BDO/DKI-Studie 2025

Cybersicherheit im Krankenhaus

DEUTSCHES KRANKENHAUS INSTITUT

BDO

Inhaltsverzeichnis

Vorwort

Prof. Dr. Volker Penter

Wirtschaftsprüfer
Steuerberater
Partner, Advisory
Gesundheitswirtschaft

Tel.: +49 351 8669 131
volker.penter@bdo.de

Prof. Dr. Alexander Schinner

Partner, Cyber Incident
Response & Crisis Center
Business Continuity Management
Security Operation Center
BDO Cyber Security GmbH

Tel.: +49 351 8669 131
volker.penter@bdo.de

Dr. Karl Blum

Vorstand, Leiter, Geschäftsbereich Forschung,
Deutsches Krankenhausinstitut GmbH

Tel.: +49 211 47051 17
karl.blum@dki.de

Effizienzgewinne, Entlastung des knappen Fachpersonals oder auch eine weitgehende Vernetzung – positive Aspekte im Rahmen der fortschreitenden Digitalisierung im Gesundheitswesen gibt es viele. Auf der anderen Seite bringt diese Entwicklung auch zunehmend Risiken mit sich, neben technischen Herausforderungen vor allem durch Cyber-Kriminalität. Gemeinsam mit dem Deutschen Krankenhausinstitut haben wir uns des Themas angenommen und liefern mit der diesjährigen Ausgabe unserer jährlichen „Krankenhausstudie“ unter der Headline „Cybersicherheit im Krankenhaus“ einen kompakten Überblick über Wahrnehmung, Betroffenheit und existierende Schutzmaßnahmen in deutschen Krankenhäusern. Das Ergebnis zeigt dabei deutlich, so viel können wir vorwegnehmen, dass Cyber-Sicherheit kein technisches Randthema ist. Vielmehr ist sie eine strategische Aufgabe, die unmittelbar die Versorgungsfähigkeit und die Patientensicherheit berührt.

Wie aber sehen die Ergebnisse im Detail aus? Welche Faktoren unterstützen Deutschlands Krankenhäuser und Ihre Verantwortlichen rund um dieses Thema und wo lauern Hemmnisse und Stolperfallen? Diesen Themen haben wir uns ebenso gewidmet, wie einer gründlichen Bestandsaufnahme.

Im Ergebnis bieten wir Ihnen nicht nur repräsentative Zahlen und Fakten rund um dieses Thema für die deutsche Krankenhauslandschaft, wir zeigen auch Handlungsfelder und Herausforderungen für Verantwortlichkeiten auf – sowohl im Bereich der Krankenhäuser als auch der Träger. Denn, und das zeigt unsere Erhebung ganz deutlich, „Luft nach oben“ ist in diesem Bereich deutlich vorhanden – sowohl im organisatorischen Bereich und rund um die Digitalisierung als auch im Bereich der Schaffung und Stärkung einer Resilienz unserer deutschen Krankenhäuser. Um die Kliniken in Deutschland effizient vor den immer skrupelloser werdenden Angriffen Krimineller zu schützen, besteht also Handlungsbedarf – sowohl auf finanzieller als auch auf praktischer Ebene.

Wir hoffen, Ihnen mit dieser Studie spannende Einblicke und Entscheidungsgrundlagen zu liefern, die Ihnen Impulse für konkrete Maßnahmen in Ihren jeweiligen Verantwortungsbereichen geben. Gerne steht BDO Ihnen mit dem gesamten Service-Portfolio rund um den Healthcare-Bereich dabei beratend zur Seite - ganz gleich ob in den klassischen Bereichen von Prüfung und Steuerberatung, mit unserer branchenerfahrenen Digitalisierungsberatung oder mit den vielfältigen Services unserer BDO Cyber Security GmbH.

Krankenhäuser nehmen eine zentrale Rolle in unserer Gesundheitsversorgung ein – und sind als Teil der kritischen Infrastruktur (KRITIS) unverzichtbar. Ihre Kernaufgabe besteht darin, die Patientenversorgung auch unter außergewöhnlichen Bedingungen aufrechtzuerhalten. Krisenereignisse wie Naturkatastrophen, Pandemien oder großflächige Stromausfälle stellen dabei komplexe Anforderungen, da sie medizinische, organisatorische und technische Strukturen gleichzeitig betreffen. Eine besonders brisante und immer drängender werdende Gefahr: Cyberangriffe auf die IT-Systeme der Krankenhäuser. Diese Bedrohung gewinnt an Bedeutung und erfordert besondere Aufmerksamkeit.

Vor diesem Hintergrund widmet sich die BDO/DKI-Krankenhausstudie 2025 dem Thema Cybersicherheit im Krankenhaus. Die Ergebnisse unterstreichen die hohe Relevanz: Jedes fünfte Krankenhaus war in den vergangenen drei Jahren von einem Cyberangriff betroffen. Zudem erwarten die meisten Einrichtungen eine Verschärfung der Bedrohungslage. Trotz umfangreicher Präventions- und Schutzmaßnahmen bleibt das Risiko für deutsche Krankenhäuser, Ziel von Cyberattacken zu werden, hoch.

Einer der Gründe für die häufig noch ausbaufähige Cyber-Abwehr deutscher Krankenhäuser ist neben fehlenden personellen Ressourcen vor allem auch eine angespannte finanzielle Situation. Vor diesem Hintergrund empfiehlt die Studie das Thema Cybersicherheit in den Kliniken klar zu priorisieren und eine stärkere politische Unterstützung einzufordern. Die Ergebnisse machen deutlich:

Investitionen in qualifiziertes Personal, strukturierte Notfallpläne und risikoorientierte Sicherheitskonzepte sind keine reine IT-Aufgabe, sondern eine Voraussetzung für die Sicherstellung der Patientenversorgung. Gleichzeitig ist die Politik gefordert, regulatorische Hürden abzubauen, die derzeit die Einführung von IT-Sicherheitsmaßnahmen erschweren, und eine angemessene Refinanzierung der zusätzlichen Kosten für die Cybersicherheit zu gewährleisten.

Das DKI bedankt sich herzlich bei allen Krankenhäusern, die durch ihre Teilnahme die Durchführung der Studie ermöglicht haben. Ebenso danken wir unserem Kooperationspartner BDO für die gewohnt sehr gute und professionelle Zusammenarbeit.

Management Summary

Die Bedrohungslage durch Cyberkriminalität hat sich durch technologische Fortschritte und globale Konflikte in den letzten Jahren stark verschärft. Besonders gefährdet sind Krankenhäuser, wo Cyberangriffe nicht nur sensible Patientendaten, sondern auch die klinische Versorgung bedrohen.

Jedes 5. Krankenhaus war in den letzten 3 Jahren bereits von Cyberkriminalität betroffen. Dabei spielten vor allem Angriffe mittels Malware (z. B. Viren, Würmer, Trojaner, Spyware und Rootkits) eine zentrale Rolle. 90 % der Krankenhäuser schätzen die Bedrohungslage durch Cyberkriminalität für ihre Einrichtung als hoch oder sehr hoch ein und erwarten eine Zunahme in den nächsten 2 Jahren. Auch Zulieferer oder Dienstleister waren bei jedem 2. Krankenhaus bereits von Cyberangriffen betroffen.

Als Schutzmaßnahmen sind Basislösungen, wie Antivirensoftware und Firewalls, nahezu flächendeckend eingeführt. Zudem werden Mitarbeiterinnen und Mitarbeiter z. B. durch Schulungen für die Risiken der IT-Sicherheit in den meisten Krankenhäusern sensibilisiert (75 %). Nachholbedarf gibt es z. B. bei der Implementierung von Business Continuity Management Systemen und bei Notfallübungen zu Cyberangriffsszenarien.

Die Umsetzung organisatorischer und technischer Maßnahmen der IT-Sicherheit wird aus Sicht der Krankenhäuser vor allem durch zu viele Anforderungen und Regularien sowie Personal- und Budgetmangel behindert. Strategisch wird die IT-Sicherheit durch Geschäftsführung und IT-Abteilung verantwortet. Die operative Umsetzung obliegt zumeist der IT-Abteilung. Eine eigene Abteilung für IT-Sicherheit ist eher selten.

Das sind zentrale Ergebnisse der Krankenhaus-Studie 2025 der BDO AG Wirtschaftsprüfungsgesellschaft (BDO) und des Deutschen Krankenhausinstituts (DKI). Die Studie fokussiert Einschätzungen zur Bedrohungslage durch Cyberangriffe, Maßnahmen der IT-Sicherheit und vorherrschende Herausforderungen bei deutschen Krankenhäusern. Mittels einer Repräsentativbefragung von Krankenhäusern wurde die aktuelle Lage in Bezug auf Cybersicherheit aus Krankenhaussicht erfasst. Bundesweit beteiligten sich 177 Allgemeinkrankenhäuser ab 100 Betten an der Repräsentativbefragung.

Studiendesign

Die Krankenhaus-Studie 2025 der BDO AG Wirtschaftsprüfungsgesellschaft (BDO) und des Deutschen Krankenhausinstituts (DKI) befasst sich mit dem Thema Cybersicherheit im Krankenhaus. Durch die steigende Digitalisierung in deutschen Krankenhäusern und globale Konflikte gewinnt das Thema Cybersicherheit im Krankenhaus zunehmend an Bedeutung. Krankenhäuser müssen sich immer stärker der Verantwortung für den Schutz sensibler Patientendaten und den sicheren Betrieb medizinischer Systeme stellen. Gleichzeitig steigt das Risiko für Cyberkriminalität. Folgende Fragen stehen im Zentrum der vorliegenden Analyse: Wie schätzen Krankenhäuser die Bedrohungslage durch Cyberkriminalität ein? Wie stark sind Krankenhäuser bereits betroffen? Welche Sicherheitsmaßnahmen werden technisch und organisatorisch bereits umgesetzt? Wie sind operative und strategische Verantwortlichkeiten bezüglich IT-Sicherheit geregelt? Wo besteht Optimierungsbedarf und was sind die größten Hindernisse?

Mittels einer Repräsentativbefragung von Krankenhäusern wurden diese Fragen aus Krankenhaussicht beantwortet.

Grundgesamtheit der Studie bilden alle Allgemeinkrankenhäuser ab 100 Betten. Krankenhäuser unter 100 Betten wurden nicht in die Erhebung einbezogen, da es sich vielfach um Kliniken mit besonderer Struktur handelt (z. B. Privatkliniken ohne Versorgungsvertrag, kleine Fach- und Belegkliniken). Durch die Nicht-Einbeziehung dieser Häuser, auf die bundesweit nur rund 4 % der Betten, der Patienten und des Krankenhauspersonals entfallen, wird eine homogenere Gruppe der kleineren Krankenhäuser in der Grund- und Regelversorgung geschaffen.

Die standardisierte Befragung wurde von Mitte Juli 2025 bis Mitte August 2025 durchgeführt. Der Fragebogen konnte wahlweise schriftlich oder online beantwortet werden. Grundlage der Befragung bildete ein von BDO und DKI entwickelter Fragebogen mit rund 100 Items. Adressat der Befragung waren die Geschäftsführungen der Krankenhäuser.

An der Befragung beteiligten sich bundesweit insgesamt 177 Krankenhäuser. Die Ergebnisse sind repräsentativ für die Grundgesamtheit der Krankenhauslandschaft.

Gesetzliche Rahmenbedingungen

Die Verpflichtung zur Umsetzung der IT-Sicherheit gilt für Krankenhäuser aller Größen. Dabei steht § 391 SGB V im Zentrum der gesetzlichen Regelungen für Krankenhäuser und verpflichtet die Einrichtungen, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu treffen.

Die Funktionsfähigkeit des Krankenhauses und der Schutz der Patientendaten sollen dabei an erster Stelle stehen. In der vorliegenden Studie wurden die Krankenhäuser daher nach der Umsetzung von konkreten IT-Sicherheitsstandards, wie z. B. dem Branchenspezifischen Sicherheitsstandard B3S gefragt.

Welche IT-spezifischen Sicherheitsstandards werden innerhalb Ihrer Einrichtung umgesetzt? (Krankenhäuser in %)

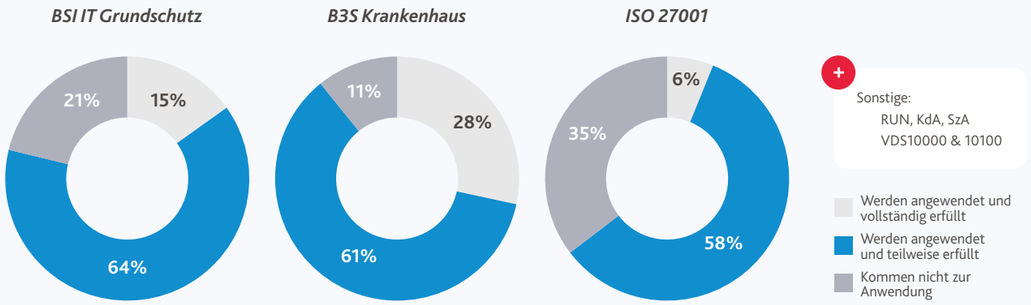


Abbildung: 1 Anwendung IT-spezifischer Sicherheitsstandards

Die meisten Krankenhäuser in Deutschland setzen mehrere IT-spezifische Sicherheitsstandards um. In jeweils rund 60 % der Einrichtungen werden der BSI IT-Grundschutz, der B3S Krankenhaus und die ISO 27001 angewendet und teilweise erfüllt. 28 % der Krankenhäuser erfüllen den B3S und 15 % den BSI IT-Grundschutz vollständig, während die ISO 27001 seltener vollständig umgesetzt ist (6 %) (vgl. Abbildung: 1).

25 % der befragten Einrichtungen gaben an, dass sie als Betreiber Kritischer Infrastrukturen (KRITIS) im Sinne der BSI-KRITIS-VO (mindestens 30.000 vollstationäre Fälle/Jahr) beim Bundesamt für Sicherheit in der Informationstechnik registriert sind (Daten nicht dargestellt).

Haben Sie bereits eine NIS-2 Betroffenheitsanalyse hinsichtlich der NIS-2-Richtlinie („Network and Information Security (NIS) Directive") durchgeführt? (Krankenhäuser in %)

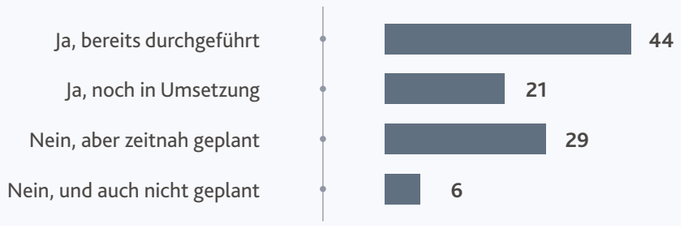


Abbildung: 2 Durchführung einer NIS-2 Betroffenheitsanalyse

Die NIS-2-Richtlinie (NIS, Network and Information Security) ist ein EU-Regelwerk zur Stärkung der Cybersicherheit und zum Schutz kritischer Infrastrukturen durch verschärfte Sicherheitsanforderungen und ein verbessertes Management bei Vorfällen. Die Umsetzung erfolgt in Deutschland durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), welches sich aktuell noch im Gesetzgebungsverfahren befindet. NIS-2 ersetzt die aktuelle erste NIS-Richtlinie und erweitert Cybersecurity-Pflichten für Gesundheitseinrichtungen.

Eine NIS-2 Betroffenheitsanalyse hinsichtlich der NIS-2-Richtlinie haben bereits 44 % der Krankenhäuser durchgeführt. Bei weiteren 21 % der Befragten ist sie noch in Umsetzung und in 29 % der Häuser zeitnah geplant (vgl. Abbildung: 2).

Welche IT-spezifischen Sicherheitsstandards werden innerhalb Ihrer Einrichtung umgesetzt? (Krankenhäuser in %)

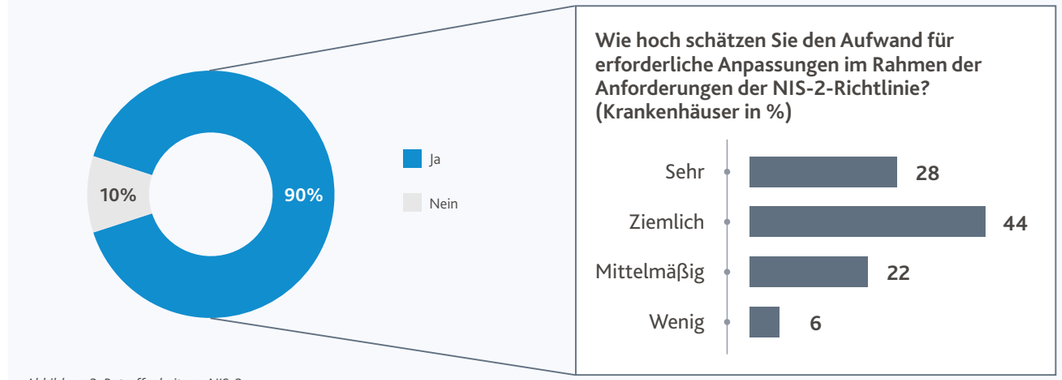


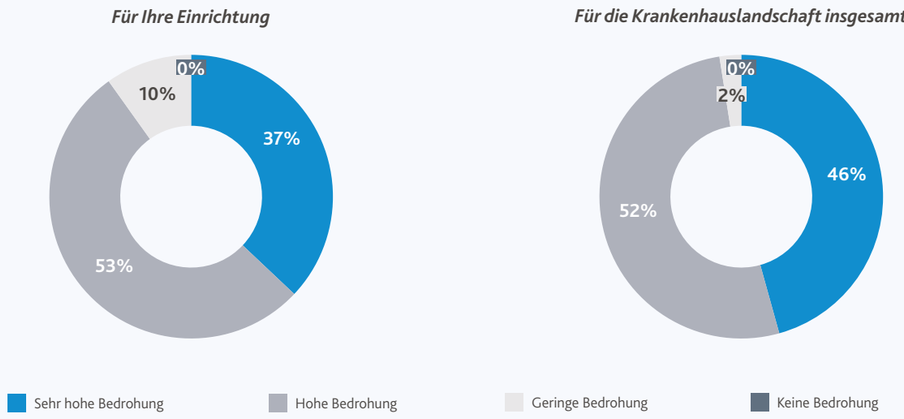
Abbildung 3: Betroffenheit von NIS-2

Nach aktuellem Kenntnisstand werden etwa 90 % der Allgemeinkrankenhäuser ab 100 Betten unter die NIS-2-Richtlinie fallen. Den Aufwand für erforderliche Anpassungen im Rahmen der Anforderungen der NIS-2-Richtlinie schätzen 28 % der Häuser als sehr hoch und 44 % als ziemlich hoch ein.

Bedrohungslage Cyberkriminalität

Einschätzung zur Bedrohungslage

Wie schätzen Sie die Bedrohung durch Cyberkriminalität aktuell ein? (Krankenhäuser in %)



Wie wird sich die Bedrohungslage durch Cyberkriminalität Ihrer Einschätzung nach in den nächsten 2 Jahren für Ihre Einrichtung entwickeln? (Krankenhäuser in %)

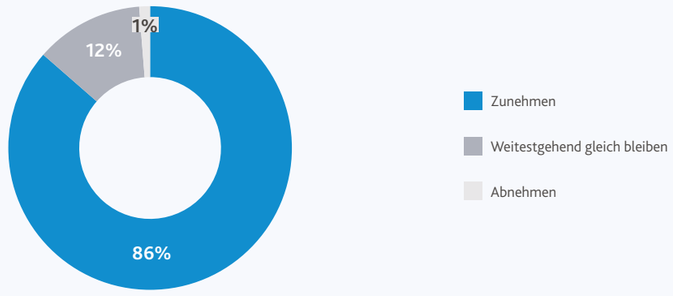


Abbildung: 2 Durchführung einer NIS-2 Betroffenheitsanalyse

Die Krankenhäuser in Deutschland sind sich ihrer Bedrohungslage durch Cyberkriminalität bewusst. Für ihre Einrichtung schätzen 90 % der Befragten die Bedrohung durch Cyberkriminalität als sehr hoch (37 %) oder hoch ein (53 %). 10 % der Häuser sehen nur eine geringe Bedrohung. Kein Stichprobenkrankenhaus gab an, nicht bedroht zu sein.

Mit Blick auf die Krankenhauslandschaft insgesamt fällt die Bedrohungslage noch kritischer aus. 98 % der Krankenhäuser gehen hier von einer hohen (52 %) bis sehr hohen Bedrohung aus (46 %) (vgl. Abbildung 4).

Kleinere Krankenhäuser unter 300 Betten sehen sich durch Cyberkriminalität tendenziell etwas weniger bedroht als größere Häuser (Ergebnisse nicht dargestellt).

Die Bedrohungslage dürfte sich, den Befragten zufolge, zukünftig noch verschärfen. 86 % der Befragten gehen für ihr Krankenhaus von einer zunehmenden Bedrohungslage aus. Kaum ein Haus erwartet eine abnehmende Bedrohung.

Betroffenheit

War Ihre Einrichtung in den letzten 3 Jahren von Cyberkriminalität (meldepflichtige Vorfälle: Cyberangriffe, Störungen der kritischen Infrastruktur, Datenpannen) betroffen? (Krankenhäuser in %)

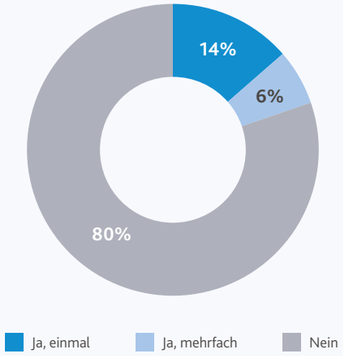


Abbildung 5: Betroffenheit von Cyberkriminalität

20 % der Allgemeinkrankenhäuser ab 100 Betten sind in den letzten 3 Jahren von Cyberkriminalität betroffen gewesen, konkret von meldepflichtigen Vorfällen wie Cyberangriffen, Störungen der kritischen Infrastruktur und Datenpannen. 14 % der Häuser sind einmal und 6 % mehrfach Opfer von Cyberkriminalität geworden. Kleinere Häuser unter 300 Betten sind davon weniger betroffen. Während hier rund 10 % Cyberkriminalität erfahren haben, waren es in den größeren Häusern rund 30 %.

Wie lange liegt der letzte Angriff auf die IT-Sicherheit in Ihrer Einrichtung zurück? (Krankenhäuser, die von Cyberkriminalität betroffen waren in %)

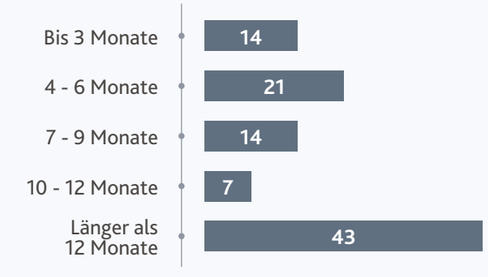


Abbildung 6: Zeitpunkt des Cyberangriffs

Bei 57 % der Befragten, die in den letzten 3 Jahren von Cyberkriminalität betroffen waren, erfolgte der letzte Angriff auf die IT-Sicherheit ihrer Einrichtung in den 12 Monaten vor Durchführung der Befragung. Die Aufteilung auf die verschiedenen Monatsintervalle kann im Einzelnen Abbildung 6 entnommen werden. Die Ergebnisse legen insofern eine beträchtliche Zunahme der Angriffe im Betrachtungszeitraum nahe.

Inwieweit war Ihr Krankenhausbetrieb nach dem letzten Angriff beeinträchtigt?(Krankenhäuser, die von Cyberkriminalität betroffen waren, in %)

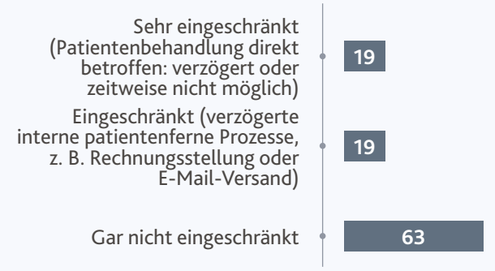


Abbildung 7: Beeinträchtigung des Krankenhausbetriebs durch Cyberangriffe

In der Mehrzahl der betroffenen Krankenhäuser (63 %) hat der letzte Angriff auf die IT-Sicherheit den Krankenhausbetrieb nicht beeinträchtigt. In 19 % der Fälle war der Betrieb sehr eingeschränkt. Hier war die Patientenbehandlung direkt betroffen; das heißt, sie erfolgte verzögert oder war zeitweise nicht möglich. Bei weiteren 19 % der Fälle war der Krankenhausbetrieb bei internen patientenfernen Prozessen eingeschränkt, zum Beispiel bei der Rechnungsstellung oder dem E-Mail-Versand.

Zur Dauer der Einschränkungen des Krankenhausbetriebes haben nur sehr wenige Befragungsteilnehmer Angaben gemacht. Von daher sind die Ergebnisse kaum generalisierbar. In der Stichprobe variierten die Einschränkungen zwischen 6 Stunden (Minimum) und 80 Tagen (Maximum). Der Median der Verteilung lag bei 5 Tagen.

Zu welcher IT-spezifischen Bedrohung ist es in Ihrer Einrichtung gekommen? (Mehrfachauswahl möglich) (Krankenhäuser, die von Cyberkriminalität betroffen waren, in %)

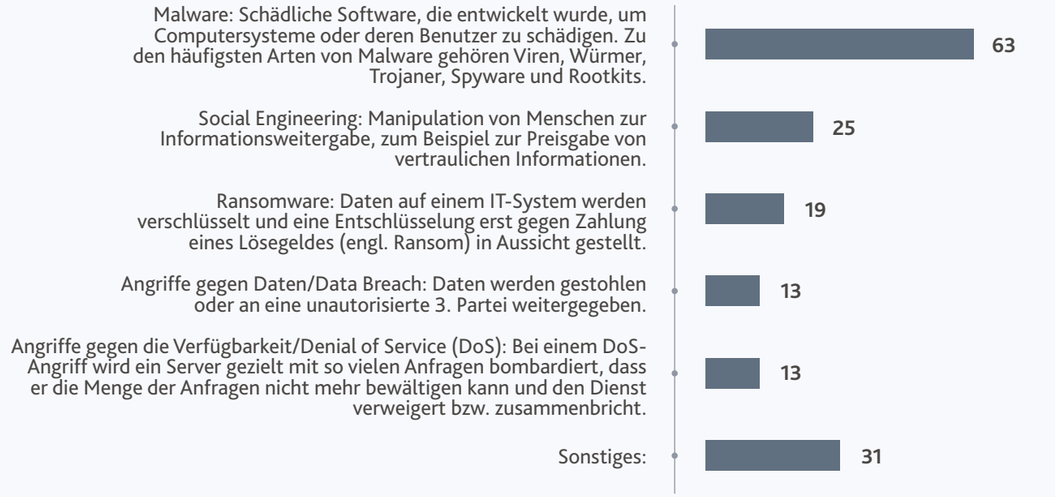


Abbildung 8: Vorkommen IT-spezifischer Bedrohung

In den von Cyberkriminalität betroffenen Krankenhäusern stellt Malware die am häufigsten vorkommende IT-spezifische Bedrohung dar. 63 % dieser Krankenhäuser berichten von entsprechenden Angriffen durch eine schädliche Software, die entwickelt wurde, um Computer zu schädigen, etwa durch Viren oder Trojaner. Ebenfalls stärker verbreitet sind Social Engineering zur Manipulation von Menschen zur Informationsweitergabe (31 %) und Angriffe gegen die Verfügbarkeit/Denial of Service (25 %). Weniger verbreitet sind Ransomware und Data Breach.

Über die Betroffenheit der eigenen Einrichtung hinaus wurden die Krankenhäuser gefragt, ob Dienstleister oder Zulieferer in der Lieferkette von Cyberkriminalität betroffen waren, zum Beispiel durch Cyberangriffe, Störungen der kritischen Infrastruktur oder Datenpannen. Dies war in den letzten 3 Jahren in etwa jedem 2. Krankenhaus der Fall. Im Rahmen einer offenen Frage wurden hier insbesondere KIS-Hersteller, IT-Dienstleister, Medizingeräte- und Medizinproduktehersteller genannt.

Waren Dienstleister/Zulieferer im Rahmen Ihrer Lieferkette in den letzten 3 Jahren von Cyberkriminalität (z. B. Cyberangriffe, Störungen der kritischen Infrastruktur, Datenpannen) betroffen? Wenn ja, welcher Servicebereich oder Dienstleister (z. B. IT-Dienstleister)? (Krankenhäuser in %)

Abbildung 9: Betroffenheit von Dienstleistern und Zulieferern

Die Krankenhäuser wurden gebeten einzuschätzen, welche Technik und Software nach Kapitel 4.4. des branchenspezifischen Sicherheitsstandards B3S besonders schützenswert sind (vgl. Abbildung 10). Mit Abstand am häufigsten wird hier das Krankenhausinformationssystem (KIS) genannt. 94 % der Befragten betrachten es als sehr schützenswert und 6 % als ziemlich schützenswert. Aufgrund der zentralen Bedeutung eines KIS für die Krankenhausprozesse fällt das Ergebnis erwartungsgemäß aus. Im KIS laufen wichtige Informationen in unterschiedlichen Datenformaten (z. B. Diagnosen, Röntgenbilder, Medikationspläne und Labordaten) mit entsprechenden (unterschiedlichen) Schnittstellen, wie z. B. HL7, DICOM oder FHIR, zusammen. In leichter Abstufung folgen das Picture Archive and Communication System (PACS), das Laborinformationssystem (LIS) und das Radiologieinformationssystem (RIS). Am unteren Ende der Rangfolge stehen Tertiärbereiche wie Versorgungstechnik und Versorgungsdienste oder die Transportlogistik.

Wie schützenswert schätzen Sie branchenspezifische Technik und Software nach Kapitel 4.4 des branchenspezifischen Sicherheitsstandards B3S Krankenhaus ein?(Krankenhäuser in %)

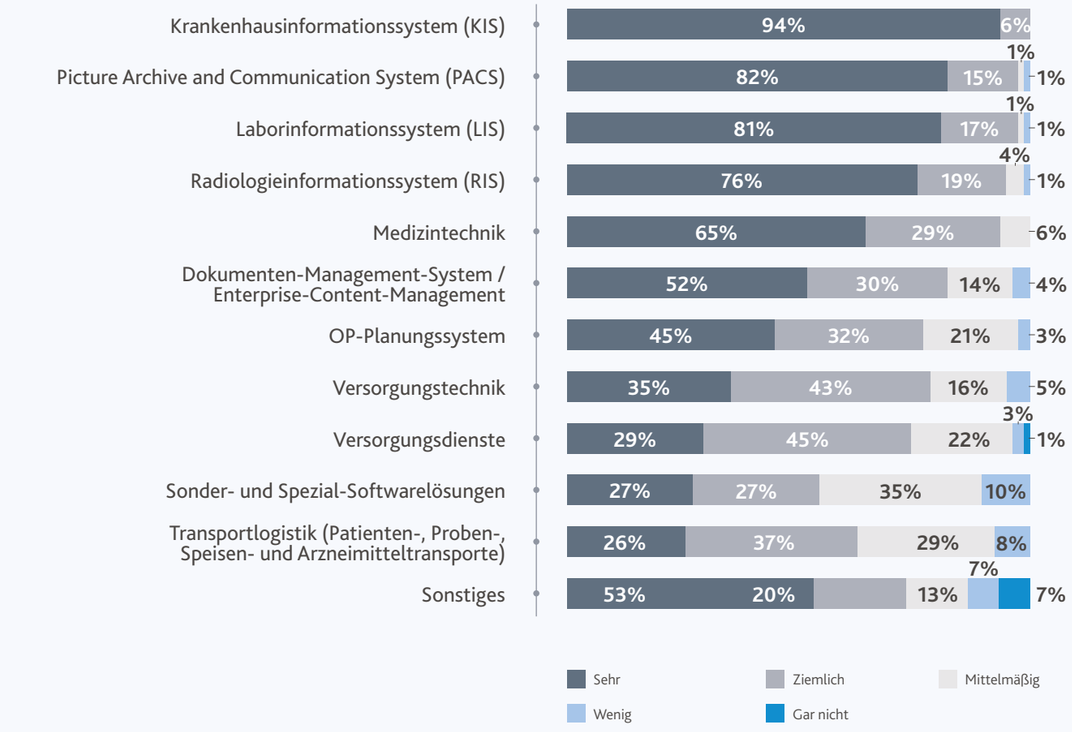


Abbildung 10: Einschätzung zum besonderen Schutz von Technik und Software

Maßnahmen der IT-Sicherheit

Technisch

Die Krankenhäuser in Deutschland setzen in hohem Maße auf technische Schutzmaßnahmen zur IT-Sicherheit (vgl. Abbildung 11 und Abbildung 12). Nahezu flächendeckend eingeführt sind Basislösungen wie Antivirensoftware (99 %) und Firewalls (97 %). Auch zentrale E-Mail-Scans gegen Malware und Phishing (92 %) sowie sichere Remote-Zugänge über VPN oder VDI (92 %) gehören inzwischen zum Standard. Sehr verbreitet sind zudem getrennte Backups (84 %) und Endpoint Detection & Response-Systeme (81 %) zur kontinuierlichen Überwachung von Endgeräten, um Cyberbedrohungen zu erkennen, zu analysieren und darauf zu reagieren.

Welche technischen Maßnahmen zum Schutz ihrer IT-Sicherheit haben Sie bereits eingeführt oder planen diese? (Krankenhäuser in %)

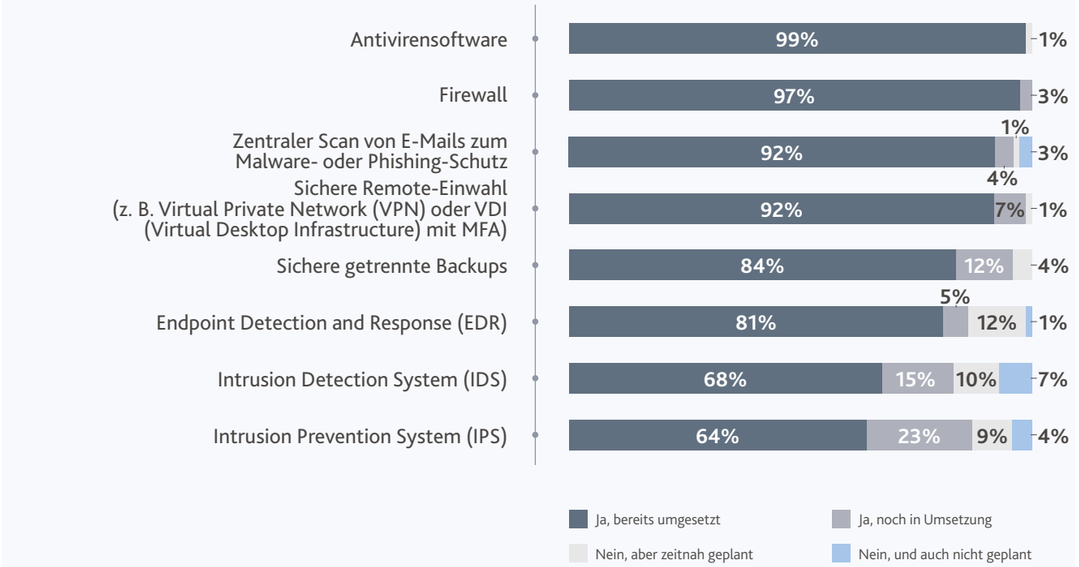


Abbildung 11: Technische Maßnahmen der IT-Sicherheit (Teil 1)

Etwas zurückhaltender ist der Einsatz bei Intrusion Detection Systemen zur frühzeitigen Erkennung von Sicherheitsrisiken und -bedrohungen (68 % bereits umgesetzt), wobei weitere 15 % aktuell noch in der Umsetzung sind. Ähnlich verhält es sich mit Intrusion Prevention Systemen: 64 % der Häuser haben diese eingeführt, während sie sich zusätzlich bei 23 % im Aufbau befinden. Noch komplexere Netzwerksegmentierungen mit Network Access Control (NAC) setzen 53 % der Häuser ein, weitere 29 % arbeiten derzeit an der Umsetzung.

Im mittleren Bereich bewegen sich Maßnahmen wie Multi-Faktor-Authentifizierung (52 % umgesetzt, 32 % in Umsetzung), die Verschlüsselung mobiler Speichermedien (46 % umgesetzt, 31 % in Umsetzung) oder der Aufbau von Incident-Response-Teams (44 % umgesetzt, 20 % in Umsetzung). Relativ gering ist bislang die Verbreitung von SIEM- und SOC-Lösungen zur Datensammlung und -aggregation sowie deren Analyse (42 % umgesetzt, 26 % in Umsetzung) und zentrale Logserver (42 % umgesetzt, 27 % in Umsetzung).

Im Vergleich ausbaufähig erscheinen Maßnahmen wie E-Mail-Verschlüsselung mittels S/MIME oder PGP (24 % umgesetzt, 41 % in Umsetzung) und Notfallkommunikation über Funk- oder Satellitentechnik (25 % umgesetzt, 12 % in Umsetzung).

Welche technischen Maßnahmen zum Schutz ihrer IT-Sicherheit haben Sie bereits eingeführt oder planen diese? (Krankenhäuser in %)

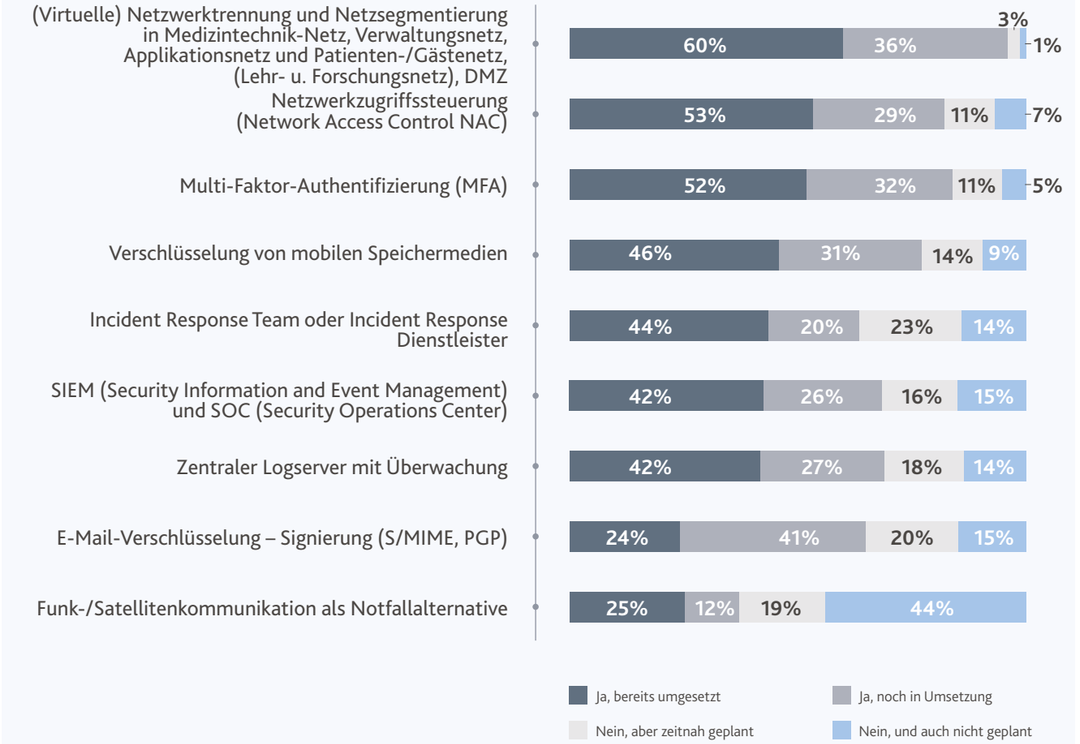


Abbildung 12: Technische Maßnahmen der IT-Sicherheit (Teil 2)

Organisatorisch

Neben den technischen Vorkehrungen haben auch organisatorische Maßnahmen eine hohe Bedeutung für die IT-Sicherheit der Krankenhäuser. Besonders stark verbreitet sind Schulungen zu Datenschutz und Informationssicherheit, die bereits in 72 % der Einrichtungen durchgeführt werden. Weitere 25 % der Häuser befinden sich hier in der Umsetzung, sodass Schulungen in absehbarer Zeit nahezu flächendeckend etabliert sein dürften. Ebenfalls weit fortgeschritten sind Patch- und Änderungsmanagement (58 % umgesetzt, 28 % in Umsetzung) zur Schließung von Sicherheitslücken sowie Richtlinien zur Nutzung eigener Geräte (BYOD) mit 51 %. Physische Zugangskontrollen, etwa durch elektronische Ausweissysteme, sind bei jedem 2. Krankenhaus im Einsatz und bei 25 % derzeit in Planung.

Welche organisatorischen Maßnahmen zum Schutz ihrer IT-Sicherheit haben Sie bereits eingeführt oder sind geplant? (Krankenhäuser in %)

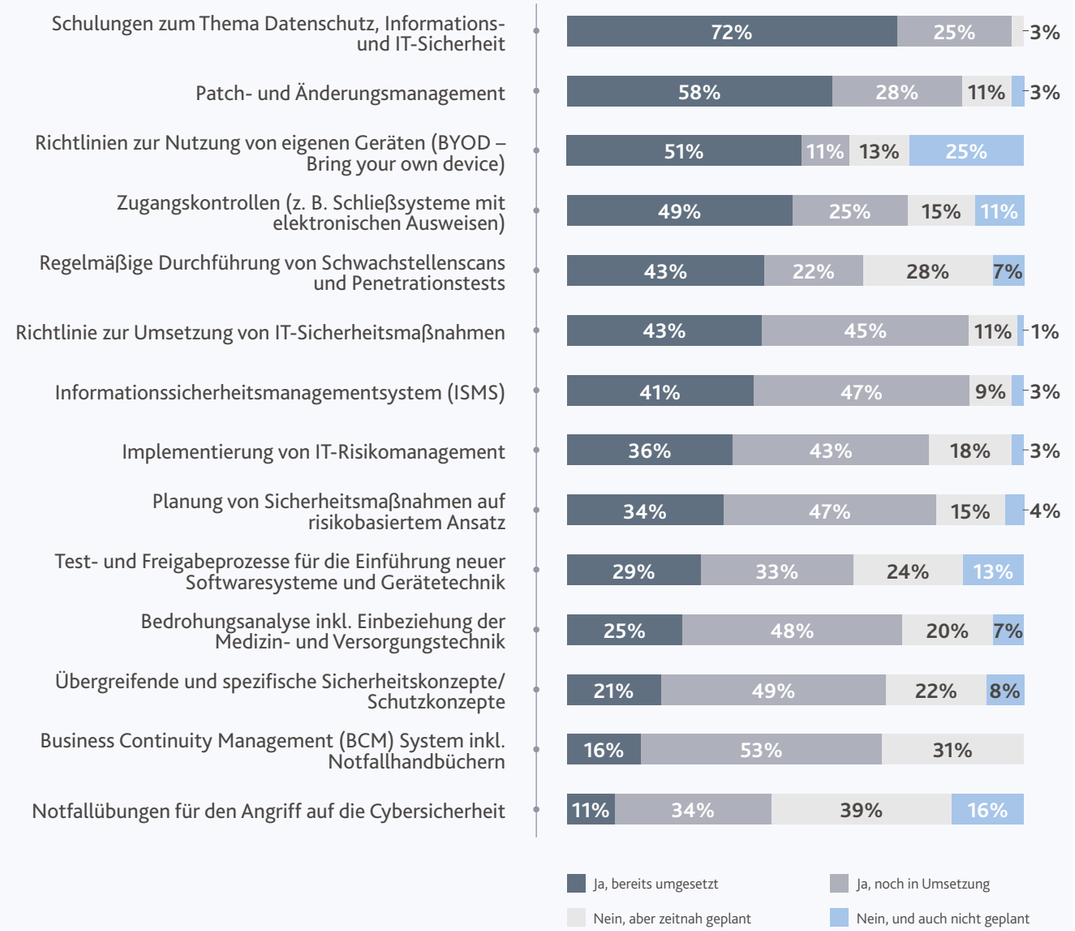


Abbildung 13: Organisatorische Maßnahmen zum Schutz der IT-Sicherheit

Deutlich heterogener ist das Bild bei systematischeren Ansätzen: So setzen bislang nur 43 % der Krankenhäuser regelmäßige Schwachstellenscans und Penetrationstests um, ebenso viele verfügen über eine formale Richtlinie zur Umsetzung von Sicherheitsmaßnahmen.

Rund ein Drittel der befragten Einrichtungen setzen ein strukturiertes IT-Risikomanagement (36 %) sowie Planungen auf Basis eines risikoorientierten Ansatzes (34 %) um. Nachholbedarf zeigt sich bei übergreifenden Sicherheitskonzepten (21 %) sowie beim Business Continuity Management (BCM) (16 %). Allerdings befindet sich ein BCM-System bei 53 % derzeit bereits in Umsetzung. Notfallübungen für Cyberangriffe werden bislang lediglich in 11 % der Häuser praktiziert.

Ein Informationssicherheitsmanagementsystem (ISMS) ist bei 41 % der Krankenhäuser etabliert. Unter den befragten Einrichtungen mit ISMS befindet sich dies in 39 % der Fälle im Reifegrad 3 (Das ISMS ist etabliert). Nur 6 % können ein ISMS mit dem höchsten Reifegrad 5 (Das ISMS wird kontinuierlich verbessert) aufweisen (vgl. Abbildung 14).

Falls ein ISMS zur Anwendung kommt: Wie würden Sie den Reifegrad Ihres Informationssicherheitsmanagementsystems (ISMS) gemäß der Reifegradbestimmung des BSI („Reife- und Umsetzungsgradbewertung im Rahmen der Nachweisprüfung (RUN)“) einschätzen? (Krankenhäuser mit ISMS in %)

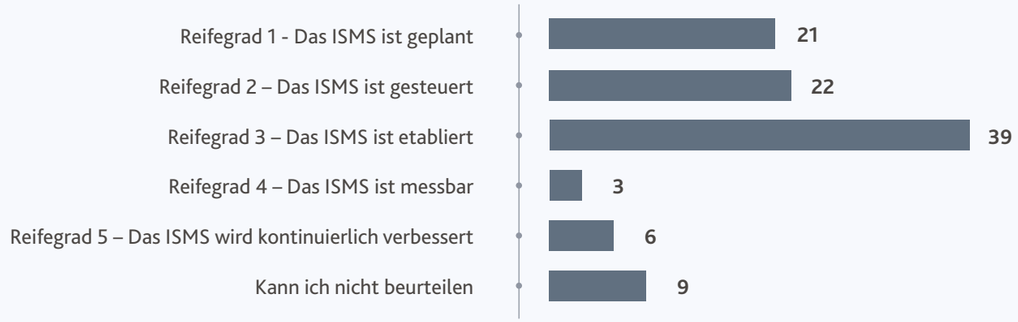


Abbildung 14: Reifegrad des Informationssicherheitsmanagementsystems

Herausforderungen

Inwieweit behindern die folgenden Faktoren Sie bei der Einführung von IT-Sicherheitsmaßnahmen? (Krankenhäuser in %)

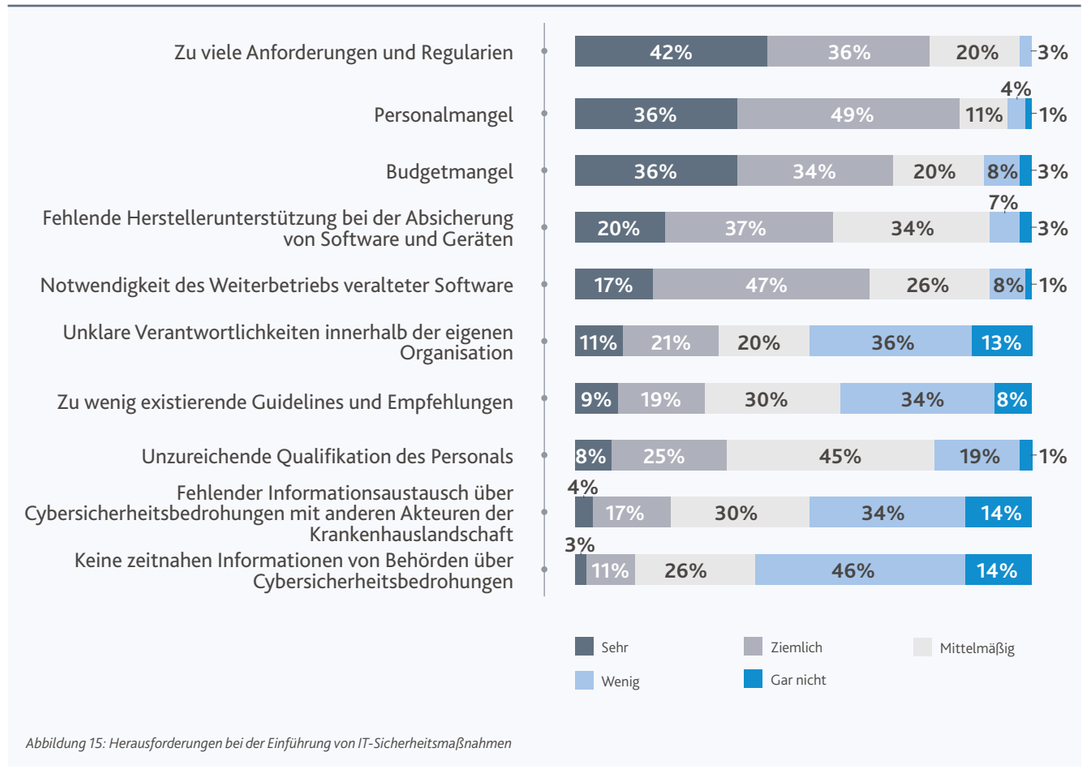


Abbildung 15: Herausforderungen bei der Einführung von IT-Sicherheitsmaßnahmen

Im Kontext der IT-Sicherheit werden zu viele Anforderungen und Regularien durch die Krankenhäuser als besonders herausfordernd wahrgenommen. 42 % behindert dieser Faktor sehr bei der Einführung von IT-Sicherheitsmaßnahmen. 85 % bzw. 70 % nehmen zudem den Personal- und Budgetmangel als ziemlich oder sehr behindernd wahr.

Verzögerte Informationen von Behörden über Cybersicherheitsbedrohungen scheinen hingehen kein großes Problem darzustellen. Ebenso wenig eine unzureichende Qualifikation des Personals.

Organisation der IT-Sicherheit im Krankenhaus

Organisatorisch ist das Thema IT-Sicherheit in den beiden Bereichen Geschäftsführung und IT-Abteilung aufgehängt. Erwartungsgemäß unterscheiden sich jedoch operative und strategische Verantwortlichkeiten. 95 % der befragten Einrichtungen gaben an, dass die operative Verantwortung der IT-Sicherheit der IT-Abteilung obliegt. In 25 % der befragten Einrichtungen werden Fragen der IT-Sicherheit operativ in einer eigenständigen Abteilung für IT-Sicherheit entschieden. Bei 14 % sind die Geschäftsführungen an operativen Entscheidungen beteiligt.

Strategische Entscheidungen sind in den meisten Krankenhäusern bei der Geschäftsführung angesiedelt (85 %), jedoch auch sehr häufig bei der IT-Abteilung (69 %). Ebenso ist die Compliance-Abteilung beteiligt (16 %). Als sonstige beteiligte Personen und Abteilungen wurden Datenschutzbeauftragte, IT-Sicherheitsbeauftragte oder ein Informationssicherheitsmanagementteam genannt.

In welchem Personalbereich sind Entscheidungen zu Fragen der IT-Sicherheit angesiedelt? (Mehrfachauswahl möglich) (Krankenhäuser in %)

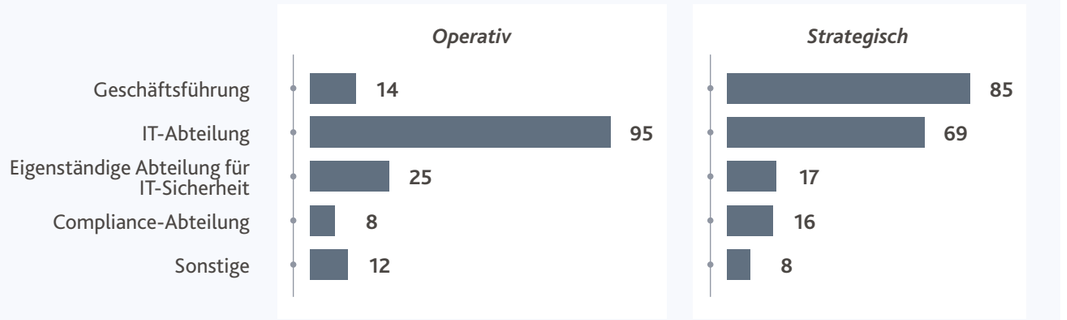


Abbildung 16: Personalbereich IT-Sicherheit

Rund ein Drittel der Krankenhäuser weist unbesetzte Stellen im Bereich der IT-Sicherheit auf. Durchschnittlich sind in diesem Tätigkeitsfeld 1,6 Stellen unbesetzt. Bei Krankenhäusern, die hierzu Angaben gemacht haben, variierte die Zahl zwischen 1 und 5 Stellen. 41 % der Krankenhäuser planen in den nächsten 2 Jahren eine Aufstockung des Personals im Bereich der IT-Sicherheit (vgl. Abbildung 17).

Sind in Ihrem Krankenhaus Stellen im Tätigkeitsfeld der IT-Sicherheit derzeit unbesetzt? (Krankenhäuser in %)

Planen Sie innerhalb der nächsten 2 Jahre eine Veränderung im Personalbestand im Bereich IT-Sicherheit?(Krankenhäuser in %)

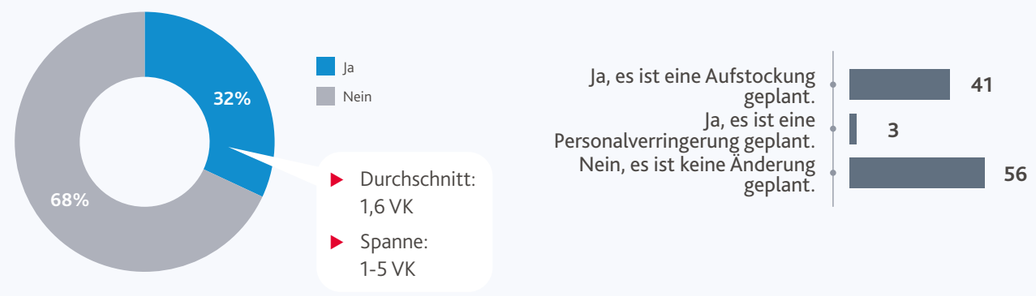


Abbildung 17: Stellenbesetzung in der IT-Sicherheit

Das Budget für IT-Sicherheit als Anteil am gesamten IT-Investitionsbudget lag 2024 durchschnittlich bei 16 %. Die Spanne der Angaben der Krankenhäuser war allerdings sehr breit und lag zwischen 1 und 50 % (Daten nicht dargestellt).

Sensibilisierung von Mitarbeiterinnen und Mitarbeitern

Neben technischen und organisatorischen Maßnahmen der IT-Sicherheit ist es wichtig, Maßnahmen zur Steigerung der Security-Awareness von Mitarbeiterinnen und Mitarbeitern in den Fokus zu rücken. Schulungen zur Informationssicherheit für alle Mitarbeiterinnen und Mitarbeiter oder auch Phishing-Simulationen können die Awareness erhöhen. Es ist von großer Bedeutung, dass die Beschäftigten die aktuellen Bedrohungen kennen und wissen, wie sie sich in konkreten Fällen verhalten und davor schützen können. Daher wurden die Krankenhäuser gefragt, wie Mitarbeiterinnen und Mitarbeiter für das Thema IT-Sicherheit sensibilisiert werden (vgl. Abbildung 18).

Einweisungen des Personals in den sicheren Umgang mit IT wird bei den allermeisten Krankenhäusern umgesetzt (84 %). 75 % führen Schulungen zu IT-Sicherheitsrisiken durch. Rund jede 2. befragte Einrichtung führt Kampagnen zur IT-Sicherheit durch. Phishing-Simulationen sind jedoch nur bei 32 % vertreten. Notfallübungen führen 23 % durch. Als sonstige Ansätze wurde z. B. Verbandsarbeit und Hersteller-Veranstaltungen genannt.

Wie werden Mitarbeiterinnen und Mitarbeiter in Ihrem Krankenhaus für das Thema IT-Sicherheit sensibilisiert? (Krankenhäuser in %, Mehrfachauswahl möglich)

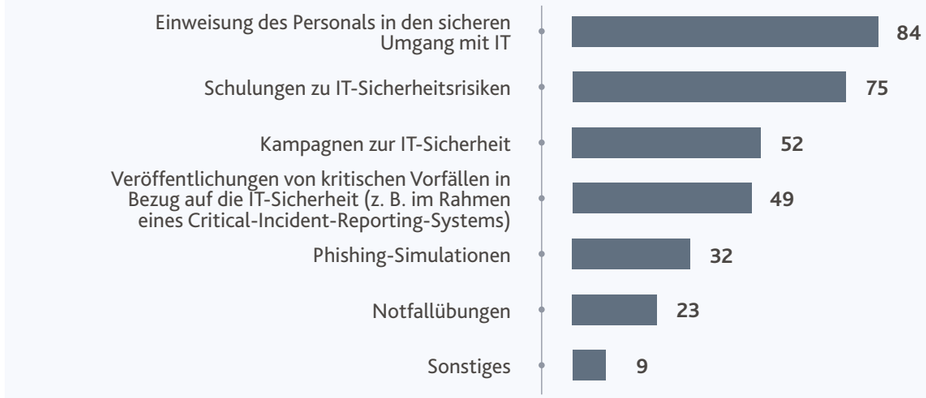


Abbildung 18: Sensibilisierung von Mitarbeiterinnen und Mitarbeitern für das Thema IT-Sicherheit

Autorinnen und Autoren

Prof. Dr. Volker Penter

Wirtschaftsprüfer, Steuerberater, Partner,
Advisory, Gesundheitswirtschaft
BDO AG Wirtschaftsprüfungsgesellschaft

Tel.: +49 351 8669 131
volker.penter@bdo.de

Tobias Kasch

Senior Manager
Cyber Incident Response and Crisis Center
BDO AG Wirtschaftsprüfungsgesellschaft

Tel.: +49 351 26352 174
tobias.kasch@bdosecurity.de

Dr. Karl Blum

Vorstand, Deutsches
Krankenhausinstitut e.V.
Leiter Geschäftsbereich Forschung

Tel.: +49 211 470 51 17
karl.blum@dki.de

Dr. Anna Levsen

Senior Research Manager
Geschäftsbereich Forschung
Deutsches Krankenhausinstitut e.V.

Tel.: +49 211 47051 14
anna.levsen@dki.de

BDO AG Wirtschaftsprüfungsgesellschaft

Weitere Informationen zum BDO Netzwerk finden Sie unter
www.bdo.de