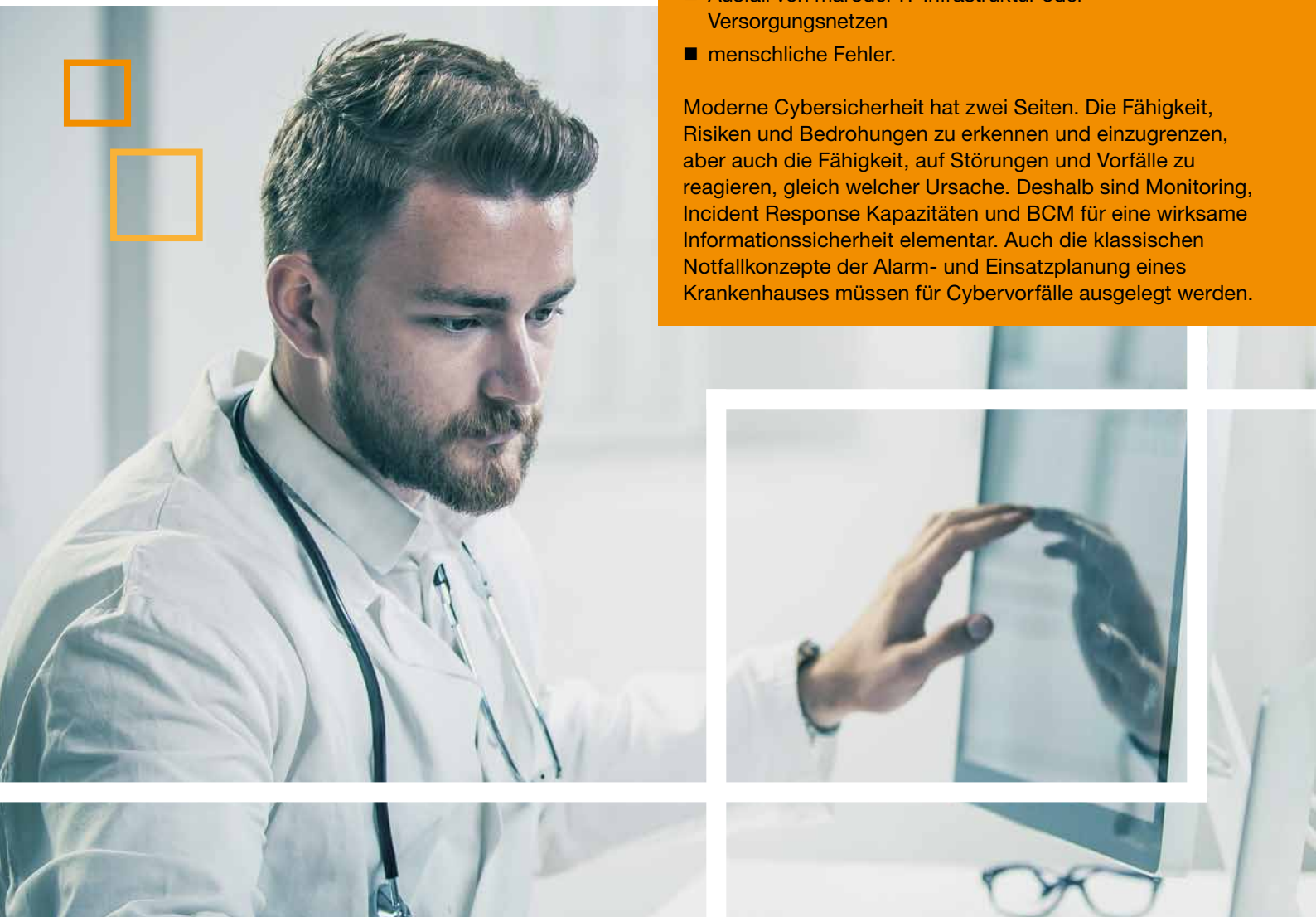
Wie können Verantwortliche angesichts dieses Handlungsdrucks klug vorgehen? Wie sehen die Risiken im Einzelnen aus und wie lassen sie sich verringern? Welche Schritte sind jetzt notwendig? Ausgehend von der Rolle der IT im Krankenhaus, der Gesetzeslage und der aktuellen Bedrohungslage werfen wir im Folgenden einen Blick auf die Folgen unzureichender Sicherheit. Anschließend skizzieren wir, wie Krankenhäuser angemessene organisatorische und technische Vorkehrungen treffen können.

Ein fähigkeitsbasierter Ansatz: Risiken minimieren und jederzeit reaktionsfähig sein

Prävention und Schutz vor Bedrohungen ist wichtig. Doch nicht immer sind Angriffe von außen Ursache für Störungen und Betriebsunterbrechungen. Auch Schwachstellen innerhalb des Krankenhauses können dazu führen, dass wichtige Systeme nicht verfügbar sind, zum Beispiel:

- Komplikationen bei Updates und Wartungsarbeiten
- Ausfall von maroder IT-Infrastruktur oder Versorgungsnetzen
- menschliche Fehler.

Moderne Cybersicherheit hat zwei Seiten. Die Fähigkeit, Risiken und Bedrohungen zu erkennen und einzugrenzen, aber auch die Fähigkeit, auf Störungen und Vorfälle zu reagieren, gleich welcher Ursache. Deshalb sind Monitoring, Incident Response Kapazitäten und BCM für eine wirksame Informationssicherheit elementar. Auch die klassischen Notfallkonzepte der Alarm- und Einsatzplanung eines Krankenhauses müssen für Cybervorfälle ausgelegt werden.



Was bedeutet Cybersicherheit im Krankenhaus?

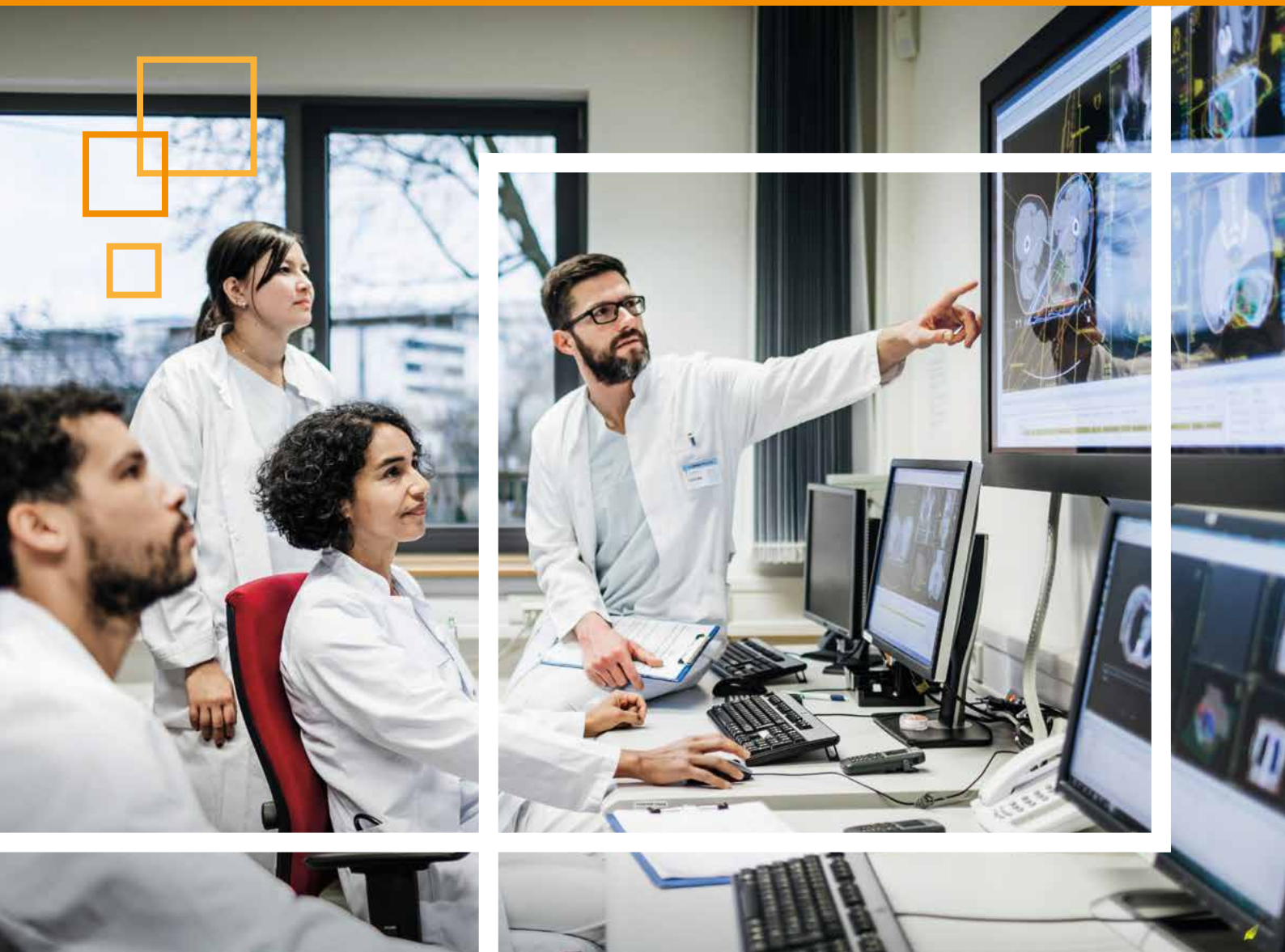
Streng genommen umfasst Informationssicherheit auch solche Informationen, die nicht mit digitalen Systemen verbunden sind, wohingegen IT-Sicherheit bzw. Cybersicherheit immer den Bezug zu technischen Systemen herstellt. Allerdings werden die Begriffe häufig synonym verwendet. Das BSI definiert den Cyberraum als „virtuellen Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme“. Dem liegt das Internet als öffentlich zugängliches Verbindungsnetz zugrunde, es kann aber durch beliebige andere Datennetze erweitert werden.

Im Krankenhaus sind das zum Beispiel Medizingerätenetze, Logistik- und Gebäudesteuerung, die Anbindungen an Krankenkassen, Aufsichtsorgane und andere Leistungserbringer (etwa die Telematikinfrastruktur), aber auch Telefon- und Kommunikationsnetze. Cybersicherheit befasst sich folglich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik im gesamten Cyberraum und schließt die davon abhängige Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein (siehe Glossar des BSI).

Im Kontext von KRITIS geht die Betrachtung weiter: Kritische Infrastrukturen sind Organisationen und Einrichtungen von hoher Bedeutung für das Funktionieren des Gemeinwesens. Sie erbringen eine kritische Dienstleistung zur Versorgung der Allgemeinheit, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde (siehe § 2 BSIG und § 1 BSI-KritisV).

Für Krankenhäuser ist das die stationäre medizinische Versorgung und hier wird deutlich, wie weit Cybersicherheit im Krankenhaus reicht: Es geht darum, die Qualität und Leistungsfähigkeit der medizinischen Versorgung abzusichern, auch bei Störung und Ausfall von IT-Systemen. IT-Betrieb in Krankenhäusern ist immer nur ein – inzwischen unentbehrliches – Mittel zum Zweck der Behandlung von Patient:innen. Gerade deswegen muss der Cybersicherheit derselbe Stellenwert eingeräumt werden wie der Hygiene und dem Qualitätsmanagement.

Das „digitale Update“ für Krankenhäuser



Digitalisierung geht nicht ohne Sicherheit
Die digitale Transformation ist ein Hoffnungsträger des Gesundheitssystems. Digitalisierung verspricht nicht weniger als die Verbesserung der Versorgung. Durch effizientere Prozesse können auch wesentliche Probleme des Gesundheitssystems wie der Mangel an Arbeitskräften gemildert werden. Diese Perspektiven treffen in vielen Krankenhäusern auf eine technologische Basis, die lange vernachlässigt wurde und nun zwangsweise einen digitalen Entwicklungssprung machen muss. Der zunehmende Digitalisierungsgrad birgt aber auch neue Cyberrisiken.

Gesetzlicher Rahmen für die digitale Transformation

Der Rechtsrahmen für die Digitalisierung des Gesundheitswesens entwickelt sich rasant weiter. Aktuell stehen Veränderungen aufgrund folgender Regelungen an:

- Durch das Krankenhauszukunftsgesetz (KHZG) wurde auch das Krankenhausentgeltgesetz (KHEntgG) ergänzt, sodass ab dem Jahr 2025 Abschläge drohen, wenn Krankenhäuser digitale Dienste, wie sie vom Krankenhauszukunftsfonds gefördert werden, nicht einführen.
- Das Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) bildet den Rahmen für digitale Gesundheitsanwendungen, den Ausbau telemedizinischer Versorgungsangebote und der Telematikinfrastruktur (E-Rezept, ePA).
- Die Gesundheits-IT-Interoperabilitäts-Governance-Verordnung (GIGV) soll die Durchgängigkeit digitaler Prozesse fördern, indem Standards und Schnittstellen informationstechnischer Systeme für alle relevanten Akteure im Gesundheitswesen transparent gemacht werden – unter anderem durch die Weiterentwicklung des Interoperabilitätsverzeichnisses vesta zu einer Wissensplattform.

Dazu kommen weitere Gesetze und Vorschriften, die unlängst im Bereich der Digitalisierung und ihrer Absicherung den Handlungsdruck gesteigert haben:

- Das Patientendaten-Schutz-Gesetz (PDSG) macht Nutzer der Telematikinfrastruktur wie Krankenhäuser für den Schutz der von ihnen verarbeiteten Patientendaten verantwortlich.
- Das KHZG macht Ausgaben von mindestens 15 Prozent zur Verbesserung der IT-Sicherheit für alle vom Krankenhauszukunftsfonds geförderten Maßnahmen verpflichtend.
- Das Onlinezugangsgesetz (OZG) verpflichtet Bund, Länder und Kommunen, bis Ende 2022 fast alle Verwaltungsleistungen auch digital anzubieten.
- Die Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) hat den Begriff der „kritischen Komponenten“ eingeführt und zwingt KRITIS-Betreiber, den erstmaligen Einsatz einer kritischen Komponente dem Bundesministerium des Innern, für Bau und Heimat anzuzeigen. Das Bundesministerium kann den Einsatz untersagen.
- Der neue § 75c SGB V macht die Absicherung nach dem Stand der Technik zu einer Pflicht für alle Krankenhäuser in Deutschland, nicht mehr nur für die KRITIS-Häuser.
- Nicht zuletzt hat die Datenschutz-Grundverordnung (DSGVO) den Bußgeldrahmen für Datenschutzverstöße auf bis zu 20 Millionen Euro festgelegt.

Keine Digitalisierung ohne Informationssicherheit
Die Initiativen zur Digitalisierung des Gesundheitswesens lassen auch die Informationssicherheit nicht außer Acht. Die Fördermittel des KHZG sind auch für Maßnahmen der Informationssicherheit vorgesehen. Die Krankenhaus-strukturfonds-Verordnung (KHSFV) schreibt vor, dass mindestens 15 Prozent der beantragten Fördermittel zur Verbesserung der Informationssicherheit genutzt werden.

Für Krankenhäuser mit mehr als 30.000 vollstationären Patienten pro Jahr greift darüber hinaus schon seit Jahren das BSI-Gesetz. Solche Krankenhäuser gelten als KRITIS. Sie müssen nachweisen, dass ihre Absicherung dem Stand der Technik entspricht, also dass sie den B3S umsetzen, und das durch „Sicherheitsaudits, Prüfungen oder Zertifizierungen“ belegen.

Mit Inkrafttreten des Patientendaten-Schutz-Gesetzes (PDSG) hat sich diese Ausnahmestellung der großen Krankenhäuser in puncto IT-Sicherheit geändert. Laut § 75c SGB V sind ab dem 1. Januar 2022 nicht mehr nur KRITIS-Häuser, sondern alle Krankenhäuser in Deutschland dazu verpflichtet, „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 […]“. Dieser Verpflichtung können Krankenhäuser mit der Umsetzung der Anforderungen des B3S ausreichend nachkommen. Die Gesetzesänderung trägt der stärkeren digitalen Durchdringung zentraler Prozesse in Kranken-häusern aller Größe Rechnung und macht den B3S zum de-facto-Standard für jedes Krankenhaus.

Was ist der B3S?

B3S steht für Branchenspezifische Sicherheitsstandards. Es handelt sich dabei um Anforderungen, deren Eignung das BSI festlegt. Für den Bereich der Krankenhäuser hat die DKG einen „Branchenspezifischen Sicherheits-standard für die Gesundheitsversorgung im Krankenhaus“ entwickelt. Wer den B3S umsetzt, sorgt dafür, dass Informationen und digitale Systeme sicher und resilient organisiert werden und das Versorgungsniveau des Krankenhauses auch bei Störungen gewährleistet bleibt.

Der Standard beschreibt Managementanforderungen, verschiedene Bedrohungsszenarien, Schwachstellen und branchenspezifische Gefährdungen sowie technische und organisatorische Maßnahmen rund um die Informations-sicherheit, das Business Continuity Management und

Risikomanagement im Krankenhaus. In Summe sind es circa 200 Anforderungen und Maßnahmenempfehlungen.

Die Schutzziele sind die klassischen Ziele der Informationssicherheit:

- **Verfügbarkeit**
  Dienstleistungen, Anwendungen und Funktionen eines IT-Systems, IT-Netzinfrastruktur oder auch Informationen können Anwender:innen stets wie vorgesehen nutzen.
- **Integrität**
  Die Korrektheit, das heißt Unversehrtheit von Daten und die korrekte Funktionsweise von Systemen sind sichergestellt. Informationen sind vollständig und unverändert.
- **Vertraulichkeit**
  Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.
- **Authentizität**
  Die Informationen wurden von der angegebenen Quelle erstellt.

Der B3S für Krankenhäuser ergänzt diese Schutzziele um die Aspekte Behandlungseffektivität und Patientensicherheit, um der Bedeutung von Informationen und IT-Systemen im Klinikbetrieb sowie den möglichen Konsequenzen ihres Ausfalls Rechnung zu tragen: Es geht in erster Linie um verlässliche medizinische Versorgung.

Die Bedrohung aus dem Netz

Zeit zu handeln

Der Alltag in Krankenhäusern findet an den Betten der Patient:innen statt: gut sichtbar, konkret in der Behandlung, schnell getaktet und bestimmt durch menschliche Interaktion. Doch wie groß ist die Abhängigkeit von funktionierender IT wirklich? Gerade Krankenhäusern, die bislang keinem Cyberangriff ausgesetzt waren, mag das Risiko eines solchen Angriffs weit entfernt und abstrakt erscheinen. Zwar geben die sich häufenden Presseberichte über angegriffene Häuser Anlass zu der Befürchtung, dass die Gefahr näher rückt. Doch es gibt auch Erfolgsmeldungen im Kampf gegen Cyberkriminalität wie etwa die erfolgreiche Bekämpfung des Emotet-Botnetzes. Und wenn bisher alles gut gegangen ist, warum dann nicht auch weiterhin?

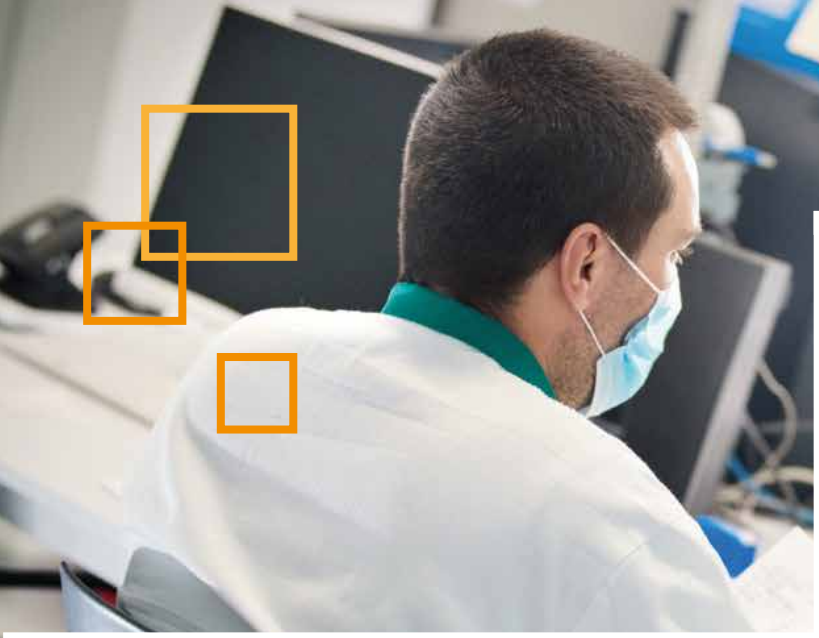
So zu denken und nichts zu tun ist nichts anderes als fahrlässig. Auch wenn die Strafverfolgungsbehörden von Zeit zu Zeit Ermittlungserfolge vorweisen können, lassen sich Cyberkriminelle nicht abschrecken und passen ihre Vorgehensweisen immer wieder an veränderte Umstände an. Viele Vorfälle gelangen außerdem gar nicht ans Licht der Öffentlichkeit, die Dunkelziffer ist hoch. Fakt ist: Das dunkle Geschäft mit der Cybererpressung floriert. Cyberkriminelle agieren in einem sich ausdifferenzierenden Ökosystem einer wachsenden Untergrundökonomie. Treffen kann es grundsätzlich jede Institution. Doch Krankenhäuser, egal welcher Größe, werden immer häufiger zu lohnenden Angriffszielen – sie sind schlichtweg gute Geiseln. Der Ausfall eines Krankenhauses erzeugt schnell öffentliches Aufsehen und wird nicht lange toleriert. Das Kalkül der Erpresser ist einfach: Je größer die Not, desto eher wird Lösegeld gezahlt.

Zero-Day-Exploits

Als Zero-Day-Exploits werden Cyberattacken bezeichnet, die Systemschwachstellen ausnutzen, die der Hersteller noch nicht erkannt hat. Am Tag 0 (zero day) gibt es also noch kein Patch oder Update, mit dem die Sicherheitslücke geschlossen werden kann. IT-Sicherheitsabteilungen sind gefordert, von solchen Vulnerabilitäten schnell zu erfahren und zur Not auch temporäre Gegenmaßnahmen zu ergreifen, zum Beispiel indem sie betroffene Systeme zeitnah vom Netz trennen oder manuell die Konfiguration anpassen. Zügiges Handeln ist oberstes Gebot; die Maßnahmen müssen notfalls auch nachts oder am Wochenende ergriffen werden.

Spätestens sobald Sicherheitsupdates verfügbar sind, gibt es keine Ausreden mehr: Die Schwachstellen waren bekannt und der Hersteller hat ein Patch zur Verfügung gestellt. Wer nicht sofort die Sicherheitslücken schließt, riskiert leichtfertig Opfer eines Angriffs zu werden. Zu professionellem Patch-Management gehört es aber auch, Updates vor der Installation zu testen, damit keine unerwünschten Nebenwirkungen auftreten und Störungen der Systeme verursachen. Geschwindigkeit und gut eingespielte Prozesse sind deshalb essenziell.



Warum Krankenhäuser im Fokus von Cyberangriffen stehen

- **Erpressung**
  Als öffentliche Infrastrukturen sind Krankenhäuser unentbehrlich. Die Bereitschaft zur Zahlung von Lösegeld scheint hoch zu sein. Es gibt Fälle, in denen zusätzlich die individuellen Patient:innen mit der Veröffentlichung ihrer Krankenakten erpresst werden.
- **Datendiebstahl**
  Patientendaten haben einen hohen Wert. Die Patientenakten von Wirtschaftsführer:innen oder Politiker:innen sowie deren Angehörigen sind besonders sensibel und von großem Interesse für Nachrichtendienste und konkurrierende Unternehmen.
- **Industrie- und Forschungsausspähung**
  Die Einsicht in Studiendaten und Patentanträge kann auf dem umkämpften Markt der Medizinbranche zum entscheidenden Wettbewerbsvorteil werden.
- **Cyberwarfare**
  Kritische Infrastrukturen sind Angriffsziele der asymmetrischen Kriegsführung. Der Ausfall eines oder mehrerer Krankenhäuser in Deutschland bindet Kräfte und Aufmerksamkeit und kann die Reaktionsfähigkeit in zwischenstaatlichen Konflikten lähmen.
- **Cyberterrorismus**
  Auch für Terroristen sind bedeutende Infrastrukturen lohnende Ziele. Die öffentliche Zugänglichkeit von Krankenhäusern und ihr vergleichsweise niedriges Schutzniveau im Cyberraum machen sie zu einfachen Opfern.

Nicht jeder Angriff zielt darauf ab, sichtbaren Schaden anzurichten oder schnelles Geld zu machen. Handelt es sich um Wirtschaftsausspähung oder Spionage durch fremde Nachrichtendienste, findet die Infiltration der Systeme heimlich statt und kann über Jahre unentdeckt bleiben.

Das Geschäft der Cyberkriminellen

- Das BSI geht in seinem Lagebericht für das Jahr 2021 von 144 Millionen neuen Schadprogrammvarianten aus und von mehr als 40.000 Bot-Infektionen deutscher Systeme pro Tag als Spitzenwert. Allein in deutschen Regierungsnetzen wurden im Durchschnitt pro Monat 44.000 E-Mails mit Schadprogrammen abgefangen.
- Das Internet Crime Complaint Center (IC3) des amerikanischen Federal Bureau of Investigation (FBI) verzeichnet eine signifikante Zunahme bekannt gewordener Schäden durch Cyberkriminalität. So stieg der Schaden von 1 Milliarde US-Dollar im Jahr 2015 auf 4,2 Milliarden US-Dollar 2020. Die Dunkelziffer, die dem IC3 nicht gemeldet wurde, dürfte um ein Vielfaches höher sein.
- Allein im Jahr 2020 wurden dem Bundeskriminalamt (BKA) 108.474 Straftaten im Bereich Cyberkriminalität in Deutschland gemeldet. Damit ist die Tendenz weiter steigend.
- Hunderte professionelle Hackergruppen lassen sich anhand ihrer Angriffsmuster unterscheiden. Sie sind Akteure in einem Ökosystem der organisierten Kriminalität, das sich zu einem hochkomplexen, arbeitsteiligen Wirtschaftszweig mit eigenen Wertschöpfungsketten entwickelt hat.
- Der Umsatz, der weltweit jährlich auf Cybercrime entfällt, wird inzwischen mit dem Bruttoinlandsprodukt von Industriestaaten verglichen und soll die Profitabilität des gesamten weltweiten Drogenhandels schon übersteigen.
- Das Strafverfolgungsrisiko ist gleich null – bei mehreren der dominanten internationalen Hackergruppen ist sogar davon auszugehen, dass sie mit staatlichen Stellen im Ausland kooperieren bzw. in einer Symbiose zusammenarbeiten. Selbst bei einfachem eCrime tun sich Ermittler und Ankläger schwer in der grenzüberschreitenden Verfolgung der Täter. Mit der Geschwindigkeit der Cyberkriminellen kann die Strafverfolgung nicht mithalten.

Cyberangriffe folgen einem typischen Muster, der sogenannten Cyber Kill Chain – von der Auskundschaftung potenzieller Ziele bis hin zur Übernahme der Kontrolle über das angegriffene System. Schadfrei abwehren lassen sich Angriffe nur in frühen Phasen.

1 **Reconnaissance**
Die Angreifer wählen das Ziel aus, spähen es aus und versuchen, Schwachstellen im Zielnetz zu finden.

2 **Weaponisation**
Die Angreifer konfigurieren eine passende Malware, zum Beispiel einen Virus oder Wurm, der auf eine oder mehrere Schwachstellen zugeschnitten ist.

3 **Delivery**
Die Angreifer übertragen die Malware in das Zielsystem (z. B. über infizierte E-Mail-Anhänge, gefälschte Websites oder USB-Sticks).

4 **Exploitation**
Der Programmcode der Malware wird im Netzwerk des Opfers ausgeführt, indem eine Schwachstelle ausgenutzt wird. Das kann auch der Mensch sein.

5 **Installation**
Die Malware installiert einen Zugangspunkt, eine sogenannte Backdoor, die dem Angreifer offensteht.

6 **Command and Control**
Die Angreifer sind zu Eindringlingen geworden, denen ein dauerhafter Zugriff auf das Netzwerk des Opfers möglich ist.

7 **Actions on Objective**
Die Eindringlinge können jetzt Maßnahmen ausführen, um ihre Ziele zu erreichen, zum Beispiel Datenexfiltration, Datenvernichtung, Störung der Systeme oder Verschlüsselung gegen Lösegeld.

Lösegeldforderung pro Organisation statt pro System
Eine der größten Gefahren für Organisationen jeder Art geht derzeit von Ransomware aus. Dabei verschaffen sich die Angreifer Zugang zu einem System, legen es lahm, indem sie Daten verschlüsseln, und fordern dann ein Lösegeld für die Entschlüsselung. Noch vor wenigen Jahren war Ransomware für eine Abrechnung pro System ausgelegt. Im Fall der Schadsoftware Locky ließ sich der Schlüssel für einen betroffenen PC für wenige Hundert Euro erwerben. Heute verschlüsseln Angreifer gleich alle Server einer Organisation und fordern Lösegelder in Millionenhöhe. Gleichzeitig verleihen sie ihrer Forderung Nachdruck, indem sie damit drohen, sensible Daten zu veröffentlichen, die sie während des Angriffs gestohlen haben – für Krankenhäuser ein Horrorszenario.

Cyberkriminelle nutzen Automatisierung und Big Data
Letztendlich treiben Cyberkriminelle ähnliche Herausforderungen wie große Unternehmen. Sie wollen effizienter werden und den Ertrag steigern. Deshalb automatisieren sie Prozesse und nutzen Big Data Technologien, um ihre Opfer im Internet zu finden und zu kompromittieren.

Dazu kommen moderne und hochgradig arbeitsteilige Organsiationsformen. Von der Entwicklung neuer Angriffsmethoden über die Infiltration von Zielen bis hin zur Abrechnung und dem „Service Desk“ für die Kommunikation mit Erpressungsopfern arbeiten viele Spezialisten an einer Attacke zusammen und sind über den Erfolg des Lösegelds incentiviert. Im Darknet lässt sich heute Ransomware-as-a-Service einfach von Profis buchen. So adaptieren Cyberkriminelle laufend neue Technologien und Organisationsformen, um ihre Ziele zu erreichen. Angreifer und Verteidiger befinden sich in einem ständigen Wettlauf um die neuesten technischen Entwicklungen.

Lösegeldforderungen für Distributed-Denial-of-Service-Attacken (DDoS-Attacken)
Die wachsende Zahl an vernetzten Endgeräten hat eine Kehrseite: Botnetze besitzen inzwischen eine höhere Angriffsqualität als noch vor wenigen Jahren. Etliche Rechner sind unbemerkt Teil eines Botnetzes, auf dem Schadcode läuft. Sie werden zum Beispiel verwendet, um Spam-Mails zu verschicken oder eine Webseite bzw. einen IT-Service mit Anfragen zu bombardieren und sie dadurch lahmzulegen. Seit Jahren steigt die Zahl solcher sogenannten DDoS-Angriffe stetig und wird weiter zunehmen, da infolge des technologischen Fortschritts immer mehr vernetzte Geräte verfügbar sind und gekapert werden können. Die Angreifer kombinieren diese Angriffe nun ähnlich wie bei Ransomware mit einer Lösegeldforderung. Die durch die DDoS-Attacke verursachte Blockade wird erst aufgehoben, wenn der Betrag gezahlt wurde. Für die Angreifer ist der Aufwand gering. Ein Botnetz mit circa 1.000 Rechnern lässt sich für die Dauer eines einstündigen Angriffs für weniger als 12 US-Dollar buchen. Dabei muss noch nicht einmal Schadcode in die Organisation eingeschleust werden. Der Angriff wird von außerhalb ausgeführt und legt wichtige Services lahm, zum Beispiel das Patientenportal oder die Schnittstellen zu vor- und nachgelagerten Leistungserbringern.




Drei Gründe für die hohe Dynamik der Bedrohungslage

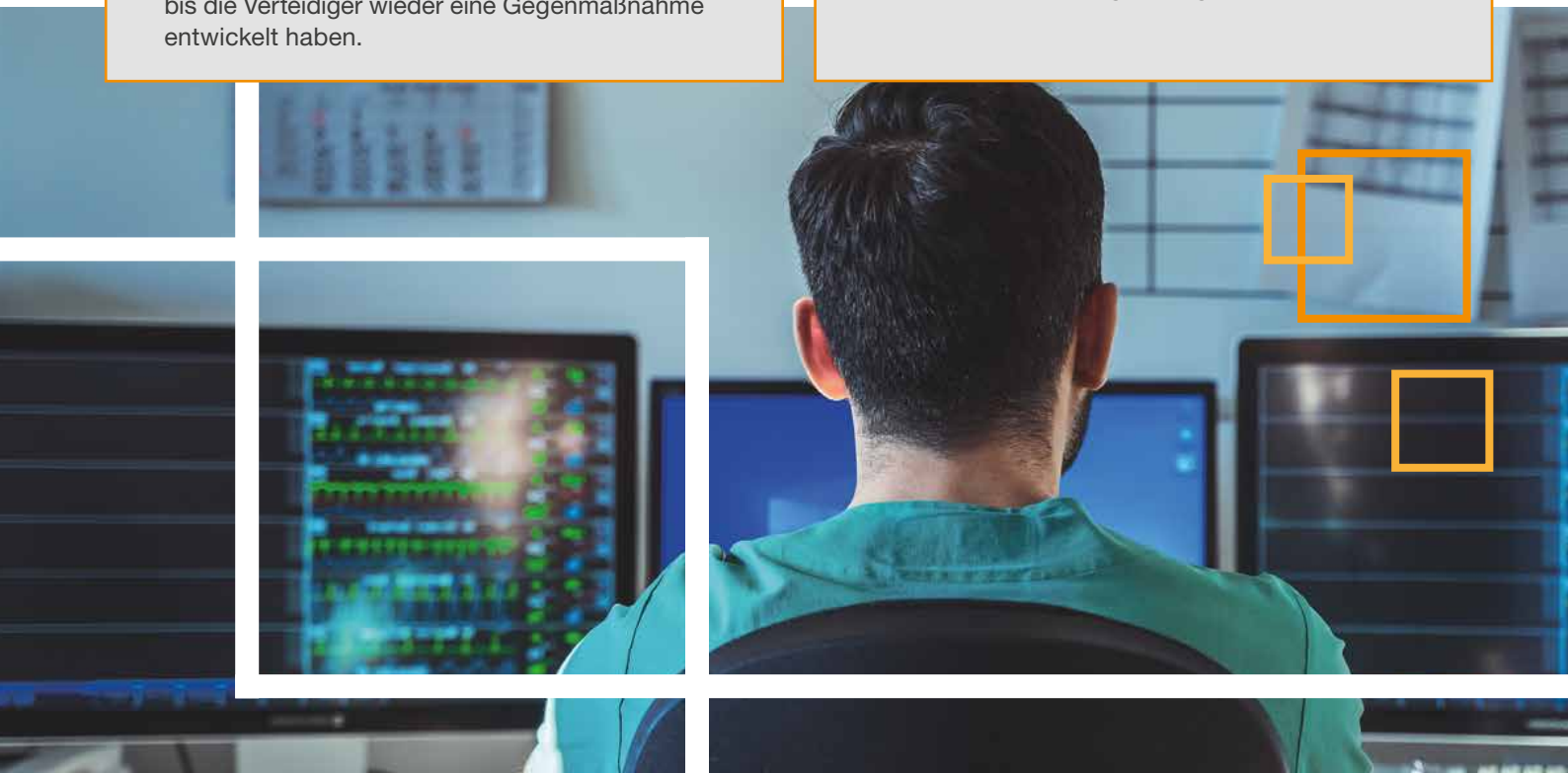
Im Bereich der digitalen Sicherheit herrscht ein Wettrennen, in dem sich die Verteidiger einer wachsenden kriminellen Industrie gegenüber sehen. Die Herausforderung entwickelt sich deshalb schneller weiter, als traditionelle Investitionszyklen und Personalgewinnung Schritt halten können.

- Cyberkriminelle sind hervorragend organisiert und in ihrem Geschäftsfeld extrem kreativ. Sie agieren in einem wachsenden, sich kontinuierlich ausdifferenzierenden Untergrundökosystem.
- Cybercrime-Organisationen agieren nach dem wirtschaftlichen Prinzip des Value-Based Pricing. Sie kennen den Wert ihrer „Leistungen“ und optimieren sukzessive ihr Geschäft.
- Die Angreifer adaptieren moderne Technologien, um den Verteidigern einen Schritt voraus zu sein – bis die Verteidiger wieder eine Gegenmaßnahme entwickelt haben.

Der Schaden ist hoch und in großen Teilen nicht versicherbar

Der Abschluss einer Cyberversicherung löst das Problem nicht. Die Kosten von Vorfällen übersteigen schnell die Deckungssummen und sind nie vollständig eingeschlossen:

- unmittelbare Betriebsunterbrechung
- Patientenschäden und Beeinträchtigung der Behandlungseffektivität
- Reputationsschäden
- Strafzahlungen
- Kosten für Sofortmaßnahmen und Nachforschungen
- Kosten für Fach- und Rechtsberatung
- Kosten für Lösegeldzahlungen
- Kosten der Wiederherstellung der Daten
- im schlimmsten Fall der Austausch der kompletten IT und Neueinrichtung der digitalen Infrastruktur.



Rechtliche Folgen unzureichender IT-Sicherheit

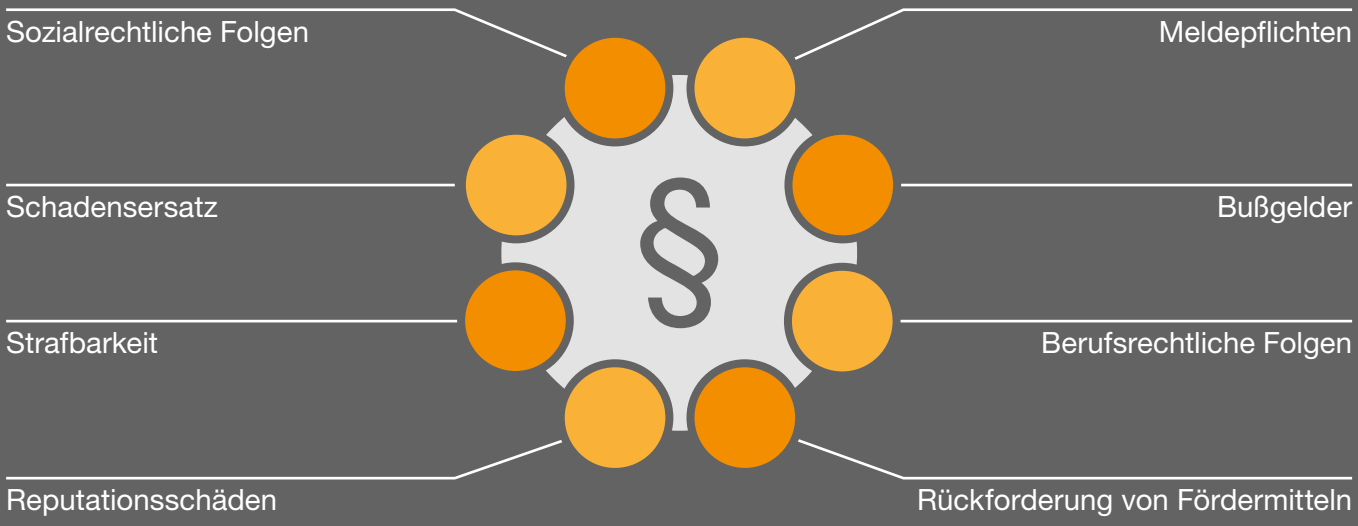
Sicherheit ist eine Organisationspficht
Was kann schon schiefgehen, wenn es ein Krankenhaus bei der IT-Sicherheit nicht allzu genau nimmt? Eine ganze Menge: Sensible Patientendaten können entwendet werden. Erfolgreiche Cyberangriffe führen im schlimmsten Fall sogar dazu, dass ein Großteil des Krankenhausbetriebs stillsteht. Je digitaler die Medizin wird, desto weniger Chancen gibt es, den Betrieb offline aufrechtzuerhalten. Das Mantra der Krankenhausalarmplanung „Zettel und Papier haben noch immer funktioniert“ ist inzwischen überholt.

Die unmittelbaren Folgen eines Cyberangriffs sind immens und reichen von Betriebsunterbrechungen über die wirtschaftlichen Kosten der Bewältigung und Wiederherstellung sowie Reputationsverluste bis hin zur Gefährdung von Patienten.

Doch auch ohne dass ein Angriff stattgefunden hat, drohen Krankenhausbetreibern und Berufsträgern eine Reihe rechtlicher Konsequenzen, wenn die IT-Sicherheitsanforderungen nicht eingehalten werden. Die Pflichten zur Absicherung der Systeme und Infrastrukturen zur Patientenbehandlung sind weitreichend. Cybersicherheit ist im Krankenhaus mittlerweile so wichtig wie Hygiene.

Im Folgenden geben wir Ihnen einen kursorischen Überblick zu den rechtlichen Folgen.

Rechtsfolgen



Sozialrechtliche Verpflichtung
Die Rechtsgrundlage für die Verpflichtung zur digitalen Absicherung von Krankenhäusern ist zunächst abhängig von der Einstufung als Kritische Infrastruktur (KRITIS) bzw. davon, in welchem Sektor der Versorgung ein Leistungserbringer tätig ist. Nachdem bislang nur die KRITIS-Krankenhäuser über das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) zur umfassenden Sicherheitsmaßnahmen verpflichtet waren, hat der Gesetzgeber mittlerweile über die §§ 75b (ambulanter Sektor) und 75c (stationärer Sektor) SGB V für beide Sektoren das abzubildende Cyber-Sicherheitsregime vollständig ausgestaltet.

Ab dem 01. Januar 2022 müssen alle Krankenhäuser angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen. Das können sie tun, indem sie einen B3S umsetzen, dessen Eignung das Bundesamt für Sicherheit in der Informationstechnologie (BSI) nach § 8a Abs. 2 BSIG festgestellt hat. Unabhängig von der Entwicklung der Standards fordert § 75c SGB V, die informationstechnischen Systeme spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen. Rechtsfolgen und Sanktionen regelt § 75c SGB V jedoch nicht. Für KRITIS-Häuser folgen diese unmittelbar aus § 8a Abs. 3 BSIG.

Im Rahmen der ambulanten Leistungserbringung müssen nach § 75b Abs. 4 SGB V alle Leistungserbringer die Anforderungen der Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung (KBV) umsetzen. Auch in § 75b SGB V sind Sanktionen bzw. Rechtsfolgen im Falle der Nicht-Umsetzung nicht unmittelbar geregelt. Da es sich jedoch um vertragsärztliche Pflichten handelt, unterliegen sie grundsätzlich dem disziplinarischen System des Vertragsarztrechts sowie die Bußgeldsanktionen der EU-Datenschutzgrundverordnung (DSGVO).

Meldepflichten nach DSGVO
Eingetretene Datenschutzverletzungen, die ein personenbezogenes Risiko beinhalten, führen nach Art. 33 DSGVO zu unverzüglichen Meldepflichten bei der dafür zuständigen Aufsichtsbehörde – möglichst innerhalb von 72 Stunden. Von Leistungserbringern im Gesundheitswesen verarbeitete Daten sind immer so sensibel, dass bei Datenschutzverletzungen solche meldepflichtigen Risiken anzunehmen sind. Mit der Meldung sind unter anderem die bereits ergriffenen Maßnahmen zur Behebung oder Abmilderung zu nennen.

Darüber hinaus müssen von allen Datenverarbeitern die von der Verletzung Betroffenen informiert werden, wenn aus der Verletzung ein hohes Risiko für ihre persönlichen Rechte resultiert (Art. 34 DSGVO). Dies wird bei Gesundheitsdaten, die ja besonders sensible Daten sind, immer anzunehmen sein. Ist eine Benachrichtigung aller Einzelpersonen nur mit unverhältnismäßigem Aufwand möglich, muss eine öffentliche Bekanntmachung erfolgen (Art. 34 Abs. 3c DSGVO).

Bußgelder
Wenn Krankenhäuser Melde- oder Benachrichtigungspflichten nicht nachkommen oder auch wenn Sicherheitsvorkehrungen unzureichend sind, können Bußgelder verhängt werden.

Bei Verstößen gegen das BSIG drohen gemäß § 14 Abs. 5 BSIG Bußgelder von bis zu 2 Millionen Euro, in besonderen Fällen sogar bis zu 20 Millionen Euro. Die DSGVO sieht Bußgelder von bis zu 10 Millionen Euro oder bis zu 2 Prozent des Jahresumsatzes vor (§ 83 Abs. 4a DSGVO). Nach Maßgabe des Art. 83 Abs. 5 in Verbindung mit Abs. 2 DSGVO können sogar bis zu 20 Millionen oder 4 % des Jahresumsatzes des Unternehmens verhängt werden, wenn es sich um besondere Kategorien von Daten oder besondere Schutzbedürftigkeit handelt.

Schadensersatz
Wenn Betroffene einen materiellen oder immateriellen Schaden erlitten haben, können sie nach Art. 82 DSGVO Schadensersatzansprüche gegen den Verantwortlichen geltend machen. Die jüngste Rechtsprechung geht davon aus, dass die Behauptung eines immateriellen Schadens und somit eines Schmerzensgeldanspruchs eine spürbare Beeinträchtigung voraussetzt. Geschädigte müssen eine objektiv nachvollziehbare Beeinträchtigung von gewissem Grad darlegen. Eine parallele vertragliche oder deliktische Haftung ist auf entsprechenden Nachweis nicht ausgeschlossen, da Art. 82 DSGVO unbeschadet der übrigen nationalen Haftungsnormen gilt.

Auch eine zivilrechtliche Haftung der Organmitglieder, sprich der Geschäftsführung und des Aufsichtsrats, sowohl im Innenverhältnis gegenüber der Krankenhausgesellschaft als auch im Außenverhältnis gegenüber den Betroffenen ist möglich.

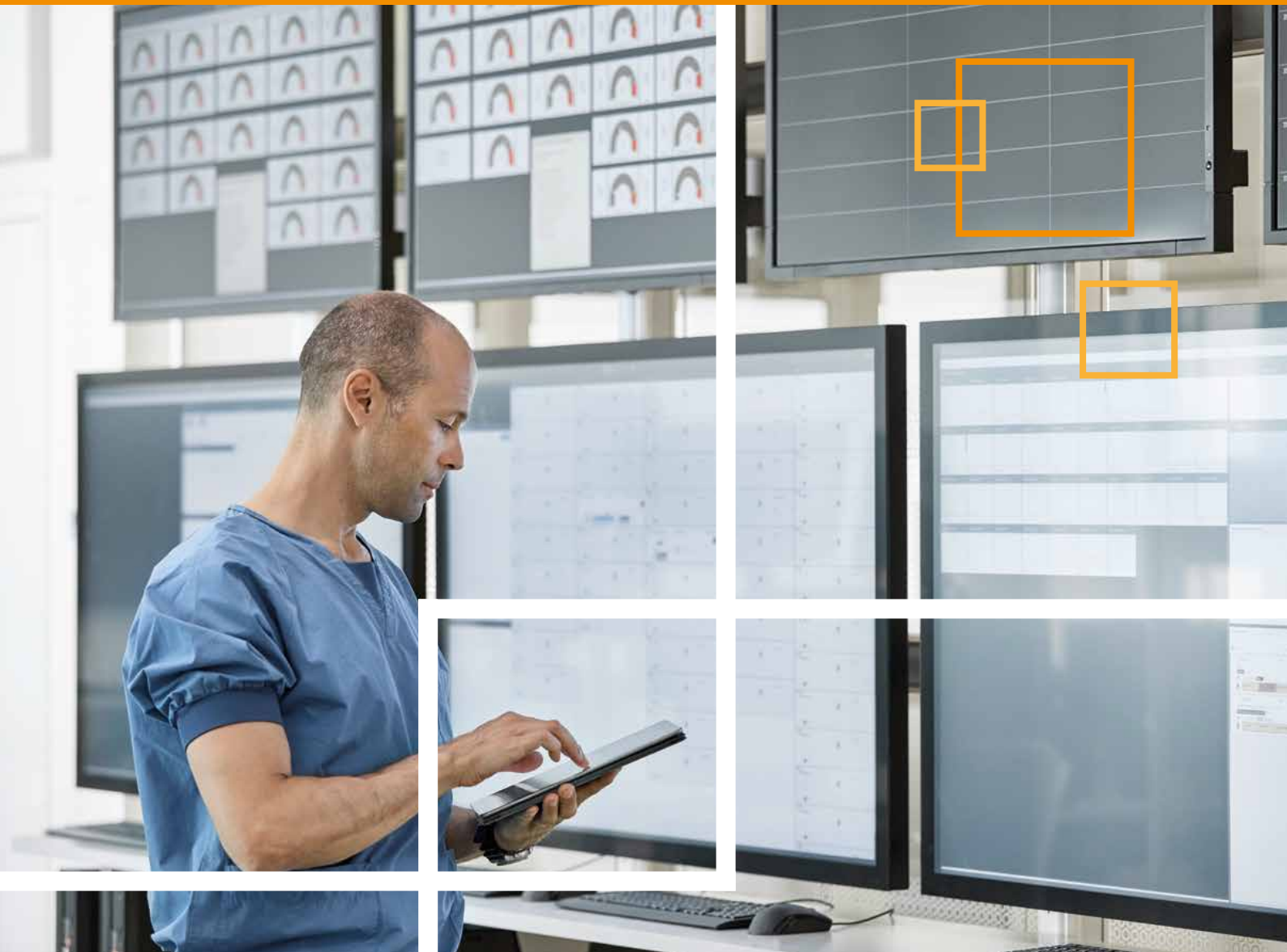
Strafbarkeit
Die besonders sensiblen Gesundheitsdaten, die Ärzt:innen im Rahmen ihrer Tätigkeit bekannt werden, sind über § 203 Abs. 1 und § 13 StGB auch strafrechtlich geschützt. Offenbaren Ärzt:innen diese Daten unbefugten Dritten, können sie sich strafbar machen. Ein Offenbaren kann auch in einem Unterlassen liegen (§ 13 StGB). Beispielsweise machen sich Ärzt:innen strafbar, wenn sie von einer Bedrohung der Daten ihrer Patient:innen wissen und dennoch nichts unternehmen, um alle (noch) nicht betroffenen Daten zu schützen. Allein aufgrund des objektiven Vorliegens von IT-Schwachstellen ist eine Strafbarkeit dagegen sehr unwahrscheinlich. In Betracht kommt sie allerdings dann, wenn die IT-Sicherheit grundlegend und bewusst vernachlässigt wird und es dadurch Dritten gelingt, auf Daten zuzugreifen. So muss nach einem Cyberangriff die Sicherheitslücke geschlossen werden, um bei einem erneuten Angriff über dieselbe Lücke vor strafrechtlichen Konsequenzen geschützt zu sein.

Berufsrechtliche Folgen
Wenn Cyberangriffe wegen unzureichender IT-Sicherheitsmaßnahmen möglich sind oder bekannt gewordene Angriffe nicht abgewendet werden, ist ein Verstoß gegen die Geheimhaltungspflicht nach § 9 Abs. 1 MBO-Ä durch Unterlassen denkbar. Berufsrechtliche Folgen greifen bei ähnlichen Gründen und Voraussetzungen wie bei der strafrechtlichen Beurteilung. Die Anforderungen sind hoch. Berufsrechtliche Maßnahmen schließen eine strafrechtliche Sanktion nicht aus.

Rückforderung von Fördermitteln
Die Auszahlungsbescheide der Fördermittel aus dem Krankenhausstrukturfonds bzw. aus dem Krankenhauszukunftsfonds stehen nach § 23 Abs. 2 Nr. 3 KHSFV unter Rückforderungsvorbehalt. Der Vorbehalt bezieht sich auf den Fall der nicht zweckentsprechenden Verwendung. So ist eine Rückforderung nach § 23 Abs. 2 und § 24 KHFSV unter anderem möglich, wenn nicht mindestens 15 Prozent der Fördermittel für die IT-Sicherheit eingesetzt wurden (§ 14a Abs. 3 Satz 5 i. V. m. Abs. 7 KHG und KHSFV).

Zukünftige Entwicklung
Grundsätzlich ist eine weitere Verschärfung der rechtlichen Anforderungen absehbar. Die kommende NIS2 Directive der EU wird eine strengere Regulierung der Cybersicherheit mit sich bringen und auf weitere Sektoren ausweiten. Eine Absenkung der KRITIS-Schwelle im Gesundheitswesen wird unabhängig davon schon länger diskutiert. Das IT-Sicherheitsgesetz 2.0 vom 28. Mai 2021 beinhaltet bereits Regelungen, welche die Sanktionen und Strafzahlungen auf das Niveau der DSGVO anheben (jetzt § 14 Abs. 5 Satz 3 BSIG mit Verweis auf § 30 Abs. 2 Satz 3 OWiG). Damit können Bußgelder von bis zu 20 Millionen Euro verhängt werden. Das bereits seit Langem angekündigte, bislang jedoch nicht umgesetzte Verbandssanktionengesetz sieht erstmals strafrechtliche Sanktionen gegen Organisationen (d. h. auch Trägergesellschaften) vor und verfolgt damit ausdrücklich das Ziel, diese zu mehr Compliance anzuhalten.

Wie funktioniert die Absicherung?



Menschen + Prozesse + Technik
Aus der Summe der Organisationsstrukturen, Prozesse, Technik und vor allem der Kompetenz der handelnden Menschen entsteht Sicherheit. Das ist in der digitalen Sphäre nicht anders als im medizinischen Betrieb und bei der physischen Sicherheit. Die gesetzlichen Verpflichtungen drängen zur Umsetzung bewährter Sicherheitsstandards, die für den medizinischen Bereich speziell adaptiert wurden.

Der B3S ist der de-facto-Standard für alle Krankenhäuser, er wird regelmäßig aktualisiert und mit dem BSI abgestimmt, um den aktuellen Stand der Technik zu reflektieren. Er ist keine Eigenentwicklung mit neuen oder überzogenen Anforderungen an Krankenhäuser, sondern basiert auf gängigen Standards, die für den Kontext von Krankenhäusern zusammengefasst wurden: ISO 27001 und 27002 (Informationstechnik), ISO 27799 (Medizinische Informatik) sowie relevante Elemente und Best Practices aus zum Beispiel ISO 27005 (Information Security Risks), ITIL (Information Technology Infrastructure Library) und COBIT (Control Objectives for Information and Related Technology). Der B3S fasst die wichtigsten Anforderungen an die Absicherung von Krankenhäusern als Kritische Infrastrukturen zusammen. Darüber hinaus kann es im Einzelfall sinnvoll sein, noch weitere Standards heranzuziehen, beispielsweise die IEC 62443 Normenreihe zur Absicherung industrieller Kommunikationsnetze. Hier muss eine Auswahl entlang des individuellen Profils und Schutzbedarfs eines Krankenhauses erfolgen.

B3S richtig umsetzen
Im Kern geht es darum, die Digitalisierung im Krankenhaus angemessen abzusichern. Die Einführung eines ISMS und eines BCM erhöht die Sicherheit der digitalen Systeme und in der Folge auch die der Patient:innen deutlich.

In der Umsetzungspraxis knirscht es jedoch im Getriebe. Noch ein Managementsystem? Noch mehr Dokumentation? Ohne die Akzeptanz der Notwendigkeit und das Verständnis für den Nutzen scheitern Projekte schon in frühen Phasen der Einbindung von Stakeholdern. Krankenhausbetreiber müssen sich zudem bewusst sein, dass ein ISMS allein noch keine Sicherheit verschafft. Es bildet lediglich den Governance-Rahmen. Wenn es nicht mit effektiven Sicherheitsmaßnahmen auf technischer und organisatorischer Ebene untermauert und in die Praxis gebracht wird, bleibt es ein leeres Konstrukt, das im Ernstfall keinen Schutz bietet.

Sicherheit als Managementaufgabe
Wenn digitale Sicherheit dauerhaft und nachhaltig gewährleistet wird, steigt nicht nur das Sicherheitsniveau. Es werden auch wieder Ressourcen frei, um mit Mut und Kreativität an der Digitalisierung des Krankenhauses der Zukunft zu arbeiten. Dem Management geben Reifegradmodelle auch im Bereich der Sicherheit eine Orientierung. Sie zeigen, wie es um die digitale Sicherheit des Hauses wirklich bestellt ist und welches Ziel erreicht werden soll. Daraus lassen sich Empfehlungen und Verbesserungsvorschläge ableiten bis zur konkreten Umsetzungsplanung. So wird Sicherheit planbar und steuerbar.

In vier Schritten zu mehr Sicherheit

Der erste Schritt bei der Verbesserung der Cybersicherheit im Krankenhaus sollte immer sein, Klarheit und eine Grundlage für die Planung und Entscheidungsfindung zu schaffen. Die anschließenden Investitionskosten sind in der Regel nicht unerheblich und Fehler in der Konzeption oder blinde Flecken in der digitalen Sicherheit können gravierende Folgen haben.

In der Security Community gilt daher dieses Sprichwort: „If you think security is expensive, try an incident."

In Sicherheitsprojekten haben sich vier methodische Schritte für den Start bewährt, die sich pragmatisch innerhalb von zwei bis vier Wochen umsetzen lassen.

1. Status-quo zu den Anforderungen des B3S erheben

Die komplette Organisation wird entlang der B3S-Anforderungen untersucht. Hierfür werden Interviews mit den Verantwortlichen zum Beispiel aus IT-Abteilung, Management, Medizintechnik, klinischem Betrieb und Qualitäts- und Risikomanagement geführt sowie Dokumente gesichtet; außerdem findet eine Begehung vor Ort statt. Der B3S führt durch alle Bereiche der Organisation, durch Klinik, Verwaltung und Logistik bis hin zu externen Dienstleistern.

Da die Status-quo-Analyse ganz am Anfang von Maßnahmen zur Steigerung der Sicherheit steht, ist es wichtig, in den ersten Gesprächen bereits Verständnis für die Anforderungen aufzubauen und die Stakeholder zu berücksichtigen. Gut moderiert und umgesetzt ist eine Status-quo-Analyse bereits ein erster Schritt auf dem Weg zu mehr Cybersicherheit.

Mangelkategorien		Feststellungen in der Prüfungs-stichprobe
1.	Informationssicherheitsmanagement-System (ISMS)	⚠
2.	Asset-Management	⚠
3.	Continuity- und Notfallmanagement für die kritische Dienstleistung	⚠
4.	Technische Informationssicherheit	⚠
5.	Personelle und organisatorische Sicherheit	⚠
6.	Bauliche/physische Sicherheit	⚠
7.	Vorfallserkennung und -bearbeitung	⚠
8.	Überprüfung im laufenden Betrieb	⚠
9.	Lieferanten, Dienstleister und Dritte	⚠
10.	Branchenspezifische Technik und (Kern-) Komponenten (Beschaffung, Entwicklung, Einsatz, Betrieb und Wartung)	⚠

2. Reifegrad und Ambitionsniveau definieren

Um im Wettlauf mit Bedrohungen im vorderen Feld zu bleiben, müssen sich die Sicherheitsverantwortlichen in Bezug auf Organisationsstrukturen, Prozesse, technische Maßnahmen und Fähigkeiten kontinuierlich weiterentwickeln. Hier ist noch kein:e Meister:in vom Himmel gefallen. Analog zum Qualitäts- und Risikomanagement muss die Organisation in einen kontinuierlichen Prozess der Verbesserung eintreten.

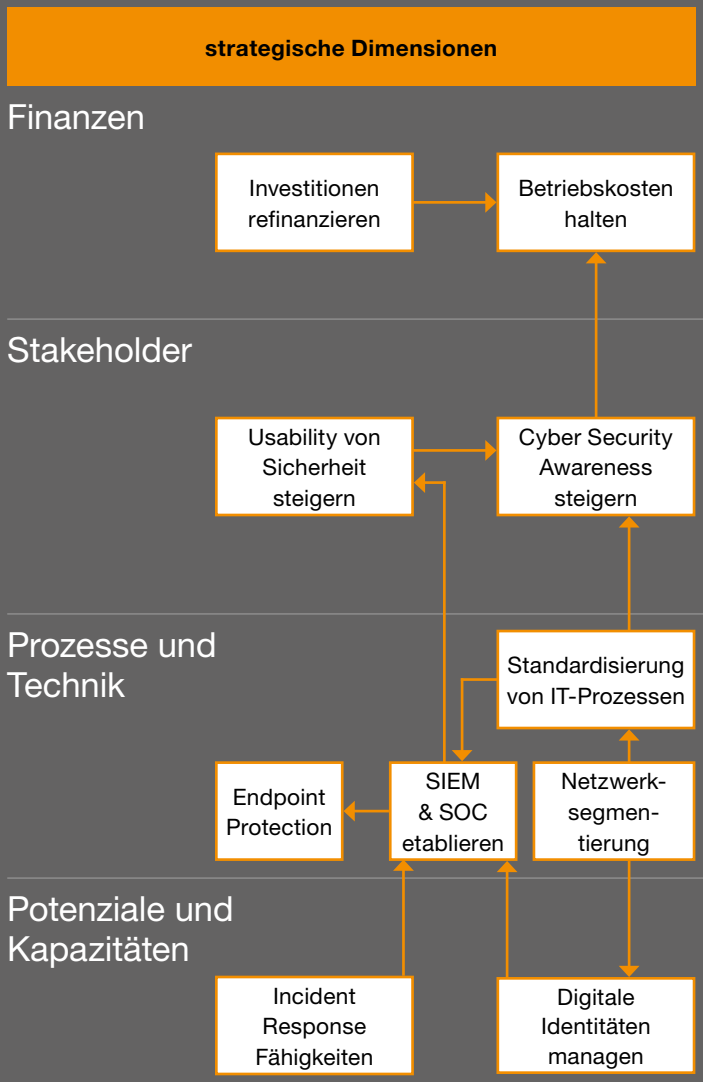
Nach Schritt 1, der Status-quo-Erhebung, lässt sich der aktuelle Reifegrad klar erkennen. Ebenso kann ein Ambitionsniveau festgelegt werden, sprich der Reifegrad, den die Organisation anstrebt. Das muss nicht immer gleich die Profiliga sein. Eine schrittweise Steigerung der Cybersicherheit ist realistischer, finanzierbar und nachhaltiger als Riesensprünge.

3. Managementmodell und Steuergrößen erstellen

Die Absicherung des Betriebs ist eine Management-verantwortung. Die Umsetzung kann in Teilen delegiert werden, für das Ergebnis bleibt die Geschäftsführung jedoch immer haftbar. Doch wie funktioniert das Management von Sicherheit aus der Perspektive der Geschäftsführung und CIOs? Unter anderem braucht es ein strategisches Modell, das festlegt, welche Faktoren wichtig sind und gestärkt werden müssen. Diese strategischen Ziele können dann mit Messgrößen, Maßnahmen und Investitionen unterlegt werden.

Alle Punkte werden in einer Cybersecurity Scorecard zusammengefasst und bilden das Management-instrument der Geschäftsführung. Die Methode ist hier beispielhaft dargestellt.

Die strategischen Handlungsfelder müsen für jedes Haus sinnvoll festgelegt werden, ebenso die Zielwerte und Maßnahmen. Auf diese Weise wird die Umsetzung von Cyber Sicherheit planbar und steuerbar von der strategischen Ebene bis hin zur Umsetzung.

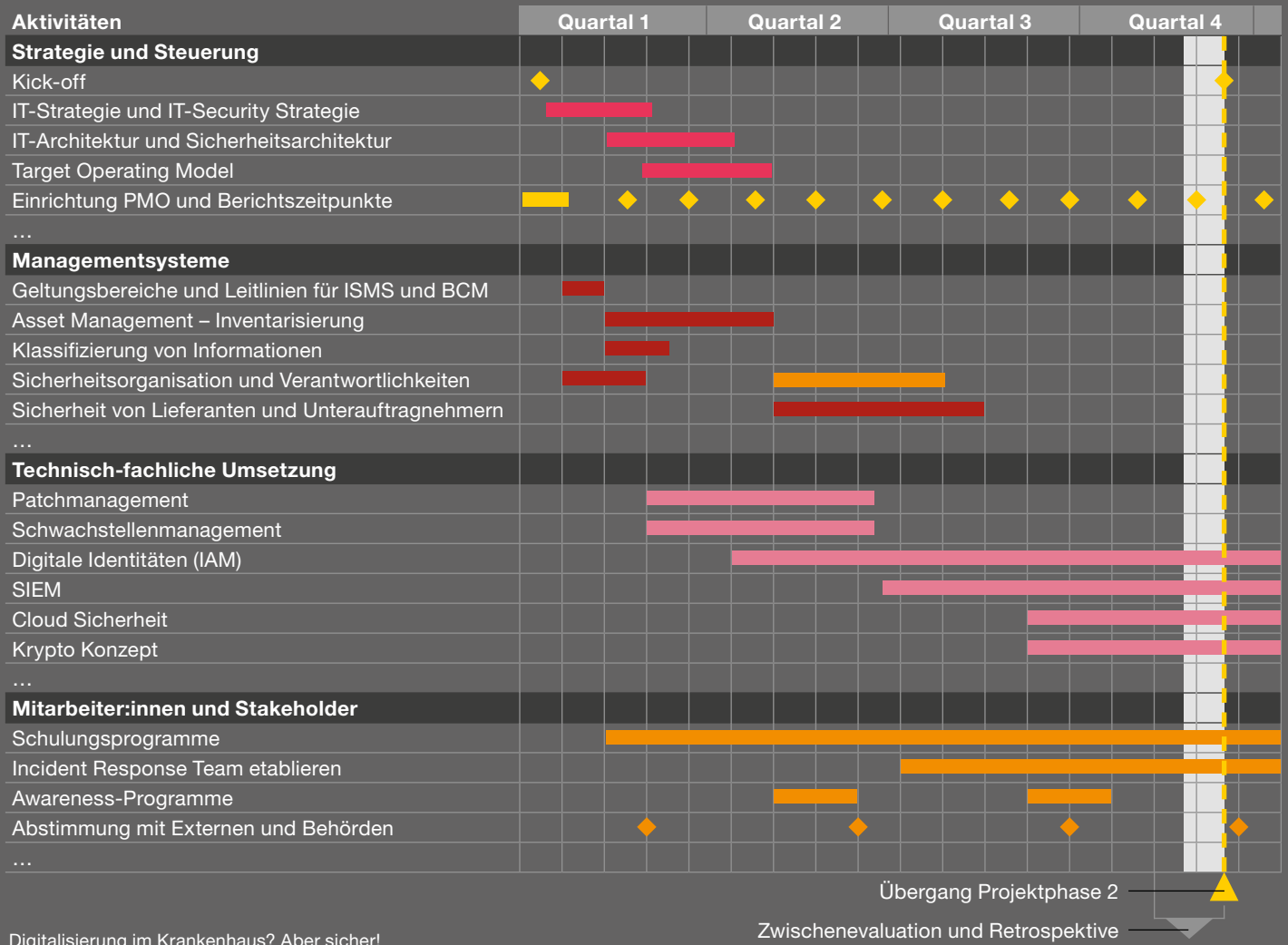


Ziele	Messgrößen	Zielwerte	Maßnahmen	Budget
• Investitionen refinanzieren, z. B. aus KHZG oder KHSF • Betriebskosten auf aktuellem Niveau halten, aber Performance steigern	• CapEx/Hardware, Software, Projekt-installation • OpEx/Betriebskosten • Fördermittelzufluss	• Förderquote von Investitionen > x % • Betriebskosten < Mittelwert 2019–2021	• Fördermittelmonitoring • Lieferanten-management • Prozessoptimierung und Outsourcing	• … • … • …
• Usability von Sicherheit aus Nutzerperspektive steigern • Cyber Security Awareness in der Klinik steigern	• Mitarbeiterbefragungen • IT-Hotline Anruferquote bzgl. Security Themen • Anzahl registrierter Regelverstöße • Teilnahme an Awareness-Schulungen	• Mitarbeiterfeedback zur Usability > x % Zustimmung • Verminderung registrierter Regel-verstöße um x % • Prozesszeit KIS Login < x Sekunden • …	• Einrichtung eines Feedbackprozesses • Einführung Service Management bei IT-Hotline • Awareness Programm • Usability als Projekt-kennzahl einführen	• … • … • … • …
• IT-Prozesse standardisieren und zentralisieren • Security Information and Event Mgt. und Security Operations Center etablierten	• Anzahl am standardisierten/ zentralisierten Prozessen • Anzahl SIEM Meldungen/SOC Incidents • …	• Prozess-standardisierung > x % • Abdeckung von > x % Geräten mit Endpoint Protection • …	• Einführung Prozess-management • SIEM installieren und schrittweise ausrollen • Projekt zur Netzwerk-segmentierung initiieren	• … • … • …
• Incident Response Fähigkeiten durch eigenes Expertenteam steigern • Zentrales Management von digitale Identitäten etablieren	• Anzahl und Kompetenzniveau des IT-Personals • Ergebnisse von Cyber-Simulationsübungen • Anzahl identitäts-führender Systeme • …	• x Mitarbeiter:innen auf Kompetenzniveau y • 100 % Erledigungsrate für Findings aus Übungen innerhalb 6 Monaten • Anzahl identitäts-führender Systeme < x %	• Personalgewinnungs- und weiterbildungs-programm • Zentralisierung Identity und Access Management	• … • …

4. Umsetzungsplan festlegen

Anschließend wird ein Umsetzungsplan erstellt, der konkrete Maßnahmen festschreibt. In der Regel gibt es nach einem Status-quo-Assessment viel zu tun – im Hinblick auf die Managementsysteme und Dokumentation genauso wie bei der Umsetzung von technischen Maßnahmen, Prozessveränderungen oder der Schulung von Mitarbeiter:innen.

Doch die richtige Reihenfolge und Taktung sind entscheidend: Nicht alles geht gleichzeitig, vielmehr sollte es eine risikoorientierte Abfolge der Maßnahmen geben. Dadurch werden die Tätigkeiten priorisiert, die den schnellsten Erfolg bei der Behebung der größten Schwachstellen und Risiken versprechen. Die folgende Darstellung ist nur ein Beispiel, die Planung muss individuell erfolgen.



Externe Datenschutz- und Informationssicherheitsbeauftragte

Es gibt viel zu tun und Expert:innen für Datenschutz und Informationssicherheit sind schwer zu finden. Die Absicherung und Umsetzung der Sicherheitsstandards dürfen aber nicht am Personalmangel scheitern. Im Zweifel bleibt die Verantwortung immer an der Geschäftsführung hängen. Kurzfristige Entlastung, aber auch dauerhafte Unterstützung können externe Datenschutz- und Informationssicherheitsbeauftragte bieten: Sie stehen mit einem festen Kontingent an Stunden und Serviceleistungen zur Verfügung. Das Krankenhaus kann so kurzfristig für Absicherung sorgen und hat Zugriff auf Expert:innen mit der Routine und Branchenkenntnis, die in dieser Form auf dem Bewerbermarkt derzeit schwer zu finden sind.

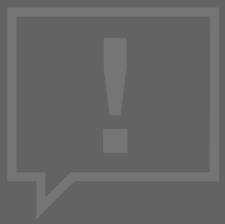
Organisations- und Kontrollversagen ausschließen
Wenn ein Krankenhaus Opfer eines Cyberangriffs wurde, bei dem möglicherweise sogar Patient:innen zu Schaden gekommen sind, ist die Führungsebene schnell mit folgenden Fragen konfrontiert:

- Hat das Management die Anforderungen an die Cybersicherheit sowie mögliche Risiken im Vorfeld ausreichend identifiziert und analysiert?
- Hat die Organisation alle notwendigen Sicherheitsvorkehrungen getroffen?
- Hat das Management überprüft, ob alle geplanten Maßnahmen auch umgesetzt wurden?

Ein standardisiertes Status-quo-Assessment und eine darauf aufbauende Umsetzungsplanung schaffen Transparenz über den Istzustand und ermöglichen es, Empfehlungen zur schrittweisen Steigerung der Sicherheit abzuleiten. Sie sind gleichzeitig der Nachweis, dass sich das Management ordnungsgemäß mit dem Thema Cybersicherheit beschäftigt hat und seinen Organisations- und Kontrollpflichten nachgekommen ist.

Handlungsempfehlungen

Keine Zeit verlieren
Die Erhöhung der Cybersicherheit entlang des B3S und die Anpassung der damit verbundenen Managementsysteme sind für Krankenhäuser wichtige Schritte, um Cyberrisiken zu verringern und die Sicherheit der Patient:innen zu gewährleisten. Wenn die Vielfalt der nötigen Maßnahmen noch unüberschaubar ist, haben sich in der Praxis folgende Handlungsfelder als sinnvolle Startpunkte bewährt.



Status quo der Cybersicherheit analysieren und Umsetzung planen

Machen Sie den Ist- und Sollzustand transparent anhand eines passenden Standards, z. B. B3S, und leiten Sie daraus eine konsequente Umsetzungsplanung ab, die aus Managementsicht auch steuerbar ist. So lässt sich ein klarer Fahrplan für weitere Maßnahmen entwickeln.

Risiken modellieren und verstehen

Schaffen Sie ein Risikobewusstsein für Ihre digitale Infrastruktur, Ihre Prozesse und die Bedrohungslage. Überprüfen Sie die Lage und Veränderungen mindestens alle drei Monate. Schließen Sie sich gegebenenfalls mit weiteren Krankenhäusern zusammen, um gemeinsam von Cybersecurity Vorfällen zu lernen und Risiken besser zu verstehen.

Regelmäßige Penetrationstests ansetzen

Führen Sie regelmäßig Penetrationstests durch, bei denen Cyberexpert:innen versuchen, in Ihre Systeme einzudringen. Wir empfehlen, sämtliche aus dem Internet erreichbaren Systeme mehrmals jährlich Penetrationstests zu unterziehen. Bei jedem Durchlauf lernen Sie neue reale Schwachstellen kennen, die geschlossen werden müssen. Verbunden werden kann das mit Phishing und Awareness Kampagnen, um die Wachsamkeit des Personals aufrechtzuerhalten.

Patch-Management professionalisieren

Aktualisierungen und Sicherheitsupdates von Software müssen unverzüglich identifiziert und möglichst schnell eingespielt werden können. Veraltete Software ist ein wesentlicher Grund dafür, dass so viele Angriffe erfolgreich sind. Vom Bekanntwerden einer Schwachstelle bis zur ersten Ausnutzung durch Angreifer vergehen keine 24 Stunden. Wenn die Schwachstellen bekannt sind, bevor der Hersteller davor warnt und Patches zur Verfügung stellt, dann spielt die Zeit noch unfairer gegen Sie.

Den Ernstfall vorbereiten

Je schneller und effektiver die Reaktion auf einen Cyberangriff ausfällt, desto höher ist die Chance, den Schaden zu begrenzen. Bauen Sie BCM und Incident-Response-Fähigkeiten in Ihrer Organisation auf. Dazu gehören Back-up-Konzepte für Daten und Systeme genauso wie Notfallpläne für IT-Personal und Management sowie regelmäßige Trainings und Simulationen von Cybervorfällen.

Digitalisierungs- und Sicherheits-expertise aus einer Hand

PwC: Digitalisierung und Sicherheit im Krankenhaus
Erfolgreiche Digitalisierung ist interdisziplinäres Teamplay – für Ihr Haus und für uns. Deswegen stellen wir Ihnen ein Paket aus Unterstützungsleistungen zur Verfügung, das alle wesentlichen Kompetenzen und Erfahrungen aus mehreren Bereichen bündelt. Für Krankenhäuser ist unsere Gesamtaufstellung besonders wertvoll. Denn der Digitalisierungsschub bewirkt, dass Sie vor einer doppelten Herausforderung stehen: Sie müssen viel Expertise und Ressourcen für Detailbereiche mobilisieren und bereithalten und parallel dazu Ihrer digitalen Transformation eine strategische Ausrichtung geben.

Um aktuelle Themen wie Digitalisierung, Prozess- und Systemberatung, IT-Sicherheit, Investitionsplanung, Fördermittel, Compliance und Haftung ganzheitlich betrachten und angehen zu können, hat PwC mehrere Fachteams in einem speziellen Health-Care-Portfolio zusammengeführt:

- Krankenhausorganisation
- IT-Management
- Cybersicherheit
- Projekt- und Change-Management
- Rechtsberatung
- Datenschutz

Sie erhalten von uns alle für Ihre Projektumsetzung benötigten Kapazitäten. Wir kümmern uns um die Planung und Steuerung und bringen umfassende Expertise und Erfahrung ein. So entlasten wir Sie, damit Sie sich auf die Konzeption und Gestaltung Ihrer digitalen Organisation konzentrieren können. Auch dabei stehen wir Ihnen selbstverständlich zur Seite.

Von der Strategie bis zur Umsetzung
Dadurch sind wir in der Lage, Sie von der strategischen Konzeption bis hin zur konkreten Umsetzung und Absicherung von Digitalisierungsvorhaben zu unterstützen. Wir kennen die Implikationen und Abhängigkeiten innerhalb des „Systems Krankenhaus“ und bilden sie in ihrer ganzen Breite und Tiefe ab. Wir verfolgen die schnelllebigen Entwicklungen Ihrer Branche genau und sind mit krankenhausrelevanten Fragen der Digitalisierung, weit über das KHZG hinaus und technologischen Entwicklungen wie 5G, Cloud Security oder der Auslagerung von Rechenzentren, sehr gut vertraut.

PwC ist historisch aus der Wirtschaftsprüfung gewachsen und hat sich zu einer führenden Beratungsgesellschaft, insbesondere für Krankenhäuser in Deutschland, weiterentwickelt. Die gründliche und nachvollziehbare Arbeitsweise ist seither Teil unserer DNA und wir sind einer hohen Qualität verpflichtet. Heute vereint PwC auf besondere Weise Fähigkeiten in der Wirtschaftsberatung und -prüfung für medizinische Einrichtungen mit einer großen Bandbreite an organisatorischen, technischen, prozessualen und juristischen Fachkompetenzen.

Ihre Ansprechpartner:innen

Digitalisierung und Sicherheit im Krankenhaus

Jörg Asma
Partner
Mobiltel.: +49 160 6142945
joerg.asma@pwc.com

Dr. Benedict Gross
Senior Manager
Mobiltel.: +49 151 14325832
benedict.gross@pwc.com

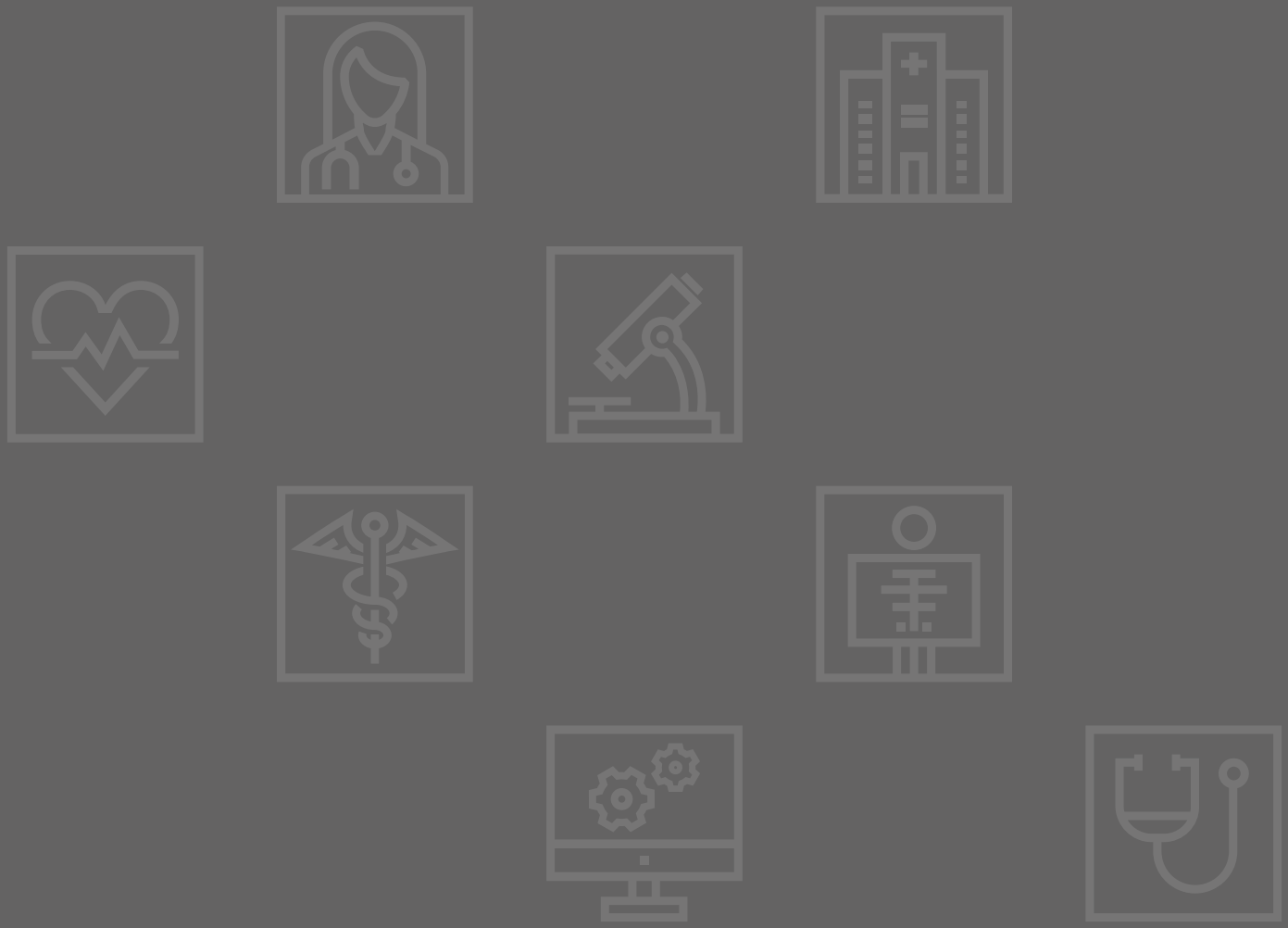
Medizinrecht und Organisations-pflichten

Jutta Dillschneider
Senior Manager
Fachanwältin für Medizinrecht und Arbeitsrecht
Mobiltel.: +49 151 54662312
jutta.dillschneider@pwc.com

Stefanie Lisson
Director
Rechtsanwältin und Steuerberaterin
Mobiltel.: +49 151 14749198
stefanie.lisson@pwc.com

Über uns
Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 155 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Rund 12.000 engagierte Menschen an 21 Standorten. 2,3 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.



www.pwc.de