Die Bedeutung der IT-Sicherheit bei Digitalisierungsprojekten

Anforderung an das Management in Krankenhäusern bei der Transformation

Von Alexander Miller, Christian Weimar und Yusuf Bicen

Das Gebiet der IT-Sicherheit ist ein dynamisches und komplexes Feld, das sich kontinuierlich weiterentwickelt, um den wachsenden Bedrohungen im digitalen Raum entgegenzuwirken. Viele Krankenhäuser werden dabei als kritische Infrastrukturen (KRITIS) eingestuft und sind daher verpflichtet, zusätzliche Verantwortlichkeiten und Pflichten in Bezug auf IT-Sicherheit und Krisenmanagement zu erfüllen. Sie müssen sicherstellen, dass ihre Systeme vor Cyberangriffen geschützt sind und im Rahmen eines Business Continuity Management im Notfall schnell wiederhergestellt werden können. Dies erfordert nicht nur technologische Maßnahmen, sondern auch organisatorische Prozessanpassungen, kontinuierliche Verbesserungen und regelmäßige Weiterentwicklung des Personals, um sicherzustellen, dass alle Mitarbeiter und Mitarbeiterinnen in der Lage sind, auf mögliche Bedrohungen zu reagieren und angemessen zu handeln.

Keywords: *Digitalisierung, IT, Strategie*

Cyberangriffe auf medizinische Einrichtungen können die Patientenversorgung beeinflussen, indem sie wichtige medizinische Geräte und Systeme beeinträchtigen und somit die Sicherheit der medizinischen Behandlung und Vertraulichkeit von Patientendaten gefährden. Der Gesetzgeber hat daher bei der Umsetzung von Digitalisierungsprojekten einen besonderen Fokus auf IT-Sicherheit gelegt, was sich vor wenigen Jahren bereits im KHZG und nun in den Richtlinien zu C5-Testat und NIS-2-Richtlinien (Network and Information Security Directive) widerspiegelt. Bei der ersten digitalen Reifegradmessung für die Krankenhäuser in Deutschland im Jahr 2021 wurde zudem festgestellt, dass die IT-Sicherheit noch weiter ausgebaut werden kann, da hier lediglich ein Reifegrad von 46 Prozent erreicht wurde. Aufgrund der vorhandenen Schwachstellen im Bereich der IT-Sicherheit steigt das Risiko von Cyberangriffen signifikant an. Im Zeitraum 2022/23 wurden dem Bundesamt für Sicherheit in der Informationstechnik (BSI) insgesamt 132 Meldungen über Cyberangriffe aus Einrichtungen des Gesundheitswesens übermittelt.

Neben dem möglichen Verlust der Reputation und Betriebsausfällen, können Cyberangriffe auch erhebliche wirtschaftliche Schäden in Millionenhöhe für die betroffenen Einrichtungen verursachen.

Um diesen Gefahren entgegenzuwirken, sollten bereits durch das Krankenhauszukunftsgesetz (KHZG) 15 Prozent der bereitgestellten 4,3 Milliarden Euro – das entspricht über 600 Millionen Euro – explizit für Investitionen in die IT-Sicherheit im Gesundheitswesen fließen, was die Bedeutung der Cybersicherheit in diesem Bereich unterstreicht. Hierbei mussten und müssen die Kliniken die in ▶Abbildung 1 dargestellten Aspekte der IT-Sicherheit berücksichtigen.

Erfahrungsgemäß haben sich die meisten Krankenhäuser auf folgende technische und organisatorische Maßnahmen fokussiert:

Erstellung und Umsetzung eines IT-Sicherheitskonzepts: Krankenhäuser sind dazu verpflichtet, ein umfassendes IT-Sicherheitskonzept zu entwickeln, das sämtliche Aspekte der Informationssicherheit abdeckt. Hierbei sind sowohl organisatorische als auch technische Maßnahmen zu berücksichtigen. Eine regelmäßige Schulung der Mitarbeiter ist dabei ein wichtiger Bestandteil des Konzepts, um ein ho- ▶

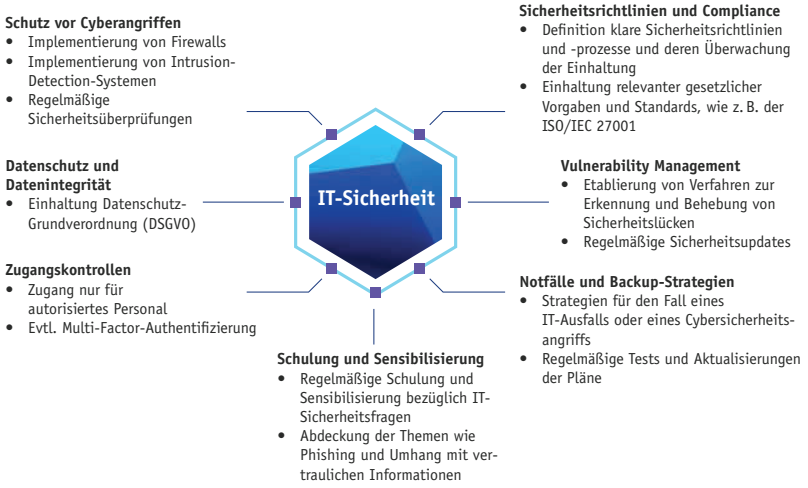

Abb. 1: Kriterien der IT-Sicherheit gemäß KHZG

Kategorie	Definition	Beispiel
Wichtige Einrichtungen	50–249 Mitarbeitende und < 50 Mio. EUR Umsatz bzw. < 43 Mio. EUR Bilanzsumme	Fachklinik mit 20 Mitarbeitenden und 15 Mio. EUR Umsatz
	< 50 Mitarbeitende und 10–50 Mio. EUR Umsatz bzw. 10–43 Mio. EUR Bilanzsumme	
Besonders wichtige Einrichtungen	> 250 Mitarbeitende und > 50 Mio. EUR Jahresumsatz bzw. > 43 Mio. Euro Bilanzsumme	Krankenhaus mit 260 Mitarbeitenden Therapiezentrum mit 55 Mio. EUR Umsatz und Bilanz von 45 Mio. EUR
Kritische Anlagen	Kritische Infrastrukturen laut BSI-Gesetz (BSIG)	Krankenhaus mit mehr als 30.000 vollstationären Fällen pro Jahr Apotheke mit mehr als 4,65 Mio. abgegebenen Packungen pro Jahr

Tab. 1: Betroffene Einrichtungen gemäß NIS-2-Richtlinie

hes Maß an IT-Sicherheit im Krankenhaus zu gewährleisten.

Einführung eines Informationssicherheitsmanagementsystems (ISMS): Ein Informationssicherheitsmanagementsystem (ISMS) hat zum Ziel, die IT-Sicherheit systematisch und kontinuierlich zu verbessern. Dabei empfiehlt es sich, sich an anerkannten Standards wie der ISO/IEC 27001 zu orientieren, um eine effektive Umsetzung des ISMS zu gewährleisten.

Die genannten Maßnahmen bilden jedoch lediglich eine Grundlage für eine sichere Organisation im Gesundheitswesen, bedürfen jedoch einer signifikanten Erweiterung, um das erforderliche Sicherheitsniveau in Zeiten von regelmäßigen Cyberattacken sowie verstärkter Nutzung von Cloud Computing zu erreichen. Die dafür erforderlichen Schritte adressiert die Regulatorik um das C5-Testat und die NIS-2-Richtlinie.

Laut einer Studie von Flying Health aus dem Jahr 2023 setzen bereits 32 Prozent der Gesundheitseinrichtungen in Deutschland auf Cloud-Computing-Dienste. Die Implementierung der elektronischen Patientenakte (ePA) sowie die verstärkte Nutzung von Telemedizin infolge der COVID-19-Pandemie haben die Adaption von Cloud-Technologien begünstigt. Krankenhäuser und Arztpraxen nutzen vermehrt Cloud-basierte Lösungen, um Patientendaten sicher zu verwalten und administrative Prozesse effizienter zu gestalten.

Das C5-Testat (Cloud Computing Compliance Controls Catalogue) ist ein Standard des Bundesamts für Sicherheit in der Informationstechnik (BSI), der die spezifischen Anforderungen an die Sicherheit von Cloud-Diensten definiert. Seit dem 1. Juli 2024 müssen Cloud-Anbieter im Rahmen des Digitalisierungsgesetzes (DigiG) ein C5-Testat Typ 1 (Prüfung der Angemessenheit) vorweisen, um die Sicherheitsstandards und Compliance-Anforderungen gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu erfüllen. Ab 1. Juli 2025 ist die Nachweis von C5-Testat Typ 2 (Wirksamkeitsprüfung) erforderlich. Diese Regelung gilt für Anbieter, die Cloud-Computing-Dienste im Gesundheitswesen zur Verarbeitung von personenbezogenen Gesundheits- und Sozialdaten nutzen. Die Anforderung ist im neu eingeführten § 393 des Fünften Buches Sozialgesetzbuch (SGB V) festgelegt, welcher im Rahmen des DigiG umgesetzt wurde. Das C5-Testat ist ein Prüfungsnachweis, der regelmäßig ab dem Zeitpunkt der Ersttestierung jährlich erneuert werden sollte, um die fortlaufende Einhaltung der Sicherheitsanforderungen sicherzustellen.

Wenn Cloud-Anbieter das C5-Testat nachweisen müssen, welche Maßnahmen müssen dann die Geschäftsführer von Gesundheitseinrichtungen ergreifen, um sicherzustellen, dass die Cloud-Dienstleistungen den Anforderungen des C5-Standards entsprechen und die Sicherheit der verarbeiteten personenbezogenen Gesundheits- und Sozialdaten gewährleistet ist?

Anbieterauswahl: Bei der Auswahl von Cloud-Diensten müssen Krankenhäuser sicherstellen, dass die Anbieter regelmäßig das C5-Testat nachweisen können. Dies erfordert eine sorgfältige Prüfung und Bewertung der Anbieter.

„Die genannten Maßnahmen bilden jedoch lediglich eine Grundlage für eine sichere Organisation im Gesundheitswesen, bedürfen jedoch einer signifikanten Erweiterung, um das erforderliche Sicherheitsniveau in Zeiten von regelmäßigen Cyberattacken sowie verstärkter Nutzung von Cloud Computing zu erreichen. Die dafür erforderlichen Schritte adressiert die Regulatorik um das C5-Testat und die NIS-2-Richtlinie."

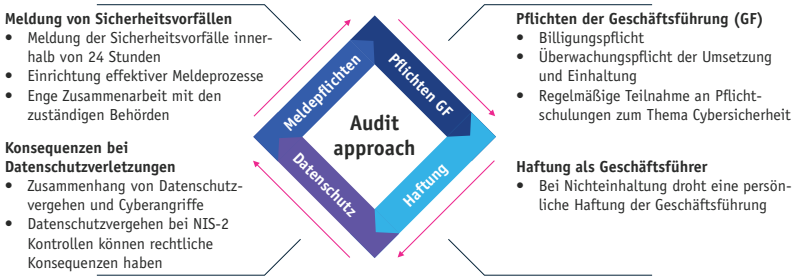

Abb. 2: Handlungsmaßnahmen und Folgen bei Nicht-Einhaltung für NIS-2-Richtlinie

Tatbestand	Betreiber kritischer Anlagen	Besonders wichtige Einrichtungen	Wichtige Einrichtungen
Kontaktstelle ist nicht erreichbar	bis zu 100.000 EUR	bis zu 100.000 EUR	bis zu 100.000 EUR
Die Registrierung wurde nicht (rechtzeitig) vorgenommen	bis zu 500.000 EUR	bis zu 500.000 EUR	bis zu 500.000 EUR
Risikomanagement und Sicherheitsmaßnahmen wurden nicht richtig / vollständig / rechtzeitig umgesetzt	bis zu 10 Mio. EUR oder 2 % des Jahresumsatzes des Vorjahres	bis zu 10 Mio. EUR oder 2 % des Jahresumsatzes des Vorjahres	max. 7 Mio. EUR oder 1,4 % des Jahresumsatzes des Vorjahres
Ein Sicherheitsvorfall wurde nicht (rechtzeitig) gemeldet	bis zu 10 Mio. EUR oder 2 % des Jahresumsatzes des Vorjahres	bis zu 10 Mio. EUR oder 2 % des Jahresumsatzes des Vorjahres	max. 7 Mio. EUR oder 1,4 % des Jahresumsatzes des Vorjahres
Ein Nachweis zur Anforderungserfüllung wurde nicht vorgelegt	bis zu 500.000 EUR	bis zu 500.000 EUR	bis zu 500.000 EUR

Tab. 2: Bußgeldkatalog (Auszug) für NIS-2-Richtlinie

Compliance-Management: Um sicherzustellen, dass die genutzten Cloud-Dienste weiterhin den Sicherheitsstandards entsprechen, ist es erforderlich, die Einhaltung der C5-Anforderungen regelmäßig zu überprüfen.

Krankenhaus als Cloud-Anbieter: Sofern ein Krankenhaus oder ein Krankenhausverbund die Cloud-First-Strategie verfolgt und selbst Cloud-Dienste entwickelt bzw. betreibt, bedarf es einer fachlichen und ggf. rechtlichen Überprüfung, ob das Krankenhaus selbst ein C5-Testat benötigt.

Parallel dazu werden auch auf europäischer Ebene die Sicherheitsanforderungen für die IT-Sicherheit signifikant verschärft, indem die Cybersicherheit von essenziellen Infrastrukturen umfassend ausgebaut und vereinheitlicht werden soll.

Die NIS-2-Richtlinie ist eine EU-weite Regelung, die im Jahr 2022 in Kraft getreten ist und das Ziel verfolgt, die Cybersicherheit in kritischen Infrastrukturen zu verbessern. Diese umfassen Einrichtungen und Systeme, die essenziell für das Funktionieren von Gesellschaft und Wirtschaft sind. Zu diesen zählen gewöhnlich Bereiche wie Energieversorgung, Transportwesen, Wasserversorgung, Gesundheitswesen, digitale Infrastrukturen und das Finanzsystem. Die EU-Mitgliedstaaten sind verpflichtet, die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umzusetzen. Krankenhäuser gehören zu den betroffenen Sektoren und müssen nun strengere Sicherheitsanforderungen erfüllen, um den Anforderungen der NIS-2-Richtlinie zu entsprechen. Die Einstufung der Krankenhäuser als wichtige Einrichtungen richtet sich nach der Kapazität der Einrichtung (▶Tab. 1).

Um die Anforderungen zu erfüllen und Sanktionen zu vermeiden, muss die Geschäftsführung der betroffenen Krankenhäuser geeignete organisatorische Maßnahmen ergreifen (▶Abb. 2). Welche Maßnahmen dies im Einzelnen sind, hängt von den spezifischen Anforderungen ab und erfordert eine sorgfältige Analyse und Planung. Die Art der Sanktionen bei Nichteinhaltung der Richtlinien hängt von den jeweiligen Anforderungen ab. Finanzielle Sanktionen können für Krankenhäuser, die ohnehin wirtschaftlich angeschlagen sind, zu zusätzlichen Liquiditätsproblemen führen (▶Tab. 2).

Fazit

Die regulatorischen Vorgaben nach KHZG, C5-Testat und NIS-2-Richtlinie unterstreichen die Notwendigkeit für Krankenhäuser, nicht nur technische Mittel bereitzustellen, sondern auch auf die Auswahl und Überprüfung bei der Kriterien Erfüllung von IT-Dienstleistern, die Implementierung von Risikomanagementprozessen und den Aufbau der IT-Kompetenz des Managements zu achten. Es obliegt der Geschäftsführung, die Implementierung der IT-Sicherheitsanforderungen zu steuern, und sie trägt die Verantwortung für alle Konsequenzen, die sich aus einer Nichterfüllung dieser Anforderungen ergeben. Daher ergeben sich für die Geschäftsführungen der Krankenhäuser hierbei zwei besondere Herausforderungen. Zum einen sind die Spezifikationen der gesetzlichen Anforderungen nicht einheitlich, zum anderen ist die Umsetzung der Maßnahmen mit Kosten verbunden, die nur zum Teil durch Förderung refinanziert werden.
Um eine effektive Etablierung der IT-Sicherheitsmaßnahmen in den Gesundheitseinrichtungen zu ermöglichen, empfiehlt es sich, das Thema IT-Sicherheit als expliziten Baustein der Digitalisierungsstrategie zu integrieren. Diese sollte dann Eingang in der kurz-, mittel- und langfristigen Unternehmensstrategie finden, damit die erforderlichen technischen, personellen und organisatorischen Auswirkungen frühzeitig auch in den Wirtschaftsplänen kalkulieren werden können. ■

Alexander Miller
Senior Manager Healthcare
KPMG AG Wirtschaftsprüfungsgesellschaft
alexandermiller@kpmg.com

Christian Weimar
Manager Healthcare
KPMG AG Wirtschaftsprüfungsgesellschaft
cweimar@kpmg.com

Yusuf Bicen
Healthcare
KPMG AG Wirtschaftsprüfungsgesellschaft