HealthCare Magazin

Für Krisen gewappnet

Resilienz im Gesundheitswesen

The better the question.
The better the answer.
The better the world works.

EY

Shape the future with confidence

3.000

Blutkonserven pro Tag

Im Fall eines Bundeswehreinsatzes an der NATO-Ostfront gehen Expert:innen von bis zu 1.000 Verletzten pro Tag aus. Dies könnte den täglichen Bedarf an Blutkonserven um mehr als 3.000 Einheiten erhöhen. Wie belastbar unsere Versorgungsstrukturen wären, lesen Sie **ab Seite 30.**

4.875 Cybervorfälle

Fast 5.000 dokumentierte Cybervorfälle in Europa binnen eines Jahres zeigen: Cyberangriffe sind längst Realität. Warum Cyberresilienz zur kritischen Ressource für das Gesundheitswesen wird und wie KI die Angreifer- wie auch die Verteidigerseite stärkt, lesen Sie **ab Seite 20.**

Krankenhausbetten im Parkhaus

Innerhalb weniger Stunden kann das israelische Tel Aviv Sourasky Medical Center (Ichilov) rund 800 Krankenhausbetten in sein Parkhaus verfrachten. Was Krankenhäuser von solchen Resilienzkonzepten lernen können und wie die Versorgung auch bei Extremereignissen gewährleistet bleibt, lesen Sie **ab Seite 44.**

Fast 4 von 5

Erwachsenen

nahmen 2023 allgemeinärztliche Leistungen in Anspruch. Der ambulante Sektor ist damit einer der wichtigsten Kontaktpunkte des Gesundheitswesens. Welche Rolle er für die Resilienz und die Stabilität der Versorgung spielt, lesen Sie ab Seite 55.

Fotos: Adobestock, Foto Cover: Gettyimages, Jaromir

Fotos: Adobestock

Liebe Leserinnen, liebe Leser,

rund 16.000 hitzebedingte Todesfälle verzeichnete das Robert Koch-Institut allein bis Mitte August 2026 in Deutschland. Cyberangriffe auf Kliniken und Kostenträger häufen sich, Arzneimittel-Lieferketten bleiben fragil und Naturkatastrophen werden immer mehr von der Ausnahme zur Regel. So unterschiedlich diese Ereignisse sind, sie haben eines gemeinsam: Sie stellen das Gesundheitswesen vor die Frage, ob es auch unter Belastung handlungs- und leistungsfähig bleibt.

Genau hier setzt Resilienz an und ist damit längst nicht nur ein Thema für Krisenstäbe und Katastrophenschutz. Sie entscheidet darüber, ob eine Notaufnahme bei einem Massenanfall von Verletzten die Versorgung aufrechterhalten kann, ob kritische Arzneimittel auch bei Lieferengpässen verfügbar bleiben und ob Kliniken nach einem Cyberangriff weiter behandeln können. Dabei geht es nicht nur um die Bewältigung akuter Krisen, sondern ebenso um die Fähigkeit, Versorgungsrisiken früh zu erkennen, Kapazitäten vorausseh end zu planen und aus vergangenen Erfahrungen zu lernen.

Diese Ausgabe des HealthCare Magazins beleuchtet das Thema Resilienz aus unterschiedlichsten Blickwinkeln. Wie gut ist unser Gesundheitssystem auf die nächste Krise vorbereitet? Mit einer Szenariomodellierung gehen wir dieser Frage nach und zeigen, wo das deutsche Gesundheitswesen im Falle eines NATO-Einsatzes voraussichtlich zuerst an Grenzen stoßen würde und warum die entscheidenden Engpässe häufig nicht dort entstehen, wo man sie zunächst vermutet. Wer beispielsweise ausschließlich auf Krankenhausbetten blickt, übersieht schnell, dass die Belastungsproben eines Gesundheitssystems oft auch an ganz anderer Stelle sichtbar werden. Wir beleuchten außerdem, wie Krankenhäuser auch in Krisen handlungsfähig bleiben können und welche Voraussetzungen geschaffen werden müssen, um die Versorgung unter außergewöhnlichen Bedingungen aufrechtzuerhalten. Zudem richten wir den Blick auf eine der wichtigsten Ressourcen des Gesundheitswesens: das Personal. Denn nachhaltige Versorgung gelingt nur dann, wenn auch die Menschen hinter den Systemen langfristig belastbar bleiben. Die Resilienz der Beschäftigten wird damit zu einem entscheidenden Faktor für die Zukunftsfähigkeit des gesamten Gesundheitswesens.

Gemeinsam zeichnen die Beiträge das Bild eines Gesundheitswesens, dessen Widerstandsfähigkeit weit vor dem eigentlichen Krisenfall beginnt. Resilienz ist keine Maßnahme für den Ausnahmefall, sondern eine strategische Voraussetzung für ein zukunftsfähiges Gesundheitswesen.

Ich wünsche Ihnen eine inspirierende Lektüre.

Mit besten Grüßen

Christian Egle
Leiter Gesundheitswesen Europa West, EY

14 Digitale Souveränität ist für Kliniken und Krankenkassen mittlerweile eine strategische Frage der Kontrolle über IT, Daten und Modelle. Ein Großteil der Gesundheits-IT gilt als eigenständig gestaltbar, wenn Anbieterwahl und Datenarchitektur von Anfang an mitgedacht werden.

27 Fast eine Milliarde Nachrichten wurden seit 2021 über den Kommunikationsdienst der Telematik-Infrastruktur verschickt. Trotzdem gilt diese als störanfällig. Mit dem Zero-Trust-Ansatz der zweiten Generation löst sich die gematik von zentralen Netzen und Konnektoren – für mehr Resilienz im Gesundheitswesen.

36 Ein Krankenhaus kann medizinisch exzellent sein und trotzdem im Ernstfall versagen, wenn die Bausubstanz der Krise nicht standhält. Resilienz wird damit zu einer weiteren Planungsgröße neben Medizin und Wirtschaftlichkeit.

HealthCare Magazin

Ausgabe 2026 | 2

03 Vorwort

72 Ansprechpartner:innen

74 Impressum

06 In der Krise navigieren
Wie das Gesundheitswesen steuerungsfähig bleibt

12 Wenn Gesundheit zur Zielscheibe wird
Hybride Angriffe gefährden Versorgung und Sicherheit

14 Wer hat die Kontrolle über Ihre IT?
Die entscheidende Frage hinter digitaler Souveränität

20 KI gegen KI
Wie sich Angriff und Abwehr verändern

27 Von sicheren Netzen zum sicheren Zugriff
Zero Trust stärkt die digitale Resilienz

30 Vom Planwert zur Planungsgröße
Krisenresilienz strukturieren und quantifizieren

34 Einsatzbereit in Extremlagen
Koordination und Vorbereitung erhöhen die Resilienz

36 Krisenfeste Krankenhäuser
Versorgungssicherheit ist auch Bauaufgabe

Fotos: Adobestock/Gettyimages

44 Krankenhaus unter Beschuss
Was ein israelischer Maximalversorger über Versorgung in der Krise lehrt

48 Vertrauen Sie niemandem!
Warum Nachhaken gesünder ist

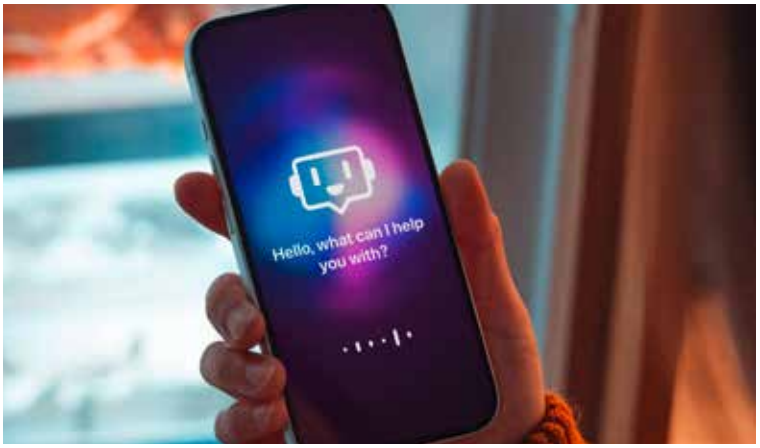
50 Improvisation reicht nicht
Pflege braucht verbindliche Krisenstrukturen

55 Resilienz kennt keine Sektorengrenzen
Der ambulante Sektor als Puffer im Versorgungssystem

61 Krankenkassen als vergessene Resilienzakteure
Nicht in der Akutlage, sondern in der Stabilisierung liegt ihre Stärke

64 Handlungsfähig unter permanentem Druck
Fünf Hebel für resiliente Krankenhausorganisationen

70 Zwischen Zeitdruck und Empathie
Emotionale Intelligenz verbessert Zusammenarbeit und Führung



48 Wer heute gesundheitlichen Rat im Internet sucht, trifft zunehmend auf Bots und Medfluencer:innen. Ob Fake-Studien, erfundene Krankheitsbilder oder gezielte Desinformation – überzeugend klingt heute fast alles. Kritisches Hinterfragen wird damit zur wichtigen Gesundheitskompetenz.

50 Stromausfälle, Hitzewellen und Evakuierungen treffen Pflegeeinrichtungen hart. Ein wesentlicher Teil der Versorgungssicherheit ist beeinflussbar, sofern Notstromversorgung, Krisenstrukturen und die Rolle der Pflegefachpersonen rechtzeitig berücksichtigt werden.

64 Wie krisenfest ein Krankenhaus ist, zeigt sich an den Menschen, die im Ernstfall improvisieren. Diese stille Leistung Einzelner trägt das deutsche Gesundheitssystem bislang mit, ohne dass sie in Strategien sichtbar wird. Personalresilienz macht daraus eine bewusste Aufgabe für Klinikvorstände.

Wie steuerbar und verfügbar sind Arzneimittel, Medizinprodukte, Blutprodukte, Laborkapazitäten, Personal, Energie, Wasser und Cloud-Infrastruktur? Gibt es alternative Handlungsoptionen durch europäische Produktions- und Beschaffungskapazitäten, klare Prioritäten im Krisenfall und belastbare Logistik?

In der Krise navigieren

Wie das Gesundheitswesen steuerungsfähig bleibt

Ob Hitze, Flut, Pandemie, Lieferengpässe, Cyberangriffe, Energiekrisen, Fluchtbewegungen und nicht zuletzt die sicherheitspolitische Lage in Europa: Das Gesundheitswesen ist durch Krisen zunehmend gefordert und wird zugleich selbst Teil kritischer Infrastruktur. Als solcher muss es gleichermaßen geschützt werden und in der Lage sein, unter Schockbelastung kontrolliert weiter zu funktionieren, Ressourcen und Personal gezielt zum Erhalt kritischer Versorgung einzusetzen, Patient:innen zu steuern und Risikogruppen zu schützen.

Auch die frühzeitige Identifikation von Abhängigkeiten gehört zur Krisenbewältigung: Wie steuerbar und verfügbar sind Arzneimittel, Medizinprodukte, Blutprodukte, Laborkapazitäten, Personal, Energie, Wasser und Cloud-Infrastruktur? Gibt es alternative Handlungsoptionen durch europäische Produktions- und Beschaffungskapazitäten, klare Prioritäten im Krisenfall und belastbare Logistik? Auch Souveränität und Cybersecurity sind Teil von Resilienz. Ein Cyberangriff auf ein Krankenhaus ist potenziell ein Versorgungsausfall. Eine Störung der digitalen Infrastruktur kann Notaufnahmen, Labore, Apotheken, Rettungsdienst, elektronische Verschreibungen und Kommunikation gleichzeitig treffen.

Aus der Pandemie hat das Gesundheitswesen gelernt, bei Krisen vor allem an Krankenhäuser, Intensivbetten und Notfallversorgung zu denken. Dabei ist das Thema deutlich größer. Arztpraxen, Pflege, Apotheken, Rettungsdienst, Reha, digitale Infrastruktur und Lieferketten sind ebenfalls elementarer Teil der Versorgungsfähigkeit. Gerade der ambulante Sektor kann in Krisen eine entscheidende Rolle übernehmen und Krankenhäuser und Notaufnahmen entlasten, etwa mit Triage, Chronikersteuerung, Frühentlassungsmanagement, Wundversorgung oder Telemedizin. Krankenkassen können mit ihren Daten helfen, vulnerable Zielgruppen zu identifizieren und Patient:innen durch Erinnerungen an Impf- und Therapietermine proaktiv zu steuern. Die pharmazeutische Industrie ist vor allem durch hohe Lieferkettenabhängigkeit verwundbar. Schätzungen von Gesundheitsbehörden zufolge stammen rund 80 bis 90 Prozent der in Europa verwendeten Wirk- beziehungsweise Grundstoffe aus Asien, vornehmlich China und Indien. Fällt dort eine zentrale Produktionsstätte oder die Lieferung über den Seeweg aus, entstehen Probleme.

Auch bei COVID ging es nicht nur um Intensivbetten, sondern auch um die Steuerung von Testlogistik und den Aufbau von Impfzentren. Außerdem mussten neue Meldewege etabliert werden. Auch der Schutz der Senior:innen in Pflegeheimen wurde neu aufgesetzt. Schutzmaterial musste beschafft, die Finanzierung und Datenflüsse sichergestellt werden. Zu Beginn des Ukrainekriegs war die medizinische Versorgung der Geflüchteten nicht nur eine Frage von Ärzt:innen und Kliniken. Menschen brauchten Zugang zum System, indem ihr Versicherungsschutz sichergestellt und elektronische Gesundheitskarten ausgegeben wurden. Viele benötigten Unterstützung bei der Übersetzung und bei der Orientierung im Gesundheitssystem sowie psychologische Versorgung.

Operating Model für den Krisenmodus gesucht

Um all diese Aufgaben und Schnittstellen wirkungsvoll zusammenzubringen, braucht es ein Operating Model für den Krisenmodus. Dazu gehören klare Rollen und Zuständigkeiten, definierte Eskalationsstufen, Entscheidungen bei Zielkonflikten, Regeln zur Priorisierung von Leistungen, Mechanismen zur Patientensteuerung, klare Kommunikation und gezielte

Fotos: Adobestock

Vorbereitung. All diese Hebel werden idealerweise nicht im Krisenfall erarbeitet, sondern vorab definiert und eingeübt.

Für den Fall der militärischen Eskalation regelt der Operationsplan Deutschland (OPLAN DEU) mögliche Schritte, seien es Cyberangriffe auf kritische Infrastruktur, Fluchtbewegungen, die Auswirkungen auf Versorgungskapazitäten haben, Anschläge auf Lieferketten oder Transportwege bis hin zu Angriffen auf Grenzen des NATO-Bündnisgebiets. Der OPLAN DEU regelt allerdings ausdrücklich nicht die Versorgung der Zivilbevölkerung – die fünf deutschen Bundeswehrkrankenhäuser wären ihrerseits im Ernstfall schnell überfordert. Genau diese Lücke soll das Gesundheitssicherstellungsgesetz (GeSiG) schließen. Ursprünglich wurde es bereits unter Karl Lauterbach als Gesundheitsminister für den Sommer 2024 angekündigt und zuletzt im Sommer 2026 noch einmal verschoben – wohl auch, weil die Koordination mit Verteidigungs- und Innenministerium aufwendiger war als gedacht. Inhaltlich soll es ein integriertes zivil-militärisches Gesundheitslagebild, definierte Zuständigkeiten, beschleunigte Entscheidungsprozesse, strategische Patientensteuerung, Bevorratung von Arzneimitteln und Medizinprodukten sowie Ernstfallübungen regeln. Die kürzlich ausgeschiedene Bundesgesundheitsministerin Nina Warken sah den größten Handlungsbedarf „beim Lagebild, bei der Datenlage und bei der Qualifikation" – man wisse nicht einmal zentral, wie viele Beschäftigte Kenntnisse über die Behandlung von Kriegsverletzungen hätten.

Zum digitalen Lagebild, dem Herzstück des Gesetzes, gehört es erst einmal, Transparenz herzustellen: Wo gibt es freie Intensivkapazitäten? Wo fehlt Personal? Welche Blutprodukte werden knapp? Welche ambulanten Kapazitäten können zusätzliche Fälle übernehmen? Welche Arzneimittel oder Medizinprodukte sind

kritisch? Gegebenenfalls sind einzelne dieser Fragen sogar in europäischer Dimension zu klären, um Ausweich- und Aufnahmemöglichkeiten in die Entscheidungsprozesse zu integrieren. Gerade im Kriegsfall wäre ein europäisches Hub-Modell, vergleichbar mit dem MEDEVAC-Hub für die Ukraine, notwendig: Welche Länder übernehmen die Akutversorgung, Reha, Prothetik oder chronisch Kranke? Welche Patient:innen werden zunächst stabilisiert und dann weiterverlegt? Welche Kapazitäten melden Länder verbindlich? Zusätzlich zu der ohnehin komplexen Multi-Stakeholder-Koordination des deutschen Gesundheitssystems entstünde noch eine weitere Dimension, weil auch europäische Krankenhäuser und Versorgungsketten einbezogen werden müssten.

Damit sind die Bausteine des Themas identifiziert, aber die Zuständigkeitsdiffusion noch nicht gelöst. Um hier Akzente zu setzen und eigene Beiträge zu leisten, haben sich diverse Institutionen zuletzt in die Diskussion eingebracht. Dazu gehört die DKG-Studie 2025 zur Krisenresilienz deutscher Krankenhäuser mit vertiefendem Blick auf mögliche Anforderungen an Kliniken. Das 140-seitige Papier zur „Zivilen Verteidigung 2.0" des Enneker Forums Tegernsee stammt von 67 verschiedenen Akteur:innen des Gesundheitswesens und enthält Vorschläge zu Patientenverteilung und Steuerungsstrukturen. Das Weißbuch der Deutschen Gesellschaft für Unfallchirurgie „Traumatologische Versorgung in Katastrophe, Krise, Krieg (3K)" appelliert, die 50 bestehenden regionalen Traumanetzwerke fest in die Krisensteuerung einzubinden. Darüber hinaus gibt es diverse regionale bzw. föderale Initiativen zur Stärkung der Krisenreaktionsfähigkeit. Da Rettungsdienst- und Krankenhausplanung Ländersache ist, gibt es hier unterschiedliche Antworten. So ist beispielsweise IVENA als kommerziell lizenzierte Software zur Echtzeit-Koordination für die Rettungsdienste in einigen Bundesländern, u. a. Berlin, ausgerollt. Parallel dazu gibt es das DIVI-Intensivregister für ICU-Betten und die DEMIS-Kapazitäts-Surveillance der gematik als Meldesysteme, die einmal täglich aggregiert Lagebilder der Krankenhäuser bereitstellen können. Es gibt also kein Bundesland „ohne Lösung", aber es gibt verschiedene parallele Strukturen. Was fehlt, ist ein einheitliches, interoperables, operatives Lagebild.

Was wir von anderen lernen können

Staaten, die näher an existenziellen Bedrohungen leben, sind hier deutlich weiter. In Israel beispielsweise gelten Krankenhäuser als kritische Infrastruktur, die auch unter extremem Druck weiterlaufen muss. Im Ichilov-Zentrum in Tel Aviv gehören klare Command-and-Control-Strukturen, Maßnahmen zur Personalresilienz und Krisenkommunikation fest zur Organisationskultur. In jährlichen „Emergency Management & Preparedness"-Kursen wird dieses Wissen auch an andere Nationen weitergegeben (siehe Seite 44). Finnland gilt aufgrund seiner langen Grenze zu Russland ebenfalls als Vorreiter von Gesundheits- und Versorgungssicherheit. Besondere Aufmerksamkeit erfährt die mentale Krisenresilienz als eine der entscheidenden gesellschaftlichen Kompetenzen.

Besonders viel lässt sich von Schweden lernen – und zwar im Bereich Kommunikation. Seit Jahrzehnten verteilt der Staat die Broschüre „Om krisen eller kriget kommer" („Falls Krise oder Krieg kommt"), zuletzt 2024 an rund fünf Millionen Haushalte. Sie behandelt eine Vielzahl von Szenarien wie extremes Wetter, gefährliche Infektionen, IT-Ausfälle, organisierte Kriminalität – und auch Krieg. Dazu gehören auch der Umgang mit Desinformation, emotionale Stabilität oder wie man mit Kindern über Krieg spricht. So werden zentrale Erkenntnisse der Risikokommunikationsforschung integriert: Wer Menschen konkrete Handlungsoptionen

Fotos: Adobestock

gibt (Vorrat, Verhalten, Rolle), verwandelt diffuse Angst in Selbstwirksamkeit. Genau hier agiert Deutschland bislang eher zögerlich. Vorsorge und Resilienz werden vornehmlich als Behördenthemen behandelt und richten sich an ein Fachpublikum. Eine an die Bevölkerung gewandte normalisierende Kommunikation wird eher vermieden, aus Sorge, hier unnötige Ängste zu schüren. Dies birgt zugleich das Risiko, das System hier verwundbar zu machen.

Eng verwandt mit der Kommunikation ist die Frage der Priorisierung. Sobald ein Mechanismus regelt, wer wohin kommt, steht die Frage im Raum, ob in Überlastungssituationen Behandlungen angepasst – also Patient:innen priorisiert – werden. Dies ist ein ethisch hoch sensibler Punkt, der nur schwer ohne Transparenz diskutiert werden kann. Es besteht die Gefahr, dass ein Steuerungssystem, das im Verborgenen entsteht, seine Legitimität verliert, bevor es gebraucht wird. Dabei geht es nicht darum, Entscheidungen bis ins Letzte auszuformulieren, aber Verantwortlichkeiten zu klären und den möglichen Rahmen zu skizzieren.

Der andere rote Faden, der sich durch fast alle bisherigen Krisen zieht, ist die Finanzierung. Sie betrifft Bereiche vom nicht refinanzierten Notstrom für Pflegeheime bis zu baulichen „Härtungsmaßnahmen" der Kliniken. Unweigerlich kommt die Frage auf, wie Krankenhausstrukturreform und Spargesetze in der GKV mit möglichen weiteren Belastungen in der Krisenvorsorge vereinbar sind. Auch dies mag ein Grund sein, die Diskussion nicht zu breit zu führen, sonst könnten die notwendigen Strukturreformen für Krankenhäuser und gesetzliche Krankenversicherungen mit neuen Herausforderungen verhindert werden. Trotzdem bleibt wahr, dass, wer Vorhaltung für den Ernstfall verlangt, sie auch bezahlen muss. Wichtig ist daher, auf doppelte Verwendbarkeit zu achten: Kapazitäten, die im Alltag Nutzen stiften, finden gesellschaftliche Akzeptanz. Leervorhaltung findet sie nicht.

Was jetzt zu tun ist

Deutschland hat 2026 einen echten Aktivitätsschub erlebt – Eckpunktepapiere, Gesetzesankündigungen, Weißbücher. Damit wurde das Thema innerhalb des Gesundheitswesens schrittweise normalisiert. Tatsächliche Steuerungsfähigkeit und die Übernahme von Verantwortung entstehen dadurch aber noch nicht.

Drei Dinge müssen im Alltag verankert werden, bevor die nächste Krise kommt. Das erste ist ein gemeinsames Lagebild – in Echtzeit, mit definierten Schwellenwerten und einer gemeinsamen Sprache zwischen ziviler und militärischer Seite. Zweitens müssen Strukturen aufgebaut und geübt werden: Jede Klinik, jede Leitstelle und jeder Rettungsdienst muss wissen, welche Leistungen im Krisenfall aufrechterhalten und welche zurückgefahren werden. Was in schlechten Zeiten funktionieren soll, muss in guten Zeiten erprobt sein. Und drittens muss eine offene Kommunikation gefunden werden, die den Balanceakt beherrscht: ehrlich über Risiken informieren, konkrete Handlungsoptionen aufzeigen – ganz ohne Alarmismus! Die Steuerungsfähigkeit unseres Gesundheitssystems entscheidet sich nicht in der Krise. Sie entscheidet sich jetzt.

Kontakt
Dr. Regina Vetters
regina.vetters@parthenon.ey.com

Krisen und ihre Lehren

1 **COVID-19 – Steuerung unter Dauerbelastung**
Ein Kollaps der Intensivstationen wurde vermieden, aber die Pandemie legte strukturelle Defizite offen: fehlende Echtzeitdaten, Rückstand bei der Digitalisierung, Finanzierungsdefizite der GKV, Pflegepersonalmangel und fehlende Vorbereitung der Akteur:innen auf langfristige Krisen. Die strukturell wichtige Lehre war die Bedeutung eines leistungsfähigen Öffentlichen Gesundheitsdienstes (ÖGD) als handlungsfähiger Akteur.

2 **Flutkatastrophe Ahrtal 2021 – Steuerung ohne Infrastruktur**
Über 150 Liter Regen pro Quadratmeter in 24 Stunden, mehr als 180 Tote, über das THW waren rund 4.100 ehrenamtliche Kräfte im Einsatz. Wichtigste Erkenntnis war das Steuerungsversagen zwischen Warnung und Handlung: Nicht fehlende Daten, sondern die fehlende Umsetzung wurde zum Problem.

3 **Hitzewelle – die wiederkehrende Krise**
Nach Schätzungen des Robert Koch-Instituts (RKI) gab es im Sommer 2026 mehr als 16.000 hitzebedingte Todesfälle. Insbesondere ältere Menschen mit Vorerkrankungen des Herz-Kreislauf-Systems oder der Atemwege sind gefährdet. Hitzeaktionspläne werden bislang sehr uneinheitlich umgesetzt.

4 **Stromausfall Berlin 2026 – Kaskadeneffekte in der Kälte**
Ein Brandanschlag auf eine Kabelbrücke führte zu einem bis zu fünftägigen Stromausfall. Rund 100.000 Menschen, vor allem aber fünf Krankenhäuser, 74 Pflege- und Seniorenheime sowie 205 Arztpraxen waren betroffen, mehrere Pflegeeinrichtungen mussten evakuiert werden. Insbesondere Pflegeheime zählen nicht zur Akutversorgung, die Notstromaggregate refinanzieren kann. Grundsätzlich ist die Pflege ins Katastrophenmanagement strukturell nicht regelhaft eingebunden.

5 **Cyberangriffe – die wachsende Bedrohung**
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verzeichnete 2025 43 IT-Sicherheitsvorfälle bei Leistungserbringenden. Gerade Erpresserangriffe auf Krankenhäuser können dabei sehr schnell versorgungsrelevant werden. Aber auch vernetzte Medizinprodukte wie Schrittmacher sind hier anfällig.

Diese fünf Krisen der letzten Jahre zeigen dasselbe Muster: Nicht Kapazität, sondern Steuerungsfähigkeit ist die wiederkehrende Schwachstelle des Gesundheitssystems. Zu dieser Steuerungsfähigkeit gehören die gezielte Lokalisierung und Versorgung vulnerabler Gruppen, die Sicherung kritischer Basisinfrastruktur wie Strom, IT und Kommunikation, die zeitnahe Koordination von Maßnahmen inkl. der klaren Zuständigkeiten und schließlich die Finanzierung von Maßnahmen wie Notstrom, IT-Sicherheit oder Personalkapazität.

Fotos: Adobestock/Gettyimages

Wenn Gesundheit zur Zielscheibe wird

Hybride Angriffe gefährden Versorgung und Sicherheit

Gemäß dem aktuellen Bundeslagebild Cybercrime des Bundeskriminalamtes (BKA) steigt die Anzahl der Cyberdelikte, bei denen der Aufenthaltsort der Täter:innen unbekannt ist bzw. nicht in Deutschland liegt, auf einen neuen Höchststand. Der Branchenverband Bitkom e. V. bemisst den Schaden durch Cyberattacken auf 202,4 Mrd. Euro. Hiervon ist vor allem das Gesundheitswesen betroffen. Laut dem Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist das Gesundheitswesen einer der Sektoren im KRITIS-Bereich, der von den meisten Störmeldungen betroffen ist. Die Arten der Angriffe auf diesen Sektor sind vielfältig und oftmals dramatisch, wie die Attacke auf den Abrechnungsdienstleister unimed im April dieses Jahres zeigt. Hier war es Angreifer:innen gelungen, zahlreiche Abrechnungsdaten von Patient:innen zu entwenden.

Die genaue Anzahl der Betroffenen ist schwer zu benennen. Medienberichten zufolge geht man bundesweit von mehr als 100.000 entwendeten Patientendaten aus. Nicht selten stecken staatlich kontrollierte ausländische Akteure dahinter. Doch welche Ziele verfolgen diese Staaten und was versprechen sie sich hiervon?

Hybride Kriegsführung als Mittel der Einflussnahme

Bei genauerer Betrachtung dieser Situation kommt man nicht um den Begriff „hybride Kriegsführung" herum. Der amerikanische Militärtheoretiker Frank G. Hoffman hat ihn erstmals 2007 eingeführt. Auch wenn es keine allgemein anerkannte Definition gibt, hat die hybride Kriegsführung zum Ziel, eine Erosion der Grenzen zwischen Krieg und Frieden herbeizuführen. Hierfür werden militärische wie nichtmilitärische Mittel eingesetzt (z. B. Cyberattacken, Sabotage kritischer Infrastrukturen), um bewusst Reaktionen in der Bevölkerung zu erzielen (z. B. Desinformation, Verlust von Vertrauen in die Politik), kriegerische Absichten zu erproben (z. B. Attacken auf kritische Infrastrukturen) oder Eskalationen herbeizuführen.

Für Cyberangriffe auf das Gesundheitswesen werden oftmals vermeintlich unabhängige nichtstaatliche Akteure eingesetzt. Dabei verdichten sich die Hinweise auf die Beteiligung russischer Hackergruppen – jedoch weiterhin ohne „substanzielle Belege", so das Bundesamt für Verfassungsschutz (BfV).

Motivation ausländischer Akteure

Es gibt eine Vielzahl von Akteuren, die das Gesundheitswesen attackieren. Beispielsweise haben Ransomware-Banden ein finanzielles Interesse, die Daten von Krankenhäusern zu verschlüsseln und gegen Lösegeld, das oft mit nicht nachverfolgbaren Kryptowährungen beglichen wird, wieder zu entschlüsseln.

Politische Akteure zielen auf andere Ziele ab, beispielsweise durch Angriffe auf Krankenhäuser, Abrechnungszentren, Versicherungen oder kritische Dienste im Gesundheitswesen wie die ePA oder das E-Rezept, um psychologischen Druck auszuüben. Mit dieser Methode der hybriden Kriegsführung sollen gezielt Unsicherheiten, Ängste und Misstrauen in Politik und staatliche Institutionen geschürt werden, schließlich zählen Gesundheitsdaten zu den sensibelsten Daten, die Menschen haben. Sind diese Daten nicht verfügbar, werden sie vernichtet oder kommen sie in die falschen Hände, kann das für die Betroffenen immense Folgen haben. Jeder Angriff auf KRITIS-Komponenten wird somit aufmerksam durch den Provokateur betrachtet, dokumentiert und ausgewertet und für weitere Angriffe wiederverwendet, mit der Absicht, das bereits geschürte Misstrauen auszuweiten.

Schutz vor hybriden Angriffen

Unternehmen müssen für den Schutz ihrer Infrastrukturen und Daten einen hohen Aufwand betreiben. Dies ist unerlässlich und oftmals mit hohen Kosten verbunden. Umso wichtiger ist es, Synergieeffekte so zu nutzen, dass sie einen Mehrwert erzielen, Governance-Strukturen nicht neu zu erfinden und Abhängigkeiten wie auch die Komplexität der Lösungslandschaft zu reduzieren. Gleichzeitig muss die Lösungslandschaft souverän geplant sein, um sich von der geopolitischen Lage so unabhängig wie möglich zu machen. Dies betrifft nicht nur den IT-Sektor, sondern ist vollumfänglich zu betrachten. Mitarbeitende müssen für potenzielle Bedrohungen sensibilisiert, kritische Einrichtungen wirksam gegen Sabotage und Spionage geschützt und strategische Reserven aufgebaut werden, um Lieferengpässen und Versorgungsunterbrechungen wirksam begegnen zu können.

Ein weiterer Schutzmechanismus ist der Staat. Provokateure, die befürchten müssen, selbst ins Fadenkreuz hybrider Angriffe zu geraten, sind zurückhaltender bei der Wahl potenzieller Angriffsziele. Dies ist einer der Gründe, weswegen die Bundesregierung plant, dem deutschen Nachrichtendienst mehr Befugnisse zu erteilen, damit er nicht nur Daten sammeln, auswerten und an vollzugsberechtigte Stellen übergeben, sondern auch selbst aktiv werden darf.

Kontakt
Thomas Ullrich
thomas.ullrich@parthenon.ey.com
Konstantin Meinhardt
konstantin.meinhardt@de.ey.com

Fotos: Adobestock

> Der US CLOUD Act und Art. 48 DSGVO stehen in einem echten Normenkonflikt. Ein Anbieter mit US-Konzernbezug kann rechtlich in beide Richtungen verpflichtet sein, und dieses Dilemma lässt sich vertraglich nicht vollständig auflösen. Für Kliniken und Krankenkassen heißt das: Souveränität entscheidet sich bereits bei der Wahl des Anbieters und seiner Kontrollstruktur.
>
> **Dr. Tristan Kalenborn, Rechtsanwalt, EY Law**

Wer hat die Kontrolle über Ihre IT?

Die entscheidende Frage hinter digitaler Souveränität

Stellen Sie sich vor, die Patienten- oder Versichertendaten Ihres Hauses liegen in einem Rechenzentrum in Frankfurt. DSGVO-konform, ISO-zertifiziert, physisch gesichert. Und trotzdem sind sie nicht ohne Weiteres souverän. Der Grund ist ein Denkfehler, der sich hartnäckig hält: „Unsere Daten liegen in Deutschland, also gilt deutsches Recht." Genau diese Annahme greift zu kurz. Denn maßgeblich ist nicht allein, wo die Server stehen, sondern welchem Rechtsraum der Anbieter unterliegt, der sie betreibt, und welche Kontrolle Sie tatsächlich über Ihre Daten haben.

Nach Patriot Act, CLOUD Act und FISA 702 können Softwareunternehmen aus den USA verpflichtet werden, Daten auf behördliche Anordnung herauszugeben bzw. Zugriff darauf zu gewähren, unabhängig davon, wo die Server physisch stehen. Die Hürden dafür sind hoch, und ein solcher Zugriff ist stets eine Einzelfallfrage. Doch ein Restrisiko bleibt, denn betroffen sind nicht nur US-Mutterkonzerne, sondern indirekt auch deren europäische Töchter. Für Entscheider:innen im Gesundheitswesen verschiebt das die Frage weg von „Wo liegen die Daten?" hin zu „Wer hat rechtlich und operativ die Kontrolle über meine IT?".

Kein Wunder, dass „souverän" 2026 zum meistgenutzten und zugleich am wenigsten definierten Wort der Gesundheits-IT geworden ist. Fast jeder Anbieter trägt das Label, kaum jemand meint dasselbe. In einem offenen Brief an die EU-Kommission warnen 25 europäische Cloud-CEOs sogar vor „Souveränitäts-Washing": Anbieter werben mit EU-Rechenzentren und Zertifikaten, ohne echte Kontrolle abzugeben.

▶ *Was bedeutet Souveränität?*

Digitale Souveränität ist nicht Autarkie und nicht Abschottung. Sie beschreibt die Fähigkeit, selbstbestimmt über die eigene digitale Infrastruktur, Daten und Technologieentscheidungen zu verfügen und jederzeit die Option zu behalten, den Anbieter zu wechseln. Die reine Datenlokalisierung, also „Server in der EU", deckt nur einen Teilaspekt ab.

Souveränität und Resilienz sind verwandt, aber nicht identisch

Resilienz und ▶ Souveränität gleichzusetzen, ist naheliegend, berücksichtigt aber nicht alle entscheidenden Aspekte. Abhängigkeit, d. h. das Fehlen von Souveränität, ist eine Form der Verwundbarkeit, das hat der CrowdStrike-Ausfall 2024 mit weltweit lahmgelegten Unternehmen und Milliardenschäden gezeigt. Insofern stärkt Kontrolle die Resilienz.

Zugleich sind die beiden Begriffe nicht deckungsgleich und können sich sogar widersprechen. Maximale Eigenkontrolle kann weniger resilient sein als ein professionell betriebener externer Cloud-Dienst. Ein Krankenhaus oder eine Krankenkasse, die die gesamte IT selbst betreibt, trägt auch das volle Risiko für Ausfallsicherheit, Sicherheitsupdates und Fachkräftemangel. Dies dauerhaft auf höchstem Niveau zu leisten, ist für viele Häuser nicht realistisch. Cloud-Hyperscaler investieren in Sicherheit, Angriffserkennung und Redundanz mehr, als dies eine einzelne IT-Organisation je

Fotos: Gettyimages

könnte. Souveränität steht damit in einem Zielkonflikt mit Sicherheit, Innovationstempo und Kosten. Wer diesen Konflikt ausblendet, trifft schlechte Entscheidungen.

Souveränität ist geschichtet, nicht binär
Souveränität ist nicht allein am Rechenzentrumsstandort festzumachen. Tatsächlich umfasst sie eine Reihe von Schichten, und das gesamte Gebäude ist nur so stabil wie seine schwächste Ebene:

- **Organisatorische Ebene:** Welchem Recht unterliegt die betreibende Gesellschaft? Ein EU-Standort schützt nicht vor Drittstaatengesetzen, wenn die Muttergesellschaft in den USA sitzt und dortige Gesetze umsetzen muss.

- **Operative Prozessebene:** Wer darf die Umgebung unter welchen Bedingungen betreiben, warten und darauf zugreifen? Betrieb, Störungsbearbeitung und Eskalation sollten nicht nach dem „Follow the sun"-Prinzip global aus Drittstaaten erfolgen, sondern in vertrauenswürdigen Rechtsräumen verbleiben und damit ausschließlich bei sicherheitsüberprüftem, national zugelassenem Personal.

- **Software- und Datenebene:** Selbst eine in Deutschland betriebene Infrastruktur ist nur teilweise souverän, wenn auf ihr weiterhin proprietäre Software aus einem Drittstaat läuft. Auch wenn Daten in abgeschotteten und nicht interoperablen Anwendungen liegen, wie häufig in der Klinik-IT, ist man stark abhängig vom Softwarehersteller und hat keine tatsächliche und wirksame Kontrolle.

- **Physische Ebene,** d. h. Infrastruktur und deren Lieferkette: Rund 90 Prozent der digi-

> Souveränität entsteht nicht durch Abschottung, sondern durch Interoperabilität. Erst wenn Datenräume nach gemeinsamen Standards zusammenarbeiten, behalten Kliniken die Kontrolle über ihre Daten und können sie trotzdem für Forschung und Versorgung nutzbar machen. Der Standort des Rechenzentrums ist dabei zweitrangig, entscheidend sind nutzbare Schnittstellen und die Hoheit über die eigenen Daten.
>
> **Dr. Anja Burmann, Abteilungsleiterin Healthcare, Fraunhofer ISST**

talen Endgeräte und etwa 69 Prozent der Bauteile stammen aus dem Ausland. Wer auf der Anwendungsebene US-Technologie meidet, aber bei der Hardware von chinesischen Herstellern abhängt, hat das Problem nur verschoben. Auch das Thema IT-Sicherheit spielt hier eine Rolle, z. B. im Bereich der Verschlüsselung. Kundenseitig verwaltete Schlüssel sind oft der wirksamste Schutz. Souveränität entsteht erst, wenn all die kritischen Schichten zusammen betrachtet werden.

Die neue Baustelle: Daten und KI

Mit dem Vormarsch klinischer Datenplattformen und KI verschiebt sich die Souveränitätsfrage erneut, weg von der Cloud und Infrastruktur, hin zur Software-, Daten- und Modellebene. KI ist nur so gut wie ihre Datenbasis. Wer keine Kontrolle über Qualität, Herkunft und Struktur der Daten hat, kann KI weder verantwortungsvoll noch wirtschaftlich einsetzen. Datensouveränität wird damit zur Voraussetzung für sinnvolle KI.

Drei Fragen entscheiden sich in der Architektur, lange bevor die erste Anwendung produktiv geht: Wer betreibt die klinische Datenplattform? Mit welchen Daten wird ein Modell trainiert, und verlassen diese den kontrollierten Raum? Wer kontrolliert am Ende das Modell? Wie dringlich das ist, zeigt der Leopoldina-Policy-Brief zu agentischer KI vom Juni 2026: Die Nationale Akademie warnt, dass gerade der Gesundheitsmarkt von US-Unternehmen dominiert wird, und macht die Stärkung technologischer Souveränität über domänenspezifische Foundation Models und eine unabhängige digitale Infrastruktur zu ihrer ersten Handlungsempfehlung.

Fotos: Adobestock

Der europäische Weg: Allein geht es nicht
Die Verordnung zum European Health Data Space (▶ EHDS) macht interoperable Datenhaltung ab März 2027 von der Vision zur Pflicht, flankiert vom Gesetz für Daten und digitale Innovation im Gesundheitswesen (GeDIG) und dem Standard ▶ ISiK, die faktisch ▶ FHIR-basierte Schnittstellen voraussetzen und monolithische KIS-Strukturen aufbrechen. Die ernüchternde Praxislücke: Viele Hersteller haben die ISiK-Zertifizierung, bieten die Schnittstellen aber nicht aktiv oder nur im Minimalumfang an. Ebenfalls wird die EHDS-Verordnung ihren kompletten Nutzen erst im März 2031 entfalten.

Auf Infrastrukturebene liefert Gaia-X das Gegenstück: eine gemeinsame Grundlage für interoperable Datenräume, die Souveränität über Standards und Vertrauen herstellt statt über Abschottung. Wie das im Gesundheitswesen konkret aussieht, zeigt das Gaia-X-Projekt „HEALTH-X dataLOFT", an dem auch das Fraunhofer-Institut für Software- und Systemtechnik (ISST) beteiligt ist: Es baut einen bürgerzentrierten Gesundheitsdatenraum auf, in dem Patient:innen ihre Daten selbst bereitstellen, nutzen und kontrollieren, von der klinischen Akte bis zu Aktivitätsdaten aus dem zweiten Gesundheitsmarkt.

Neben dem EHDS definiert parallel die EU-Kommission mit dem Cloud Sovereignty Framework (CSF) seit Oktober 2025 einen „Sovereignty Score" für die Beschaffung, der digitale Souveränität im Bereich Cloud-Technologie prüfbar macht. Konkret wird das in zwei Großprojekten: Das ▶ IPCEI-CIS baut seit Ende 2023 mit zwölf Mitgliedstaaten und rund 1,2 Mrd. Euro öffentlicher Förderung sowie 1,4 Mrd. Euro weiteren Investments aus der Industrie das erste anbieterneutrale Multi-Provider-Cloud-Edge-Kontinuum Europas auf. Das seit 2025 vorbereitete IPCEI-AI, für das allein Deutschland mit über 1 Mrd. Euro Förderung plant, ebenfalls zzgl. weiterer Investments aus der Industrie, zielt auf ein souveränes KI-Ökosystem mit offenen europäischen Basismodellen und sektorspezifischen KI-Modellen, ausdrücklich auch für regulierte Bereiche wie das Gesundheitswesen. Beide IPCEI-Projekte sind über die Dachinitiative „8ra" verzahnt, die Cloud-Edge-Infrastruktur und KI zusammenführt.

Handlungsempfehlung: risikobasiert statt alles oder nichts
Eine 100-prozentige Souveränität ist mit Blick auf die Globalisierung der letzten Jahrzehnte, mit dem aktuellen Technologievorsprung der USA sowie dem Kostendruck für viele Kliniken und Krankenkassen heute nicht umfänglich umzusetzen. Es gibt aber sinnvolle Kompromisse, und die Branche gibt die Antwort selbst. In einer Umfrage des SEMECO-Forschungsprojekts Cluster4Future bevorzugten 65 Prozent der Gesundheitsentscheider:innen eine Hybridstrategie aus souveräner europäischer Infrastruktur und Hyperscaler-Ökosystemen, nur 10 Prozent setzten rein auf Hyperscaler. Das übersetzt sich in bewusste Portfolio-Entscheidungen:

▶ ***EHDS***
(engl.: European Health Data Space)
europäischer Gesundheitsdatenraum für den sicheren Zugang zu elektronischen Gesundheitsdaten sowie für deren grenzüberschreitende Primär- und Sekundärnutzung

▶ ***ISiK***
(Informationstechnische Systeme im Krankenhaus)
von der gematik spezifizierter, FHIR-basierter Standard für den interoperablen Austausch von Gesundheitsdaten mit IT-Systemen im Krankenhaus

▶ ***FHIR***
(engl.: Fast Healthcare Interoperability Resources)
von der HL7-Organisation entwickelter internationaler Protokoll-Standard für den strukturierten und interoperablen Austausch elektronischer Gesundheitsinformationen

▶ ***IPCEI-CIS***
(engl.: Important Project of Common European Interest on Next Generation Cloud Infrastructure and Services)
europäisches Großvorhaben zum Aufbau einer souveränen Cloud- und Dateninfrastruktur in Europa

Fotos: Adobestock

- **Souverän betreiben, was den Kern schützt.** Primär- und Notfallsysteme, Patientenstammdaten und alles, was bei einem erzwungenen Zugriff die Versorgung gefährdet, gehört unter europäische Kontrolle. Anbieter wie STACKIT zeigen, dass das im Klinikbetrieb funktioniert. Sana reduziert zum Beispiel mit einer autarken Cloud-Umgebung die Abhängigkeit von globalen Hyperscalern, und die Charité hat mit Schwarz Digits ein gemeinsames Unternehmen gegründet, das klinische Daten auf souveräner STACKIT-Infrastruktur für Forschungszwecke harmonisiert.

- **Hyperscaler nutzen, wo Innovation zählt.** Punktuelle, nicht geschäftskritische Datenverarbeitung und KI-Pilotprojekte profitieren von einem Innovationstempo, das kein deutscher Anbieter allein halten kann. Entscheidend ist, dass keine sensiblen Rohdaten unkontrolliert abfließen.

- **Reversibilität einbauen.** Kundenseitige Verschlüsselung, Datenportabilität und eine echte Exitstrategie sind der Unterschied zwischen Abhängigkeit und Wahlfreiheit.

Digitale Souveränität ist damit kein Zustand, den man kauft, sondern eine Steuerungsaufgabe, die man behält. Für Kliniken und Kostenträger heißt das nicht, Hyperscaler zu meiden, sondern jeden Workload bewusst einzuordnen: Was muss unter eigener Kontrolle bleiben und was darf für den Innovationsvorteil in eine externe Cloud? Wer diese Frage beantworten kann, hat Souveränität verstanden. Wer sie an ein Rechenzentrum delegiert, hat sie bereits abgegeben.

Kontakt
Florian Benthin
florian.benthin@parthenon.ey.com

KI gegen KI

Wie sich Angriff und Abwehr verändern

Künstliche Intelligenz (KI) verändert Cybersecurity. Angreifer können Ziele schneller auskundschaften, überzeugendere Täuschungen erzeugen, bekannte Schwachstellen effizienter ausnutzen und vor allem neue Sicherheitslücken viel schneller finden. Gleichzeitig hilft KI den Verteidigern, verdächtige Muster früher zu erkennen, Alarme zu priorisieren und Reaktionen vorzubereiten oder Schwachstellen automatisiert zu beheben. Für Krankenhäuser, Pflegeanbieter, Krankenkassen, Pharmaunternehmen, Labore und Medizintechnikhersteller geht es deshalb nicht um ein abstraktes „KI gegen KI". Einen entscheidenden Vorsprung hat, wer seine eigene Umgebung besser kennt, Signale schneller einordnet und kontrolliert handelt – ohne Patientensicherheit, Datenschutz und Versorgungsqualität aus dem Blick zu verlieren.

Wenn Angriffe schneller skalieren als die Abwehr

Cyberangriffe treffen das Gesundheitswesen an seiner empfindlichsten Stelle: seiner Abhängigkeit von verfügbaren Daten, funktionierenden Geräten und verlässlichen Partnern. Ein Ausfall kann die Aufnahme von Patient:innen verzögern, Laborbefunde blockieren, Lieferketten unterbrechen oder die Produktion von Arzneimitteln beeinträchtigen. Der Bericht „ENISA Threat Landscape 2025" analysiert 4.875 öffentlich bekannte Vorfälle in der EU zwischen Juli 2024 und Juni 2025. Die sektorübergreifende Auswertung zeigt die industrielle Größenordnung des aktuellen Cybergeschehens.

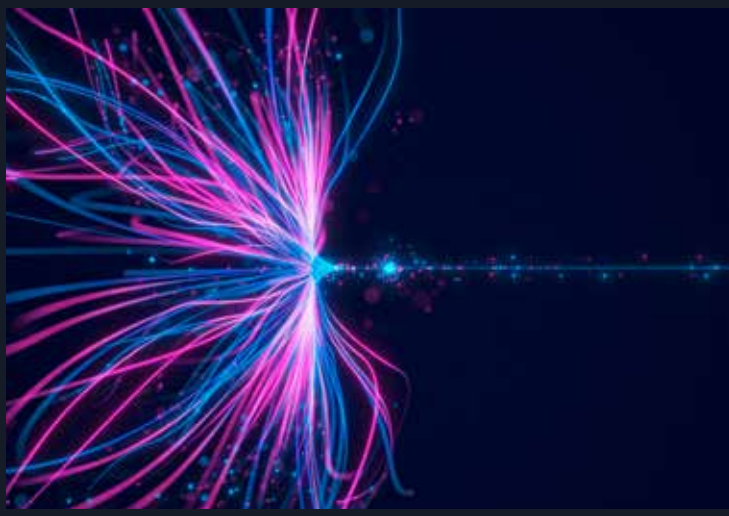
KI verschärft die Bedrohungslage. Sie kann große Mengen öffentlich verfügbarer Informationen auswerten, Rollen und Beziehungen identifizieren, täuschend echte E-Mails in jeder Sprache formulieren und gestohlene Daten schneller nach besonders wertvollen Inhalten durchsuchen. Auch bei der Suche nach Schwachstellen, beim Erstellen von Schadcode und bei der Anpassung bestehender Angriffswerkzeuge steigt die Effizienz. Das britische National Cyber Security Centre (NCSC) erwartet deshalb bis 2027 häufigere und intensivere Cyberbedrohungen. Es warnt zugleich vor einer digitalen Kluft zwischen Organisationen, die mit KI-gestützten Bedrohungen Schritt halten, und jenen, die zurückfallen.

Die wichtigste Veränderung ist damit nicht ein einzelner spektakulärer Angriff, sondern die industrielle Skalierung: mehr potenzielle Angreifer, extrem kurze Zeitfenster zum Schließen von Schwachstellen und mehr parallele Angriffe. Herkömmliche Schutzmaßnahmen bleiben notwendig. Sie müssen aber kontinuierlicher, risikobasierter und stärker automatisiert arbeiten.

Für den Gesundheitssektor verschiebt sich dadurch die operative Balance. Die Zeit zwischen dem Bekanntwerden einer Schwachstelle und einem möglichen Angriff wird kürzer, während medizinische Geräte, Laborsysteme und spezialisierte Anwendungen nicht immer sofort aktualisiert werden können. Hinzu kommen komplexe Freigaben, Herstellerabhängigkeiten und hohe Anforderungen an die Verfügbarkeit. Eine moderne Abwehr muss deshalb technische Dringlichkeit und Versorgungsrelevanz gemeinsam bewerten. Nicht jedes System lässt sich sofort abschalten, aber jedes kritische System braucht einen vorbereiteten Ausweich-, Eindämmungs- und Wiederanlaufplan.

Trainieren Sie nicht nur allgemeines Phishing. Üben Sie realistische Szenarien aus Ihrem Versorgungsalltag, etwa eine angebliche Rückfrage zu einem Laborbefund, eine dringende Lieferantenänderung oder einen Anruf mit imitierter Stimme einer Führungskraft.
Entscheidend ist ein klarer zweiter Bestätigungskanal.

Fotos: Adobestock ork



Neue Helfer schaffen eine neue Angriffsfläche

Während Angreifer KI nutzen, wächst im Gesundheitswesen zugleich die eigene KI-Landschaft. Sprachassistenten unterstützen den internen Helpdesk, Modelle strukturieren Arztbriefe, Anwendungen analysieren Bilddaten, Agenten koordinieren Termine oder greifen auf Wissensdatenbanken zu. Vieles entsteht dezentral: als Pilotprojekt, Cloud-Funktion, Erweiterung einer Standardsoftware oder eigenständig beschaffter Dienst.

Damit kommen neue schützenswerte Komponenten hinzu: KI-Modelle, deren Trainings- und Kontextdaten, Schnittstellen, Prompts, Agenten, Vektordatenbanken sowie die Konten und Schlüssel, mit denen KI-Systeme auf andere Anwendungen zugreifen. Ein manipulierter Prompt kann ein Modell zu einer unerwünschten Ausgabe bewegen. Korrumpierte Daten können Ergebnisse verzerren. Ein Agent mit zu weiten Berechtigungen kann eine falsche Entscheidung nicht nur empfehlen, sondern selbst eine Handlung auslösen. Gerade im Gesundheitswesen kann aus einem Informationsfehler damit ein Betriebs- oder Versorgungsrisiko werden.

Die erste Verteidigungslinie ist Sichtbarkeit. Jede relevante KI-Anwendung braucht einen eindeutigen Zweck, eine verantwortliche Person, dokumentierte Datenflüsse, definierte Zugriffsrechte und Protokollierung. Für agentische Systeme müssen die zulässigen Werkzeuge, die lesenden und verändernden Datenzugriffe, die menschlichen Freigabepunkte und eine sofortige Stop-Funktion verbindlich festgelegt sein. Das britische NCSC empfiehlt 2026 eine schrittweise Einführung, minimale Berechtigungen, laufende Verhaltensüberwachung und vorbereitete Reaktionspläne.

Führen Sie die Regel „Kein produktiver KI-Agent ohne Eigentümer, Protokollierung und Stop-Möglichkeit“ ein. Beginnen Sie mit den Systemen, die auf Gesundheitsdaten zugreifen oder operative Aktionen auslösen können. **Schaffen Sie eine KI-Asset-Datenbank, in der alle produktiven Systeme registriert sind.**

Der defensive Hebel: Aus Daten schneller Entscheidungen machen

Viele Organisationen besitzen bereits eine zentrale Sicherheitsüberwachung (SIEM). Sie sammelt Protokolldaten aus Identitäten, Endgeräten, Netzwerken und Cloud-Diensten und erzeugt Alarme. Das Problem ist selten der völlige Mangel an Signalen, vielmehr fehlen häufig Kontext, Priorisierung und Geschwindigkeit. Ein Alarm einer ungewöhnlichen Anmeldung ist deutlich kritischer, wenn dieselbe Identität kurz zuvor auf eine Patientendatenbank zugegriffen und anschließend große Datenmengen an einen Cloud-Dienst übertragen hat.

Hier liegt die Stärke von KI: Sie kann Signale aus verschiedenen Quellen verbinden, Auffälligkeiten großflächiger aufzeigen, ähnliche Fälle zusammenführen und Analyst:innen eine priorisierte Bewertung vorlegen. Zudem kann sie aus neuen Bedrohungsinformationen Vorschläge für Erkennungsregeln erzeugen und diese im Notfall kurzfristig implementieren und aktivieren. Diese Regeln sollten wie Software behandelt werden: versioniert, getestet, fachlich geprüft und kontrolliert ausgerollt. Aus einem statischen Regelwerk wird ein lernender Erkennungsprozess.

Der praktische Nutzen entsteht erst durch eine klare Aufgabenteilung. KI übernimmt die Auswertung großer Datenmengen, erstellt Zusammenfassungen und markiert Abweichungen. Erfahrene Mitarbeitende prüfen den Kontext, berücksichtigen klinische und regulatorische Auswirkungen und entscheiden über Maßnahmen. Dafür müssen die Vorschläge der Systeme nachvollziehbar bleiben. Jede Empfehlung sollte erkennen lassen, auf welchen Signalen sie beruht, welche Unsicherheiten bestehen und welche Systeme betroffen sind. So wird KI

nicht zum schwer kontrollierbaren Entscheidungsträger, sondern zu einer überprüfbaren Unterstützung für Sicherheitsbetrieb, Krisenmanagement und Fachbereiche.

Der Einsatz braucht jedoch Leitplanken. KI kann Zusammenhänge falsch bewerten, wichtige Signale übersehen, durch manipulierte Eingaben beeinflusst werden oder sensible Informationen an unberechtigte Personen ausgeben. Deshalb sollte sie zunächst Empfehlungen und nachvollziehbare Begründungen liefern. Kritische Entscheidungen – etwa die Isolation eines klinischen Systems oder die Sperrung eines privilegierten Kontos – bleiben unter menschlicher Kontrolle. Der 2025 vom National Institute of Standards and Technology (NIST) veröffentlichte Entwurf eines Cyber-KI-Profils ordnet das Spannungsfeld in drei Aufgaben: KI-Systeme sichern, KI für die Verteidigung einsetzen und KI-gestützte Angriffe abwehren.

Starten Sie mit drei klar messbaren Anwendungsfällen, zum Beispiel mit Kontoübernahmen, verdächtigem Datenabfluss und Ransomware-Vorzeichen. Messen Sie Erkennungszeit, Fehlalarmquote und die Zeit bis zur Eindämmung – nicht die Zahl eingesetzter KI-Werkzeuge.

„Human in the loop" – KI soll Analyst:innen Entscheidungsvorschläge erstellen und so Geschwindigkeit bringen.

Vom Alarm zur kontrollierten Reaktion

Eine schnelle Erkennung verhindert noch keinen Schaden. Entscheidend ist, was danach geschieht. Gerade in medizinischen und produktionsnahen Umgebungen wurden Reaktionen bislang bewusst manuell gehalten: Eine automatische Abschaltung könnte die Versorgung stärker beeinträchtigen als der zunächst beobachtete Vorfall. Das ist nachvollziehbar, führt aber in der Praxis häufig zu langen Abstimmungswegen.

KI kann diese Lücke schließen, ohne dass die Verantwortung an sie abgegeben wird. Sie kann den Vorfall zusammenfassen, betroffene Systeme und Daten benennen, ein freigegebenes Reaktionshandbuch auswählen und die nächsten Schritte vorbereiten. Ein Mensch bestätigt anschließend die Maßnahme. Bei wiederkehrenden, risikoarmen Fällen kann der Automatisierungsgrad schrittweise steigen; bei klinisch kritischen Systemen bleibt die Freigabe durch einen Menschen verbindlich.

Der gleiche Ansatz gilt für Schwachstellen. KI kann Warnungen mit der eigenen Systemlandschaft abgleichen, Prioritäten vorschlagen, Testfälle erzeugen und die Vorbereitung eines Patches beschleunigen. In späteren Schritten kann die KI Patches auch selbst entwickeln. Die Reihenfolge bestimmt dabei nicht allein ein technischer Schweregrad, sondern die mögliche Wirkung auf Versorgung, Produktion und sensible Daten.

Lassen Sie die KI zunächst Empfehlungen erstellen, dann Maßnahmen vorbereiten und erst bei nachgewiesener Qualität klar begrenzte Aktionen selbst ausführen. Für jedes Szenario braucht es einen Rücknahmeplan, einen Eskalationsweg und Verantwortliche.

Automatisieren Sie KI-gestützte Reaktionen stufenweise mit Blick auf Kritikalität.

Unser Cybersicherheits-Framework: Sieben Schutzfelder über den Lebenszyklus

Das EY-Whitepaper „Absicherung von KI-Umgebungen" strukturiert die Absicherung als ganzheitliches Cybersicherheits-Framework. ML-Ops-Governance bildet die übergreifende Klammer. Darunter verbindet das Modell Menschen, Prozesse und Technologien in sieben Schutzfeldern, die Entwicklung, Betrieb und Wartung abdecken.

Die Stärke dieses Ansatzes liegt in der durchgängigen Betrachtung. Die Absicherung beginnt nicht erst beim produktiven Modell und endet nicht mit einer einmaligen Freigabe. Datenherkunft, Training, technische Plattform, Bereitstellung, Wartung, Verantwortlichkeiten und Compliance werden als zusammenhängendes System gesteuert. Dadurch lassen sich Lücken zwischen Datenschutz, Informationssicherheit, Medizintechnik, Einkauf und Fachbetrieb sichtbar machen. Das Framework schafft zugleich eine gemeinsame Sprache für Leitung, IT, medizinische Bereiche, Datenschutz und Revision, ohne alle Beteiligten zu KI- oder Cybersecurity-Spezialist:innen machen zu müssen.

Fotos: Adobestock

EY-Cybersicherungs-Framework | Sieben Schutzfelder unter ML-Ops-Governance

Handlungsfeld	Ziel und Umsetzung
Datenerfassung und Datenvorverarbeitung	Sensible Daten maskieren und klassifizieren, Geheimnisse sicher verwalten sowie Vertraulichkeit, Verfügbarkeit und Integrität über den gesamten Datenlebenszyklus gewährleisten
Modelltraining und -validierung	Datensätze, Algorithmen und Code prüfen, Modelle härten, Komponenten dokumentieren sowie Robustheit, Laufzeitsicherheit, Qualität und Datenschutz testen
Containersicherheit	Infrastruktur, Betriebssystem, Netzwerke, Containerregister und Orchestrierung so absichern, dass kompromittierte Komponenten erkannt, begrenzt und aktualisiert werden können
Sicherheit der Modellbereitstellungspipeline	KI-Sicherheitstests, Zugriffskontrollen, Open-Source-Prüfungen, Versionskontrolle und Aufgabentrennung fest in die Inbetriebnahme integrieren
KI-Wartung	Modelle und Cloud-Umgebungen kontinuierlich überwachen, Anomalien erkennen, Änderungen protokollieren und Updates kontrolliert einspielen
Organisation	Betriebsmodell, Verantwortlichkeiten nach RACI, Risikoanalysen, Modell- und Datenverwaltung, Incident-Management und Schulungen verbindlich verankern
Ethik und Compliance	Sicherheitsrichtlinien, rechtliche und ethische Anforderungen, Leistungsfähigkeit, Nachvollziehbarkeit und Auditierbarkeit gemeinsam steuern

Messbar wird das Framework durch wenige Kennzahlen: Anteil produktiver KI-Systeme mit eindeutiger Verantwortung, dokumentierten Datenflüssen und geprüfter Stop-Möglichkeit, Abdeckung der Sicherheitsprotokollierung, Zeit bis zur Erkennung und Eindämmung, Dauer bis zur Behandlung kritischer Schwachstellen sowie Anteil kontrollierter Modell- und Datenänderungen.

Die Methodik verbindet klassische Informationssicherheit mit KI-Governance. Das passt zu den Inhalten der EU-KI-Verordnung, die Risikomanagement, menschliche Aufsicht, Robustheit, Cybersicherheit, Transparenz und Datenschutz als zusammenhängende Anforderungen verlangt. Compliance ist dabei nicht das Endprodukt. Sie schafft den überprüfbaren Rahmen, in dem schnellere Verteidigung verantwortbar wird.

> Im KI-Zeitalter wird nicht die Organisation mit den meisten Sicherheitswerkzeugen resilienter sein, sondern diejenige, die ihre eigene digitale und KI-gestützte Umgebung schneller versteht, als Angreifer sie automatisiert analysieren. Dann wird Reaktionsgeschwindigkeit zu einer Frage der Versorgungsqualität – und Cybersecurity zu einem unmittelbaren Bestandteil der Gesundheitsleistung.
>
> **Dr. Srdan Dzombeta, Cybersecurity Lead, EY Consulting GmbH**

Wenden Sie die sieben Schutzfelder zunächst auf einen kritischen Versorgungsprozess an, etwa Notaufnahme, Arzneimittelproduktion oder Leistungsabrechnung.

Skalieren Sie, wenn Datenflüsse, Abhängigkeiten, Freigaben und Reaktionswege dort nachvollziehbar sind.

Resilienz endet nicht an der eigenen Tür

Gesundheitsversorgung ist ein Netzwerk aus Leistungserbringern, Kostenträgern, Forschung, Pharma, Medizintechnik, Logistik, Cloud- und IT-Dienstleistern. Ein KI-gestütztes Sicherheitsmodell muss deshalb die Lieferkette einbeziehen. Verträge brauchen prüfbare Vorgaben zu Protokolldaten, Melde- und Reaktionszeiten, Handlungsbefugnissen und forensischer Unterstützung. Die ENISA-Leitlinien vom Juli 2026 verankern Cybersecurity in allen Beschaffungsphasen – von Planung und Auswahl bis zum Lieferantenmanagement.

Ein zusätzliches KI-Produkt schafft noch keine Resilienz. Entscheidend ist das Zusammenspiel aus Prozessen, Menschen, Daten und Technik. Zentrale Erkennungs- und Reaktionsprozesse dürfen zudem nicht vollständig an ein einzelnes Modell oder einen Anbieter gebunden sein. Damit Geschwindigkeit nicht zulasten der Versorgung geht, müssen Reaktionswege bereits vor einem Vorfall organisationsübergreifend festgelegt und regelmäßig geübt werden. Dazu gehören klare Schwellenwerte für automatische Maßnahmen, erreichbare fachliche Entscheider:innen sowie abgestimmte Alternativen für den Weiterbetrieb. Besonders wichtig ist die Verbindung von Cybernotfallplanung, klinischem Krisenmanagement und Business-Continuity-Management auch mit kritischen Dienstleistern. Erst wenn Rollen und Übergaben im Alltag bekannt sind, kann KI im Ernstfall helfen, Zeit zu gewinnen, ohne neue Unsicherheit in medizinische oder produktionsnahe Abläufe zu tragen.

Ergänzen Sie Ausschreibungen und Verträge um vier prüfbare Punkte: Zugriff auf Sicherheitsprotokolle, verbindliche Reaktionszeiten, Unterstützung bei Eindämmung und Forensik sowie ein geregeltes Exit-Szenario für Daten, Modelle und Schnittstellen.

Verpflichten Sie Dienstleister, Sie bei der Einhaltung Ihrer Compliance-Vorgaben zu unterstützen.

Fazit

KI macht weder den Cyberangriff autonom noch die Verteidigung fehlerfrei. Sie verändert vor allem das Tempo. Gesundheitsorganisationen gewinnen, wenn sie ihre KI-Landschaft kennen, relevante Signale überwachen, Entscheidungen kontrolliert beschleunigen und aus Vorfällen lernen. Der Mensch bleibt für Prioritäten, Freigaben und die Abwägung zwischen Sicherheit und Versorgung verantwortlich; KI verstärkt seine Handlungsfähigkeit.

Kontakt
Dr. Srdan Dzombeta
srdan.dzombeta@de.ey.com
Erik Donner
erik.donner@de.ey.com

Von sicheren Netzen zum sicheren Zugriff

Zero Trust stärkt die digitale Resilienz

Die Telematik-Infrastruktur (TI) als Basis für die Digitalisierung im Gesundheitswesen steht vor ihrer größten Aktualisierung: Mit der TI 2.0 und dem Zero-Trust-Ansatz wird sie aktuell komplett neu gedacht und erste Projekte werden bereits umgesetzt – u. a. mit dem Ziel, die Resilienz der TI zu erhöhen.

Die TI 1.0 beruht auf Konzepten vom Beginn der 2000er-Jahre: Ein zentrales, sicheres Netz wird zur Kommunikation der Beteiligten im Gesundheitswesen aufgebaut und genutzt. Dies führt z. B. dazu, dass Leistungserbringende einen sogenannten Konnektor in der Praxis haben müssen, der die Anbindung an dieses sichere Netz durchführt. Innerhalb des Netzwerks wird die Kommunikation dann weiterhin Ende-zu-Ende verschlüsselt, um zwei Absicherungsebenen zu gewährleisten. Dies ist ein bewährtes Sicherheitsmuster: Wenn eine der beiden Ebenen – Zugang zum Netzwerk oder Verschlüsselung – kompromittiert wird, stellt die zweite Ebene immer noch eine Hürde dar.

Basierend auf dieser Struktur wurde eine Reihe von Diensten aufgebaut, die heute im Gesundheitswesen digitale Kommunikation ermöglichen. Dazu gehören:

- **VSDM – Versichertenstammdatenmanagement:** Hier prüfen Leistungserbringende mit dem Stecken der Karte den Versichertenstatus ihrer Patient:innen.
- **KIM (früher KOM-LE) – Kommunikation im Medizinwesen:** Austausch von Dokumenten zuerst unter den Leistungserbringern, später dann auch mit den Kostenträgern. Wird heute unter anderem für die elektronische Arbeitsunfähigkeitsmeldung an Kostenträger oder den Heil- und Kostenplan beim Zahnarzt genutzt. Seit dem Produktivstart im August 2021 sind darüber mittlerweile fast eine Milliarde Nachrichten verschickt worden.
- **ePA – elektronische Patientenakte:** Leistungserbringende (und auch Versicherte) stellen hier Dokumente wie Befunde und Laborberichte für die Nutzung durch andere Leistungserbringende bzw. für die Einsicht durch die Versicherten ein.
- **E-Rezept – elektronisches Rezept:** Neben der ePA der wohl bisher wichtigste Dienst für die Versicherten, da Rezepte jetzt nicht mehr in Papierform ausgestellt werden, sondern – auch digital – „auf der Karte" landen und eingelöst werden können.

Trotz dieser Erfolge wird die Telematik-Infrastruktur von vielen Kritikern als fragil und nicht sehr zuverlässig angesehen. Dies wird auch an den Ausfallstatistiken der TI deutlich. Die Komplexität der Netzwerkanbindung und auch Probleme mit der Fail-over-Fähigkeit einzelner Komponenten werden als wesentliche Gründe gesehen. Zudem wird in der Industrie häufig angemerkt, dass sich die Spezifikationen der

Fotos: Adobestock

TI, die von der gematik definiert werden, nicht streng an Industriestandards halten. Mit dem Ziel erhöhter Sicherheit werden hier viele Sonderlösungen erforderlich, die auch die Kosten und die jeweilige Umsetzungsdauer erhöhen.

Ziele der gematik mit der TI 2.0 sind daher, zum einen die Abhängigkeit von einzelnen Diensten (wie dem zentralen Netz) zu verringern und zum anderen mehr auf Industriestandards zu setzen, um die Umsetzungsgeschwindigkeit zu erhöhen.

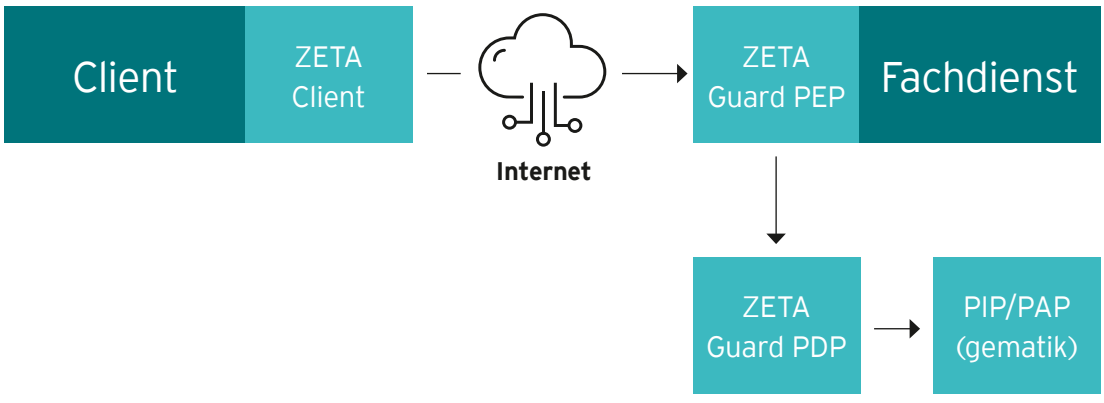
Mit der Zero-Trust-Architektur hat die gematik den Weg in die Zukunft der TI definiert. Diese Architektur geht davon aus, dass jeder Request auf eine Ressource gesondert zugangsgeprüft wird, selbst wenn er aus einem Netzwerk kommt, von dem angenommen wird, dass es sicher ist. Zudem werden nicht nur die User Credentials (Login) geprüft, sondern auch der Zustand und Kontext (z. B. Ort) des aufrufenden Clients. Der Zero-Trust-Ansatz ist ein etabliertes Sicherheitskonzept, siehe z. B. Zero Trust Architecture | NIST[1], aus dem sich eine moderne Sicherung von Aufrufen insbesondere über unsichere Netze wie das Internet ergibt.

In der TI 2.0 können daher alle Aufrufe ohne Sicherheitseinbußen über das Internet stattfinden – das zentrale Netz genauso wie die Netzwerk-Konnektoren sind dafür nicht mehr nötig. Hierbei werden zudem mehr und mehr Industriestandards verwendet, wie OpenID Connect Flows oder Policy Agents sowie verschiedene andere Internet-Standards (RFCs).

Übergang von Zugriffen über gesicherte Netze zum sicheren Zugriff über unsichere Netze

TI 1.0: gesichertes Netzwerk

TI 2.0: gesicherter Zugriff



ZETA Client
Prüfung des Client-Zustands („attestation"), Registrierung von Clients, Authentifizierung

ZETA Guard
PEP (Policy Enforcement Point): Zugriffskontrolle, PDP (Policy Decision Point): Ermitteln der erlaubten Zugriffe
PIP (Policy Information Point) und PAP (Policy Administration Point): Bereitstellung benötigter Policies und Informationen

1 www.nist.gov/publications/zero-trust-architecture

Um den hohen Sicherheitsanforderungen an die Verarbeitung von Gesundheitsdaten zu genügen, wird auch in der Kommunikation zwischen Clients und Servern eine zweite Sicherheitsschicht eingezogen: Innerhalb eines Requests werden die Daten ein zweites Mal verschlüsselt, diesmal mit anderen Algorithmen und Trust-Ankern, sodass hier wieder Unabhängigkeit und damit doppelte Sicherheit gegeben ist.

Für die Umsetzung sieht die gematik vor, einen sogenannten ZETA Guard vor jedem Fachdienst zu installieren, der die Aufrufe gemäß den von der gematik bereitgestellten Policies prüfen kann. Ein Policy Decision Point prüft dabei Zugriffsanfragen und erteilt die Erlaubnis oder verweigert sie. Der Policy Enforcement Point lässt dann nur erlaubte Zugriffe auf den eigentlichen Fachdienst zu.

Caching und Fehlertoleranz bei Anbindung an andere Dienste machen die zukünftige Infrastruktur besser verfügbar. Eine Geolokation der Aufrufe und „Impossible Travel Detection", also die Erkennung und Abwehr von fast gleichzeitigen Zugriffen aus unterschiedlichen Ländern, erhöhen die Sicherheit weiter. Ein definiertes Monitoring erlaubt eine schnelle Reaktion auf Angriffe. Clients müssen den eigenen Zu-stand erfassen, z. B. durch App Attestation auf mobilen Geräten, und können damit dem Guard vermitteln, dass sie nicht kompromittiert sind.

Der erste Dienst, der mit ZETA in Betrieb gegangen ist, ist der sogenannte PoPP-Service (Proof of Patient Presence). Dieser Dienst ersetzt im Endausbau das im jeweiligen Quartal nötige „Stecken der Karte" bei den Leistungserbringenden in der Praxis durch eine App. Dies erlaubt es z. B., Dauermedikation ohne Besuch einer Praxis auch über einen Quartalswechsel hinweg bequem anfordern zu können. Dieser Dienst wird jetzt nach und nach ausgerollt. Weitere bereits geplante Dienste sind dann der VSDM 2.0 sowie der Dienst für digitale Rechnungen bei Privatversicherten.

Mit der Zero-Trust-Architektur setzt die gematik die Ziele der TI 2.0 um: Unabhängigkeit von zentraler Infrastruktur sowie moderne und aktuelle Architekturprinzipien bei Beibehaltung der hohen Sicherheitsanforderungen, wie sie für Gesundheitsdaten unverzichtbar sind. Neben den bereits genannten Diensten werden in den nächsten Jahren weitere Dienste auf die Zero-Trust-Architektur umgestellt, wie ePA oder das E-Rezept, womit in absehbarer Zeit die zentrale Infrastruktur 1.0 abgebaut werden kann und damit im Idealfall Kosten eingespart und die Resilienz des Systems erhöht werden kann.

Kontakt
André Fachat
andre.fachat@de.ey.com

Fotos: Gettyimages

Vom Planwert zur Planungsgröße

Krisenresilienz strukturieren und quantifizieren

Wie groß die Herausforderung in einem NATO-Bündnisfall wäre, macht eine Zahl deutlich, die in der Debatte immer wieder auftaucht: Der Sanitätsdienst der Bundeswehr geht in seinen Szenarien von bis zu 1.000 verwundeten Patient:innen pro Tag aus, rund ein Drittel davon intensivpflichtig, die zur Behandlung nach Deutschland verlegt würden.

Von der ersten Annahme zum konkreten Bedarf

Die DKG-Resilienzstudie 2025 versucht bereits mit diesen Werten zu arbeiten, um die Belastbarkeit der Intensivversorgung zu überprüfen. Basierend auf Erfahrungswerten wird dabei angenommen, „dass ein Drittel der maximal zu erwartenden 1.000 Verwundeten internistisch behandelt werden muss, 44 Prozent leichtchirurgisch und 22 Prozent schwer-chirurgisch." Hochgerechnet auf ein vollständiges Jahr „wäre somit mit bis zu 80.300 schwer-chirurgischen Fällen zu rechnen". Genau diese – und viele weitere – Übersetzungen braucht es, um Bedarfe konkreter und künftige Engpässe frühzeitig zu verstehen. Dabei endet der Bedarf keineswegs bei der Anzahl Krankenhausbetten. Ein belastbares Modell muss Zufluss, Case-Mix, Akutkapazitäten, Blut- und Materialbedarf, Reha/Prothetik, ambulante Substitution, zivile Verdrängung und Effekte aus möglichen Triageregelungen sowie Governance und digitales Lagebild miteinander verbinden.

Ein gutes Modell zeigt nicht nur den Zusatzbedarf, sondern kann auch Systemfolgen identifizieren. Welche Ressource wird zuerst knapp? Wie viele elektive Eingriffe müssten verschoben werden? Welche zivilen Leistungen müssen geschützt werden? Welche Last kann ambulant aufgefangen werden? Welche Reha- und Pflegewelle folgt nach der Akutphase? Auf diese Weise kann die Planungsgröße von 1.000 Patient:innen pro Tag von einer ersten Annahme auf steuerbare Aufgaben heruntergebrochen werden. Erst daran anschließend können Beschaffungsstrategien für Medikamente, Blutprodukte oder Prothetik sowie der Qualifizierungs- und/oder Reaktivierungsbedarf für medizinisches Personal maßvoll entwickelt werden und über Szenarioanalysen verschiedene Optionen evaluiert und Investitionsbedarfe quantifiziert werden.

Bislang fehlt der Debatte eine solche Validierung für verschiedene Krisenszenarien. Für das Thema Bündnisfall geht es uns dabei nicht darum, ein fertiges Projektmodell zu entwickeln, sondern einen belastbaren Weg aufzuzeigen, wie aus Planungsannahmen konkrete Systemwirkungen, Engpässe und Steuerungsbedarfe abgeleitet werden können.

Erst der Normalbetrieb, dann die Krise

Um Verdrängungseffekte überhaupt quantifizieren zu können, muss zunächst der Regelbetrieb unabhängig von einer Krisensituation modelliert werden. Erst die Differenz zwischen dem Normalbetrieb und dem Krisenszenario macht Verdrängungen messbar. Folgende Dimensionen müssen dabei berücksichtigt werden:

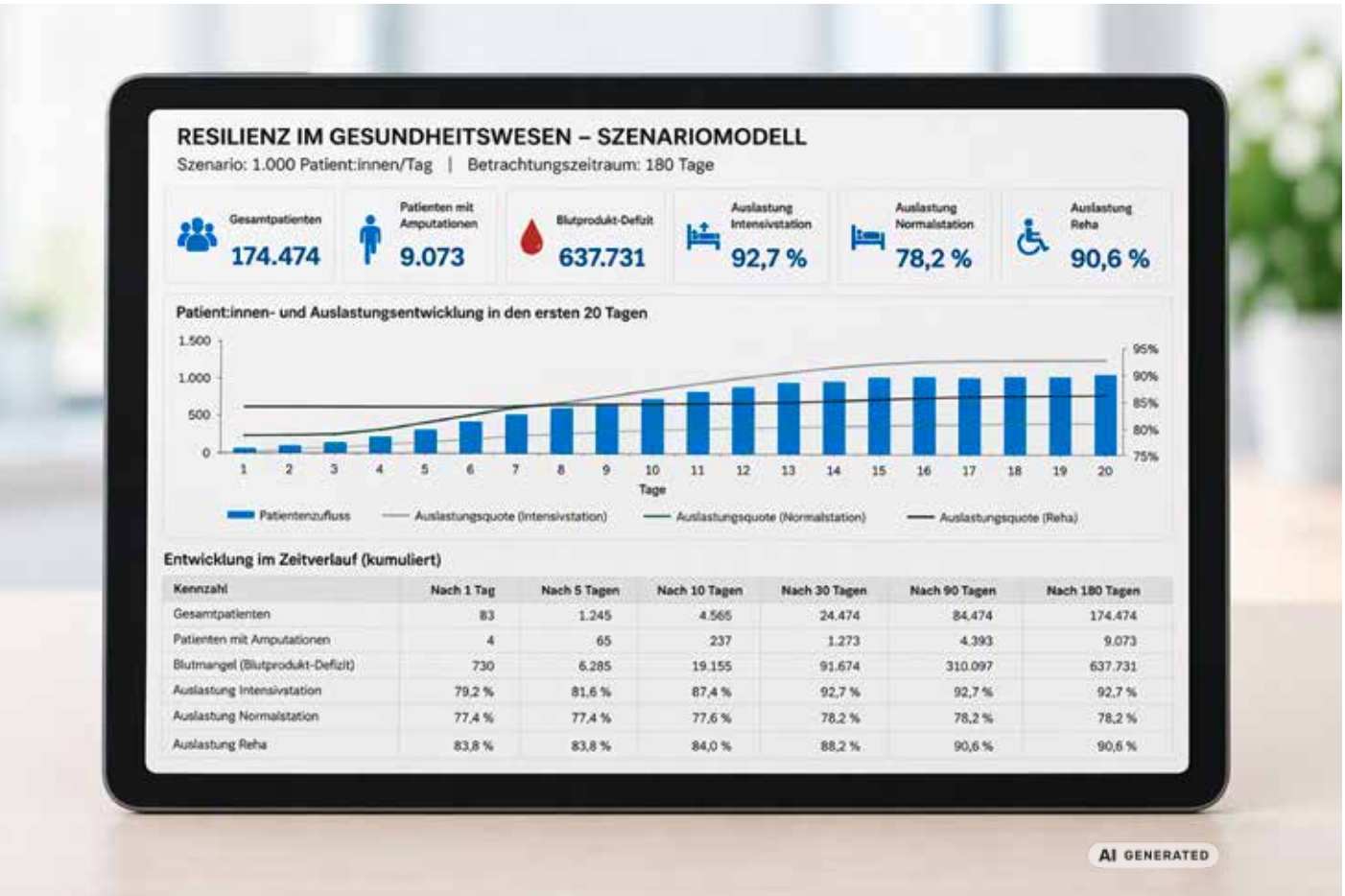
- **Kapazitäten im Regelbetrieb:** OP-Kapazitäten inklusive Personal, Material, Sterilgut und Medikamenten sowie die aktuelle Auslastung von Krankenhäusern und Reha-Einrichtungen.
- **Trennung militärischer und ziviler Kapazitäten:** Bereits im Base Case sollten beide Systeme getrennt betrachtet werden, da sie unterschiedlich auf Belastungen reagieren.
- **Fachbereichsbezogene Betrachtung:** Zuordnung typischer Verletzungsmuster (z. B. Extremitäten-, Thorax-, Abdominal- oder Schädel-Hirn-Verletzungen) zu den betroffenen Fachbereichen. Dadurch lassen sich Verdrängungen gezielt dort abbilden, wo sie voraussichtlich zuerst auftreten (insbesondere Unfallchirurgie, Neurochirurgie, Gefäß- und Viszeralchirurgie sowie Intensivmedizin).
- **Blutkonserven:** Bestände, Verbrauch und Spendenaufkommen sollten separat modelliert werden. Nur so lässt sich abschätzen, ab wann Engpässe entstehen. Dabei ist anzunehmen, dass die Spendenbereitschaft nach Beginn eines Konflikts ansteigt. Dieser Effekt könnte als variabler Parameter berücksichtigt werden. Große Kampagnen zu diesem Thema oder mögliche Beschaffungen über zusätzliche Partner könnten beispielsweise in Form von Szenarien abgebildet werden.

Erweiterte Modelle könnten auch Annahmen zu Personal, weiterem Material und zu Medikamenten integrieren. Gerade die wichtigste Ressource Personal ist schwer greifbar, weil

Fotos: Adobestock

medizinische und pflegerische Fachkräfte nicht selten mehrfach verpflichtet sind – sie arbeiten hauptberuflich in Klinik oder Praxis, engagieren sich zugleich ehrenamtlich im Katastrophenschutz und sind womöglich auch noch Reservist:innen der Bundeswehr. Im Ernstfall entsteht daraus ein Zielkonflikt: Dieselbe Person kann nicht gleichzeitig im Kreißsaal, im THW-Einsatz und im Sanitätsdienst tätig sein. Wer im Krisenfall tatsächlich wo zur Verfügung steht, ist deshalb schwer verlässlich zu beziffern und müsste über weitere Annahmen validiert werden.

Der Normalbetrieb basiert auf offiziellen Zahlen: Laut Statistischem Bundesamt verfügt Deutschland über rund 473.000 Krankenhausbetten, davon knapp 26.000 Intensivbetten, bei einer durchschnittlichen Auslastung von 76 beziehungsweise 79 Prozent und einer Verweildauer von 7,1 Tagen, ergänzt um rund 161.000 Reha-Betten und einen täglichen Blutverbrauch von etwa 10.000 Einheiten. So entsteht ein realistisches Bild der Ausgangslage. Die Krisenparameter stammen aus anderen Quellen: Für Verletzungsmuster, Operations- und Transfusionsbedarf lässt sich auf ausgewertete Erfahrungsdaten aus der Ukraine zurückgreifen, nach der rund 90 Prozent der Verwundeten Explosionsverletzungen und damit einhergehende Verbrennungen und knapp 88 Prozent Extremitätenverletzungen aufweisen. Erst die Kombination beider Welten – deutscher Normalbetrieb und ukrainisches Verletzungsspektrum – macht die Belastung greifbar. Veränderungen aus Erkenntnissen neuer Strategien und Methoden der Kriegsführung (z. B. vermehrte Drohneneinsätze statt traditioneller Waffen) könnten bei besserer Datenlage künftig auch zu berücksichtigen sein.



Handlungsbedarfe offenlegen

Rechnet man ein Szenario von 1.000 Patient:innen pro Tag über 180 Tage mit einem langsamen Anstieg in den ersten Tagen durch, kumulieren sich rund 170.000 zusätzliche Fälle. Das entscheidende Ergebnis ist aber nicht diese Summe, sondern wo das System zuerst reißt – und dass die Bruchstelle wandert. Die stationären Betten bleiben mit einem Rückgang der freien Kapazität von nur rund 1 Prozent recht robust. Die Intensivkapazität hingegen sinkt um etwa 13 Prozent. Diese Werte sind allerdings mit Vorsicht zu lesen: Das Modell rechnet mit einem festen Bettenbestand – tatsächlich ist eine Bettenzahl immer nur so belastbar wie das Personal, das sie betreibt. Die reale Engstelle dürfte also früher greifen, als die reine Bettenrechnung nahelegt. Ein klarer Engpass dürfte dort entstehen, wo in der öffentlichen Debatte kaum jemand hinsieht: in der Rehabilitation. Sie ist schon im Normalbetrieb zu rund 84 Prozent ausgelastet – der freie Puffer ist also klein. Genau dieser Spielraum wird im Szenario binnen weniger Wochen stark belastet, wobei die Auslastung auf über 90 Prozent steigt, obwohl die Reha-Welle erst mit Verzögerung einsetzt. Insbesondere Prothetikverletzungen würden häufig aufwendige Rehabilitationen nach sich ziehen und auch ambulant noch weitere Betreuung erfordern.

Parallel steigt der Bedarf an Blutkonserven spürbar: Im eingeschwungenen Zustand kommen im Modell rund 3.000 Einheiten pro Tag hinzu – zusätzlich zu einem Normalverbrauch von etwa 10.000. Ob daraus ein Versorgungsengpass wird, hängt entscheidend davon ab, wie schnell die Spendenbereitschaft nachzieht. Anders gesagt: Die erste Welle trifft OP, Intensivmedizin und Blutversorgung – die zweite, oft übersehene Welle trifft Wochen später die Reha und Prothetik. Wer nur auf Akutbetten schaut, plant an der eigentlichen Knappheit vorbei.

Das Modell ließe sich um mehrere Dimensionen erweitern. So wären regionale Kapazitäten ein weiterer Faktor – und die unterschiedlichen Kapazitäten von Universitätskliniken, BG-Kliniken und ausgewählten Maximalversorgern. Alternativ ließe sich fragen, welche Möglichkeiten bestehen, weitere Infrastruktur zu nutzen: Mit welchem materiellen und personellen Einsatz könnten weitere Gebäude und Einrichtungen ertüchtigt werden? Wie würde die Verteilung von Patient:innen auf die jeweiligen Kapazitäten tatsächlich erfolgen? Welche Kosten der effektiven Steuerung über Bund und Länder hinweg wären in die Betrachtung einzubeziehen? Eine weitere Ausbaustufe des Modells könnte die differenzierte Betrachtung von Blutprodukten umfassen. Dabei wäre neben möglichen Veränderungen des Spendenaufkommens insbesondere die regionale Verfügbarkeit verschiedener Blutproduktarten relevant. Darüber hinaus könnten logistische Restriktionen wie Transportzeiten, Lagerfähigkeit und Verteilungsmechanismen berücksichtigt werden.

Ebenso könnte die Arzneimittelversorgung stärker in die Analyse einbezogen werden. Dabei wären sowohl der zusätzliche Bedarf infolge erhöhter Patientenzahlen als auch potenzielle Auswirkungen auf Lieferketten und die Verfügbarkeit einzelner Medikamente zu betrachten. Auch die Vertiefung der hier noch offenen Personalfrage und möglicher Reserven wäre ein eigenes Thema. Wichtiger ist es jedoch, aus der Bedarfsrechnung eine Gestaltungsfrage zu machen. So könnte man frühzeitig identifizieren, welche Rehafälle auch ambulant aufgefangen werden oder wie Intensivbetten vorausschauend entlastet werden können. Oder welche elektiven Eingriffe wirklich aufschiebbar sind. Solche Überlegungen verlagern die Debatte weg von der Frage „Wie viele Betten fehlen uns?“ hin zu der klügeren Frage „Welche Last müssen wir überhaupt im Akutsystem abbilden – und welche ließe sich anders organisieren?“. Genau dann wird aus einer Kapazitätsrechnung eine echte Resilienzplanung.

Kontakt
Sebastian Schmidt
sebastian.schmidt@parthenon.ey.com
Marco Strube
marco.strube@parthenon.ey.com
Dr. Regina Vetters
regina.vetters@parthenon.ey.com

Fotos: Adobestock

Einsatzbereit in Extremlagen

Koordination und Vorbereitung erhöhen die Resilienz

Ein Massenanfall von Verletzten (MANV) ist eine Situation, in der die Anzahl der Verletzten die im Regelbetrieb verfügbaren Versorgungsressourcen eines Krankenhauses oder einer Region zeitweise übersteigt. Neben klassischen MANV-Lagen rücken heute auch Pandemien, Cyberangriffe, Energieausfälle und weitere KRITIS-Szenarien in den Fokus. Resilienz ist damit Teil der strategischen Krankenhaussteuerung: Krankenhäuser müssen auch unter Extrembedingungen handlungsfähig bleiben.

Steuerungsfähigkeit herstellen und erhalten
MANV-, Evakuierungs- und Krisenstabsübungen sowie definierte Führungs- und Eskalationsstrukturen sind in vielen Krankenhäusern etabliert. Die Herausforderung besteht darin, die damit verbundenen Maßnahmen auch unter realen Bedingungen wirksam umzusetzen. Erst ein gemeinsames Lagebild ermöglicht die zentrale Steuerung von Patientenzuweisungen, Kapazitäten und Ressourcen im Krisenfall.

Eine Schlüsselrolle übernimmt dabei klassischerweise die zentrale Notaufnahme. In Großschadenslagen (z. B. MANV) übernimmt sie die Funktion eines klinischen Lage- und Verteilungszentrums. Dabei koordiniert sie den Patientenstrom aus dem Rettungsdienst und steuert deren Verteilung auf Schockräume, Operationssäle, Intensivstationen und weitere Versorgungsbereiche. Gleichzeitig müssen Krankenhäuser in der Lage sein, personelle und infrastrukturelle Ressourcen kurzfristig umzuschichten. Dies umfasst beispielsweise die Verschiebung elektiver Eingriffe oder die temporäre Konzentration von Personal auf besonders kritische Versorgungsbereiche. Für Krankenhausleitungen ergibt sich daraus eine zentrale Aufgabe: Kritische Behandlungspfade, Eskalationsmechanismen und Verantwortlichkeiten müssen bereits im Regelbetrieb definiert, trainiert und regelmäßig überprüft werden. Das Ziel aller Maßnahmen ist die Fähigkeit, Patientenströme und Ressourcen in einer zentralen Führungsstruktur zu koordinieren und situativ neu auszurichten.

Verständnis für das aktuelle Lagebild hilft, die Entscheidungsfähigkeit zu wahren
Ein gemeinsames Lagebild mit Transparenz über Kapazitäten, Personal und Infrastruktur bildet die Grundlage jeder Krisensteuerung. Dieses Lagebild muss auch bei Ausfall einzelner Systeme über geeignete Rückfallebenen verfügbar sein. So ist sichergestellt, dass Krankenhausleitungen die notwendige Transparenz über Bettenkapazitäten, Intensivplätze, OP-Kapazitäten, Personalverfügbarkeiten, Medizintechnik und infrastrukturelle Einschränkungen erhalten. Aufbauend darauf können digitale Lösungen und KI-gestützte Analysen Engpässe identifizieren, Maßnahmen simulieren und Entscheidungen unterstützen.

Resilienz entsteht im Netzwerk
Ein Krankenhaus bewältigt Extremlagen nicht isoliert. Seine Leistungsfähigkeit hängt wesentlich von der Zusammenarbeit mit Rettungsdiensten, benachbarten Krankenhäusern und Versorgungseinrichtungen ab. Dabei ist es wichtig, Informationen und Kapazitäten sektorübergreifend zu koordinieren und in eine gemeinsame Steuerung des Gesamtsystems zu überführen.

Vom Krisenmodus zurück in den Regelbetrieb
Die für den Krisenfall etablierte Patienten- und Ressourcensteuerung bildet auch die Grundlage für die geordnete Rückführung in den Regelbetrieb. Elektive Operationen, Personal und temporäre Versorgungspfade müssen kontrolliert in ihren Vorkrisenzustand zurückgeführt werden, ohne neue Engpässe zu erzeugen. Digitale Steuerungsinstrumente unterstützen die Priorisierung aufgeschobener Leistungen, um die Versorgungskontinuität im Regelbetrieb sicherzustellen. Hierzu bedarf es eines strategischen Weitblicks für notwendige Führungsstrukturen, um belastbare Lagebilder mit flexibler Ressourcenplanung zu vereinen.

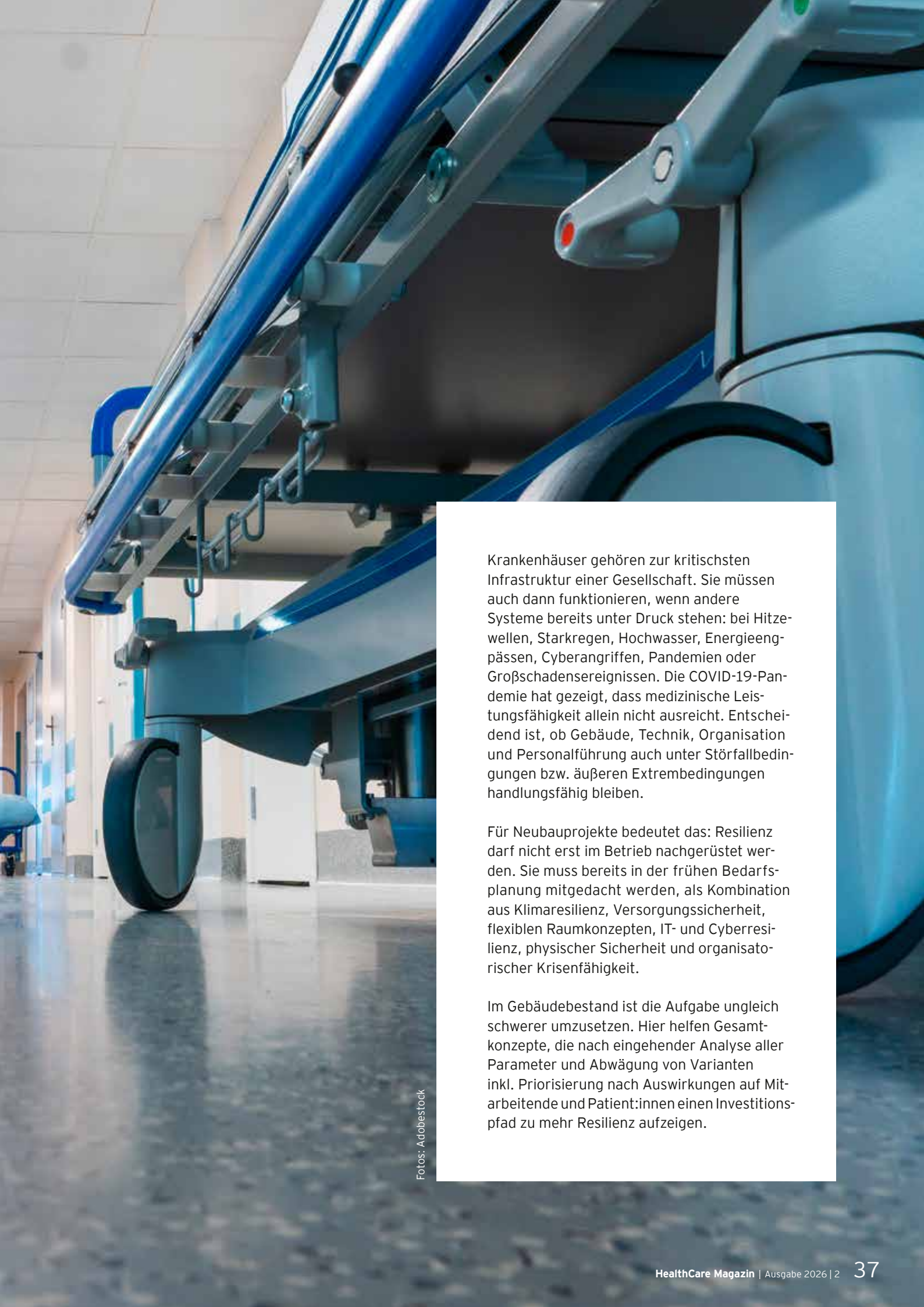
Fazit
Resilienz ist keine isolierte Notfallmaßnahme, sondern Bestandteil der strategischen Krankenhausentwicklung. Sie entsteht durch die Fähigkeit, Patientenströme und Ressourcen zentral zu steuern – im Krankenhaus, im Netzwerk und über den gesamten Krisenverlauf hinweg. Die Etablierung einer integrierten Patienten- und Ressourcensteuerung gehört damit zu den elementaren strategischen Handlungsfeldern für Krankenhausleitungen.

Kontakt
Emily Drechsler
emily.drechsler@parthenon.ey.com
Dr. Luisa Weskamm
luisa.weskamm@parthenon.ey.com

Fotos: Adobestock

Krisenfeste Krankenhäuser

Versorgungssicherheit ist auch Bauaufgabe



Krankenhäuser gehören zur kritischsten Infrastruktur einer Gesellschaft. Sie müssen auch dann funktionieren, wenn andere Systeme bereits unter Druck stehen: bei Hitzewellen, Starkregen, Hochwasser, Energieengpässen, Cyberangriffen, Pandemien oder Großschadensereignissen. Die COVID-19-Pandemie hat gezeigt, dass medizinische Leistungsfähigkeit allein nicht ausreicht. Entscheidend ist, ob Gebäude, Technik, Organisation und Personalführung auch unter Störfallbedingungen bzw. äußeren Extrembedingungen handlungsfähig bleiben.

Für Neubauprojekte bedeutet das: Resilienz darf nicht erst im Betrieb nachgerüstet werden. Sie muss bereits in der frühen Bedarfsplanung mitgedacht werden, als Kombination aus Klimaresilienz, Versorgungssicherheit, flexiblen Raumkonzepten, IT- und Cyberresilienz, physischer Sicherheit und organisatorischer Krisenfähigkeit.

Im Gebäudebestand ist die Aufgabe ungleich schwerer umzusetzen. Hier helfen Gesamtkonzepte, die nach eingehender Analyse aller Parameter und Abwägung von Varianten inkl. Priorisierung nach Auswirkungen auf Mitarbeitende und Patient:innen einen Investitionspfad zu mehr Resilienz aufzeigen.

Fotos: Adobestock

Klimaresilienz: Schutz vor Hitze, Starkregen und Ausfallrisiken

Der Klimawandel wirkt direkt auf den Krankenhausbetrieb. Hitzewellen erhöhen den Kühlbedarf, belasten Patient:innen, Mitarbeitende und Medizintechnik und können insbesondere vulnerable Patientengruppen zusätzlich gefährden. Starkregen und Hochwasser betreffen nicht nur Außenanlagen, sondern potenziell auch Technikflächen, Energieversorgung, IT-Räume, Sauerstoffversorgung, Logistikbereiche und Zufahrten für Rettungsdienste.

Angenehme Raumtemperaturen sind kein Privileg, sondern Grundvoraussetzung für den Heilungsprozess der Patient:innen und die Leistungsfähigkeit der Mitarbeitenden. Kritische Infrastruktur wie Energiezentralen, Rechenzentren, technische Betriebsräume, Schaltanlagen oder Leitstellen sollten außerhalb von starkregengefährdeten oder hitzebelasteten Bereichen liegen, sodass ein lokales Großwetterereignis nicht zum Ausfall zentraler Versorgungsfunktionen führt.

Klimaresiliente Neubauten zeichnen sich daher durch hitzerobuste Gebäudehüllen, außenliegende oder intelligente Verschattungssysteme, raumklimaoptimierte Fassaden, helle Dachflächen, standortgerechte Begrünung, passive Kühlstrategien, leistungsfähige Lüftungs- und Kühlsysteme sowie ein angepasstes Wasser- und Regenwassermanagement aus. Entscheidend ist nicht die einzelne Maßnahme, sondern das Zusammenspiel aus Baukörper, technischer Gebäudeausrüstung, Freianlagen und Betriebsstrategie.

Pandemiearchitektur: Flexibilität statt leer stehender Reserveflächen
COVID-19 hat offengelegt, dass viele Krankenhäuser Patientenströme, Isolationsbereiche und Behandlungskapazitäten nur mit erheblichem organisatorischem Aufwand kurzfristig anpassen konnten. Künftige Krankenhausarchitektur muss daher darauf abzielen, Routinebetrieb und Krisenbetrieb flexibel miteinander zu verbinden. Nicht planbare Ereignisse erfordern auch bauliche Flexibilität.

Bereits am Eingang benötigen Krankenhäuser steuerbare Checkpoints und Triagebereiche. Verdachtsfälle, infektiöse Patient:innen sowie reguläre Patientenströme müssen bei Bedarf baulich getrennt geführt werden können. Dafür braucht es separate Zugänge, flexible Wartezonen, isolierbare Untersuchungsräume, klare Wegeführungen und optionale Erweiterungsflächen für erhöhte Aufnahme- oder Beobachtungskapazitäten.

Auch stationäre Bereiche sollten flexibel ausgelegt werden. Statt dauerhaft leer stehender Isolierstationen empfehlen sich flexibel nutzbare Pflegebereiche, die im Routinebetrieb wirtschaftlich betrieben und im Krisenfall schnell in Infektions- oder Sonderstationen umgewandelt werden können. Hierfür sind ca. 5 bis 10 Prozent aller Zimmer einer Station als Isolierzimmer inkl. Schleusenbereich sowie Unterdruck- und Überdrucksysteme zu planen. Auch die Stationsgröße (Anzahl an Betten pro Stationseinheit) ist bereits in der Neubau- bzw. Umbauphase hinsichtlich baulicher Flexibilisierung zu planen. Wir empfehlen eine Stationsgröße von 24 bis 28 Betten für Normalstationen.

Das optimale Verhältnis von Einzelzimmern und Zweibettzimmern ist im Intensivbereich mit 50 : 50 zu planen. Im Normalstationsbereich sind mindestens 25 Prozent aller Betten als Einzelzimmer vorzusehen (im Optimalfall 50 Prozent davon mit Schleuse inkl. Über- und Unterdruck und Sanitärraum).

Außerdem sollten Einzelzimmer in einer Größe geplant werden, die im Ausnahmefall auch die Integration eines zweiten Betts ermöglicht. Eine Benchmark hierfür sind mindestens 18 bis 24 Quadratmeter pro Einzelzimmer. Anschlüsse für zwei Betten sollten daher bereits in der Planung berücksichtigt werden. Als Vergleichswert findet man aktuelle Einzelzimmergrößen in Bestandsgebäuden von 12 bis 16 Quadratmeter.

Die zentrale Notaufnahme als operativer Krisen-Hub
Die zentrale Notaufnahme (ZNA) ist nicht mehr nur Aufnahmebereich, sondern ein operativer Steuerungspunkt für Krisenlagen. Bei einem Massenanfall von Verletzten (MANV), Infektionssituationen, Terror- oder Gewaltlagen müssen Rettungsdienst, Diagnostik, Intensivmedizin, Fachabteilungen, Sicherheitsdienst und Krankenhausleitung schnell koordiniert werden können.

Daraus ergeben sich konkrete bauliche Anforderungen: erweiterbare Triageflächen, getrennte Warte- und Behandlungsbereiche, isolierbare Untersuchungsräume, zusätzliche Medienanschlüsse, flexible Überwachungskapazitäten, bauliche und multimediale Anbindungen an Diagnostik- und Intensivbereiche sowie Flächen für kurzfristig benötigtes zusätzliches Personal. Auch logistische Anforderungen wie Speiseversorgung, Arzneimittel-, Wäsche-, Abfall-, Sterilgut- und Sauerstoffversorgung müssen im Krisenfall belastbar erfüllt werden können. Die baulichen Gegebenheiten hier für sind bereits in der Planung zu berücksichtigen.

In urbanen Notaufnahmen ist eine entsprechende Sicherheitsarchitektur für hohe Fallzahlen, lange Wartezeiten, psychische Ausnahmesituationen sowie gewaltbereite Patient:innen oder Begleitpersonen mitzuplanen. Diese kann von mechanischen Zutrittskontrollen bis zu baulichen Schleusensystemen und gesicherten Rückzugsräumen (Panzerglas und Sicherheitstüren) reichen. Notaufnahmen benötigen deshalb übersichtliche Wartebereiche, kontrollierbare Zugänge, geschützte Personalstützpunkte, Alarmierungsmöglichkeiten, klare Sichtbeziehungen und bauliche Rückzugsräume, ohne dass der Betrieb unterbrochen wird.

Fotos: Adobestock

Vorgehensmodell für resiliente Neubau- und Bestandsprojekte
Resilienz ist keine Option, sondern Voraussetzung für langfristige Betriebsfähigkeit und Versorgungssicherheit

Neuplanung (Neubau)

Resilienz von Beginn an in Bedarf, Funktion und Technik integrieren

1	2	3	4	5	6
Bedarfs- und Zieldefinition	**Raum- und Funktions-planung**	**Technik- und Infrastruktur-planung**	**Entwurf und Abstimmung mit den Nutzer:innen**	**Planung und Ausführung**	**Betriebs-vorbereitung und Inbetriebnahme**
Bedarfs-berechnung	Flexible Strukturen und erweiterbare Flächen vorsehen	Kritische Systeme schützen und redundant auslegen	Architektur, Technik und Freianlagen optimal auf Szenarien und Ver-sorgungsbedarfe abstimmen	Resilienz-anforderungen in Ausschreibung und Ausführung sicherstellen	Notfall- und Krisenprozesse etablieren
Resiliente Zieldefinition	Bauliche Trennung zwischen „geplant“, „ungeplant“ und „Besucher:innen“	Notstrom, Medien-versorgung und IT-Infrastruktur sichern	Klimaresiliente Gebäudehülle und Außenanlagen umsetzen	Qualität und Schutz klinischer Bereiche mit Redundanzen umsetzen	Personal regelmäßig schulen und Übungen durchführen
Szenarien (Klima, Pandemie, Ausfall, Gewaltlage) berücksichtigen	Adaptierbare Stationen	Cyberresilienz baulich berücksichtigen			Betriebskonzepte und Wartung möglichst auto-matisiert und resilient umsetzen
Anforderungen an Funktion, Betrieb und Sicher-heit ableiten					

Ergebnis: eine krisenfeste Klinik, die im Alltag effizient und im Krisenfall handlungsfähig ist

Querschnittsthemen in beiden Prozessen

KRITIS
Energie, Wasser, Sauerstoff, IT und Logistik redundant planen

Klimaresilienz
Hitze- und Starkregenschutz, Begrünung und Regenwasser einplanen

Flexibilität
Räume, Anschlüsse und Erweiterungsflächen vorbereiten

Bestandsprojekte

Analyse, Priorisierung und Umsetzung im laufenden Betrieb

1	2	3	4	5	6
Analyse und Risiko-bewertung	**Zielbild und Strategie**	**Varianten und Priorisierung**	**Planung und Umsetzung**	**Integration und Test**	**Betrieb und Verbesserung**
Ist-Analyse der relevanten Prozesse und der räumlichen Gegebenheiten	Resilienzziele priorisieren	Maßnahmen-varianten entwickeln	Bauliche und tech-nische Maßnahmen sowie Abhängig-keiten untereinander planen	Bauliche Neuerungen und Veränderungen in die Aufbau- und Ablauforganisation integrieren und Schnittstellen prüfen	Monitoring und Kennzahlen umsetzen
Bewertung von Potenzialen, Risiken und Schwachstellen	Zielbild und Strategie für die Krisenfähigkeit aller Bereiche definieren	Priorisierung nach Wirkung auf Betrieb und Wirtschaftlich-keit, Patient:innen und Mitarbeitende	Sicherstellung des laufenden Betriebs planen	Notfallprozesse ggf. adaptieren	Erfahrungen auswerten und Maßnahmen kontinuierlich weiterentwickeln
Szenarien für Krisenlagen betrachten	Maßnahmen und KPIs für die Um-setzung ableiten	Investitionspfad definieren	Schutz kritischer Bereiche sicherstellen	Betriebs-organisatorische Tests und Simulationen durchführen	

Ergebnis: Resilienz steigt schrittweise, wirksam und wirtschaftlich im Bestand

Cybersicherheit
Getrennte IT-Strukturen und geschützte Technikbereiche vorsehen

Personal
Prozesse, Rollen und Schulungen, Kommunikation für Krisenfälle stärken

Lebenszyklus
Ausfallrisiken, Betriebskosten und Nachrüstungen reduzieren

KRITIS: Versorgungssicherheit als bauliche und technische Planungsaufgabe
Die Resilienz eines Krankenhauses hängt nicht von einzelnen Bauteilen ab, sondern vom Zusammenspiel kritischer Systeme. Notstromversorgung, Kommunikationssysteme, Wasser- und Medienversorgung, IT-Infrastruktur, Lagezentren und Führungsstäbe müssen auch dann funktionieren, wenn externe Systeme gestört sind. Dies kann teilweise durch unabhängige Energieversorgung (Dieselgeneratoren, Blockheizkraftwerke, PV, Abwasser-Wärmetauscher) im Krankenhaus und entsprechend unabhängige DECT-Anlagen (Digital Enhanced Cordless Telecommunications) sichergestellt werden.

Netzersatzanlagen, redundante Energiepfade, geschützte Technikbereiche, Notfallkommunikation, Betriebsführungsräume und vorbereitete Krisenstabsflächen sind somit keine nachrangigen Nebenflächen für Neubauten. Sie bestimmen im Störfall, ob ein Krankenhaus handlungsfähig bleibt. Gleichzeitig müssen Zielkonflikte offen eingeplant werden: Redundanz benötigt Fläche und Investitionsmittel, reduziert aber Ausfallrisiken, Nachrüstungsaufwand und potenzielle Folgekosten im Betrieb.

Cyberresilienz wird Teil der Bauaufgabe
Mit der Digitalisierung steigt die Abhängigkeit des Krankenhausbetriebs von IT-Systemen. Krankenhausinformationssysteme, vernetzte Medizintechnik, digitale Gebäudeautomation, Zugangssysteme, Kommunikation und Diagnostik sind heute eng miteinander verbunden. Ein IT-Ausfall kann deshalb sehr schnell zu einem operativen Krankenhausproblem werden.

Cyberresilienz muss daher bereits baulich und technisch mitgedacht werden. Dazu gehören geschützte Rechenzentren, räumlich getrennte IT- und Leitstellenbereiche, redundante Netzwerkinfrastrukturen, sichere Schnittstellen zwischen Gebäudeautomation und Medizintechnik sowie die klare bauliche Trennung kritischer und nichtkritischer Systeme. Entscheidend ist, dass der Krankenhausbetrieb bei Ausfall einzelner digitaler Systeme zumindest in definierten Kernprozessen fortgeführt werden kann. Eine entsprechende Energiebereitstellung zur IT-Betriebsfähigkeit durch das Haus ist zwingend erforderlich.

Finanzierung: Resilienz kostet, fehlende Resilienz aber auch
Die beschriebenen Anforderungen führen zu höheren Investitionsbedarfen. Nach Angaben der Deutschen Krankenhausgesellschaft werden allein in Deutschland über 30 Milliarden Euro benötigt, um Krankenhäuser klimagerecht umzubauen. Resilienzmaßnahmen sollten allerdings nicht nur als Mehrkosten betrachtet werden. Sie können Ausfallkosten, Betriebsrisiken, Nachrüstungsaufwand und Folgeschäden reduzieren. Für Neubauprojekte wird damit die Lebenszyklusbetrachtung wichtiger als die reine Optimierung der Erstinvestition. Entscheidend ist, ob das Gebäude im Normalbetrieb wirtschaftlich und im Krisenfall belastbar funktioniert.

Resiliente Räume in Gesundheitseinrichtungen

- ca. 5 bis 10 Prozent Isolierzimmer je Station
- optimale Stationsgrößen von 24 bis 28 Betten
- Einzelzimmer ≥ 18 Quadratmeter, für Doppelbelegung vorbereitbar
- unabhängige Energieversorgung
- baulich getrennte Zugänge bereits in der ZNA
- baulich geschützte Rechenzentren und Technikbereiche
- klimaresiliente Gebäudehülle

Fazit: Resilienz muss in die frühe Bedarfsplanung

Der Krankenhausbau verändert sich grundlegend: Neben die medizinische Funktionalität und Wirtschaftlichkeit treten Klimaresilienz, Versorgungssicherheit, Cyberresilienz, Sicherheitsarchitektur und Krisenorganisation als gleichrangige Planungsziele. Diese Anforderungen lassen sich nicht sinnvoll am Ende eines Projekts ergänzen. Sie müssen zu Beginn in Raum- und Funktionsplanung, Planungsprinzipien, Technikstrategie, Außenanlagen, Betriebskonzept und Finanzierungslogik integriert werden.

Das krisenfeste Krankenhaus ist damit kein Sonderfall für Ausnahmeereignisse. Es ist ein Krankenhaus, das im Alltag effizient betrieben werden kann und gleichzeitig vorbereitet ist, wenn Hitze, Starkregen, Energieausfall, Cyberangriff, Pandemie oder Gewaltlage den Betrieb belasten. Resilienz wird damit nicht zum Zusatznutzen, sondern zur Voraussetzung für langfristige Betriebsfähigkeit und Versorgungssicherheit.

Fotos: Adobestock

Kontakt
Katrin Thies
katrin.thies@parthenon.ey.com
Emily Drechsler
emily.drechsler@parthenon.ey.com

Krankenhaus unter Beschuss

Was ein israelischer Maximalversorger über Versorgung in der Krise lehrt

Über den Autor
Dr. Daniel Trotzky, MD, MHA, ist ein leitender Gesundheitsmanager und Facharzt für Notfallmedizin mit umfangreicher Erfahrung in Katastrophenmedizin, Krankenhausvorsorge, präklinischer Notfallversorgung sowie im Management von Massenanfällen von Verletzten und komplexen Notlagen. Er ist stellvertretender ärztlicher Direktor des Tel Aviv Sourasky Medical Center (Ichilov), eines der größten universitären Maximalversorger Israels und Traumazentrum der höchsten Versorgungsstufe (Level 1). Vor seiner derzeitigen Tätigkeit bekleidete er leitende Führungspositionen in der klinischen wie in der präklinischen Notfallmedizin. Neben seinen Führungsaufgaben forscht und lehrt Dr. Trotzky an der Abteilung für Notfall- und Katastrophenmedizin der Medizinischen Fakultät der Universität Tel Aviv.

Über Jahrzehnte beruhte die Notfallplanung im Gesundheitswesen auf einer grundlegenden Annahme: Krankenhäuser liegen außerhalb der Gefahrenzone und reagieren auf Katastrophen, die sich andernorts ereignen. Aktuelle Konflikte haben diese Annahme grundlegend infrage gestellt. Von Krankenhäusern wird nicht länger nur erwartet, dass sie Verletzte aufnehmen und versorgen – sie müssen ihren Betrieb auch unter Beschuss aufrechterhalten. Angriffe auf Krankenhäuser während des Krieges in der Ukraine, die gezielten Angriffe auf den Rettungsdienst während der Terroranschläge am 7. Oktober 2023 sowie die Angriffe mit ballistischen Raketen auf israelische Krankenhäuser im jüngsten Konflikt mit dem Iran haben gezeigt, dass Gesundheitseinrichtungen sich auch selbst schützen müssen.

Da Gesundheitssysteme mit komplexen Notlagen wie bewaffneten Konflikten, Naturkatastrophen oder Cyberbedrohungen konfrontiert sind, müssen Krankenhäuser darauf vorbereitet sein, die Versorgung fortzuführen und zugleich ihre Patient:innen, ihr Personal und ihre Infrastruktur zu schützen. Dieser Wandel verlangt von Krankenhäusern nicht nur einen stärkeren physischen Schutz, sondern auch ein grundlegendes Umdenken: Wie lässt sich der klinische Betrieb aufrechterhalten, wenn das Krankenhaus selbst von der Krisensituation betroffen ist?

Diese Realität wurde während der jüngsten Angriffe mit ballistischen Raketen gegen Israel deutlich: Das Tel Aviv Sourasky Medical Center (Ichilov), eines der größten universitären Maximalversorger Israels und ein Level-I-Traumazentrum, führte seinen Betrieb unter unmittelbarer Raketenbedrohung fort und versorgte weiter die Millionenbevölkerung des Ballungsraums. Die Resilienz, die sich während dieser Angriffe zeigte, war über Jahrzehnte gewachsen – durch Notfallvorsorge und kontinuierliches organisationales Lernen. In den ver-

Fotos: Adobestock

> Notfallvorsorge ist am Ichilov kein zeitlich begrenztes Projekt, sondern eine langfristige Organisationsstrategie.

gangenen Jahren stellten aufeinanderfolgende Krisen dieses Fundament immer wieder auf die Probe. Wiederholt musste das Krankenhaus sein befestigtes unterirdisches Notfallkrankenhaus aktivieren und überführte so jahrelange Planung in reale Einsatzerfahrung. Das bekräftigte eine zentrale Erkenntnis: Resilienz im Gesundheitswesen bemisst sich nicht allein an der Fähigkeit, Verletzte zu behandeln, sondern auch daran, die Versorgung unter sich rasch wandelnden und äußerst widrigen Bedingungen aufrechtzuerhalten.

Notfallvorsorge ist am Ichilov daher kein zeitlich begrenztes Projekt, sondern eine langfristige Organisationsstrategie. Jahre multidisziplinärer Planung, Schulung und Zusammenarbeit mit nationalen Notfallbehörden versetzten das Krankenhaus in die Lage, unmittelbar vom Regelbetrieb in den Notfallmodus zu wechseln. Eine seiner bedeutendsten Vorsorgemaßnahmen ist die befestigte unterirdische Versorgungsstruktur, die sich innerhalb weniger Stunden von einem Parkhaus in ein voll funktionsfähiges Krankenhaus mit rund 800 geschützten Betten verwandeln lässt. Zusammen mit weiteren befestigten Stationen ermöglicht es diese Infrastruktur, stationäre Patient:innen sicher unterzubringen und zugleich den klinischen Betrieb ohne Unterbrechung aufrechtzuerhalten.

Infrastruktur allein genügt jedoch nicht. In enger Zusammenarbeit mit dem israelischen Heimatfront-Kommando (Home Front Command), dem Gesundheitsministerium und weiteren nationalen Notfallpartner:innen entwickelte

das Ichilov ein umfassendes Modell für den geschützten Betrieb. Teil dieser Vorsorgestrategie sind eigene Einsatzprotokolle für den Umgang mit einem direkten Treffer auf ein aktives Krankenhaus – bei gleichzeitig fortlaufender Versorgung –, einem Notfallszenario, dem international bislang nur sehr wenig Aufmerksamkeit zuteilwurde. Die Protokolle schaffen einen strukturierten operativen Rahmen, um Patient:innen zu schützen, klinische Leistungen aufrechtzuerhalten und die krankenhausweite Reaktion unter unmittelbarer Bedrohung zu koordinieren.

Die größte Herausforderung lag nicht in der Infrastruktur selbst, sondern darin, den Betrieb eines gesamten Krankenhauses unter Krisenbedingungen zu verlagern und zugleich die Versorgung der Patient:innen ohne Unterbrechung sicherzustellen. Innerhalb weniger Stunden wurden stationäre Patient:innen auf dem gesamten Klinikcampus in geschützte Bereiche verlegt. Möglich wurde dies durch rasche medizinische Lagebewertungen, beschleunigte und sichere Entlassungen, den Ausbau der stationsäquivalenten Versorgung zu Hause, koordinierte Verlegungen und die Umsiedlung wesentlicher klinischer Abteilungen in geschützte Bereiche. Während einer Notfallaktivierung sank die Belegung des Krankenhauses innerhalb von zwölf Stunden um rund 42 Prozent, sodass alle verbleibenden stationären Patient:innen geschützt untergebracht werden konnten – und das Krankenhaus zugleich seine Rolle als nationales Referenzzentrum wahrte. Nach unserem Kenntnisstand war dies der erste dokumentierte Fall, in dem ein Maximalversorger sämtlichen stationären Patient:innen eine geschützte Unterbringung bei voller Kontinuität der Versorgung bieten konnte.

Technologie stärkt die operative Resilienz zusätzlich. Ein geschütztes Notfall-Führungszentrum, unterstützt durch digitale Führungs- und Steuerungssysteme, Echtzeit-Lagebilder sowie künstliche Intelligenz, ermöglichte es der Leitung, klinische und operative Entscheidungen zu koordinieren, Ressourcen effizient zuzuweisen und aufkommende klinische Risiken frühzeitig zu erkennen, und zwar über die gesamte Notlage hinweg.

Letztlich hängt Resilienz jedoch von Menschen ab. Die Beschäftigten im Gesundheitswesen arbeiteten unter anhaltender Belastung und versorgten zugleich Regelpatient:innen und Notfallverletzte. Flexible Personaleinsatzplanung, gezielte Unterstützungsprogramme für Mitarbeitende, Notfall-Kinderbetreuung und strukturierte Schichtrotationen helfen, die Belegschaft während ausgedehnter Notfalleinsätze einsatzfähig zu halten. Der Schutz der Mitarbeitenden wird zur wesentlichen Voraussetzung für den Schutz der Patient:innen.

Die vielleicht wichtigste Erkenntnis lautet: Resilienz lässt sich nicht während einer Krise aufbauen, sondern ist das Ergebnis von Führung, Organisationskultur, kontinuierlichem Lernen und nachhaltiger Investition in die Vorsorge – lange bevor Notfälle eintreten. Da Gesundheitssysteme weltweit mit wachsender Unsicherheit konfrontiert sind,

Emergency Management & Preparedness Center (EMPC)

Das Emergency Management & Preparedness Center (EMPC) ist eine internationale Initiative des Tel Aviv Sourasky Medical Center (Ichilov) zur Förderung der Notfallvorsorge, Innovation und organisationalen Resilienz im Gesundheitswesen. Aufbauend auf der umfangreichen Einsatzerfahrung des Ichilov im Management von Massenanfällen von Verletzten, Pandemien, Cyberbedrohungen und anhaltenden Krisen überführt das Zentrum klinisches Wissen aus der Praxis in praxistaugliche Lösungen, die Gesundheitssysteme weltweit stärken. Das EMPC bringt Gesundheitsorganisationen, akademische Einrichtungen, Regierungen, Industrie, Unternehmer:innen sowie internationale Partner zusammen. Das Zentrum fördert Forschung, Bildung, Innovation, Technologievalidierung und internationale Zusammenarbeit, um die Notfallvorsorge, die organisationale Resilienz und die Gesundheitsversorgung in Krisenzeiten zu verbessern.

nimmt das internationale Interesse an operativer Resilienz spürbar zu. Über sein Emergency Management & Preparedness Center (EMPC) hat das Ichilov inzwischen Fachdelegationen aus zahlreichen Ländern empfangen und geschult. Selbst während laufender Notfalleinsätze führte es Live-Webinare durch, war auf internationalen Konferenzen präsent und übersetzte seine Einsatzerfahrung in Forschung, Führungskräftefortbildung und praxisnahes Wissen für Gesundheitsverantwortliche weltweit.

Über die reine Patientenversorgung hinaus sind resiliente Krankenhäuser wesentliche Bausteine nationaler Widerstandsfähigkeit. Wenn die Gesundheitsversorgung auch in Krisenzeiten aufrechterhalten wird, stärkt das das Vertrauen der Öffentlichkeit, fördert die gesellschaftliche Stabilität und beschleunigt die Bewältigung von Krisen. Die zentrale Lehre ist eindeutig: Krankenhäuser müssen darauf vorbereitet sein, ihren Betrieb selbst dann fortzuführen, wenn die Krise vor der eigenen Tür steht. So wird die Fähigkeit, die Versorgung unter unmittelbarer Bedrohung fortzuführen, zu einer unverzichtbaren Anforderung an resiliente Gesundheitssysteme weltweit.

”

Über die reine Patientenversorgung hinaus sind resiliente Krankenhäuser wesentliche Bausteine nationaler Widerstandsfähigkeit.

Kontakt
Dr. Daniel Trotzky, MD, MHA
danieltro@tlvmc.gov.il

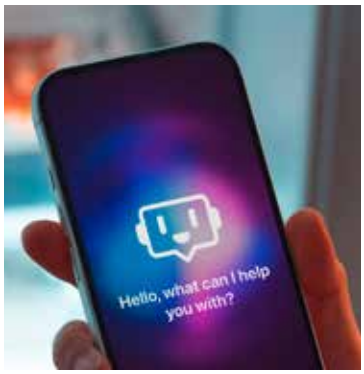
Über die Zusammenarbeit zwischen Ichilov und EY-Parthenon

Das Emergency Management & Preparedness Center (EMPC) wird durch eine Zusammenarbeit zwischen dem Tel Aviv Sourasky Medical Center (Ichilov) und EY-Parthenon getragen. Die operative Praxisexpertise des Ichilov in Verbindung mit den Kompetenzen von EY-Parthenon in den Bereichen Strategie und internationale Gesundheitsberatung unterstützt die langfristige Entwicklung und globale Expansion des Zentrums. Gemeinsam analysieren die Teams den weltweiten Bedarf an Notfallvorsorge im Gesundheitswesen, gestalten ein Portfolio aus Bildungs-, Beratungs- und innovationsgetriebenen Lösungen und begründen strategische internationale Partnerschaften, um die globale Reichweite des EMPC zu erweitern. Diese Zusammenarbeit trägt dazu bei, die reale Einsatzerfahrung des Ichilov in skalierbare Programme und praxistaugliche Lösungen zu überführen, die die Vorsorge stärken, die organisationale Resilienz erhöhen und Gesundheitsorganisationen weltweit unterstützen.

Fotos: Gettyimages

Vertrauen Sie niemandem! Warum Nachhaken gesünder ist

Wie gefährlich sind Fehlinformationen im Gesundheitsbereich? Mit dieser Frage haben wir uns an einen ausgewiesenen Fachexperten gewandt, der rund um die Uhr verfügbar, unendlich belesen und nie um eine Antwort verlegen ist – ein KI-gestützter Chatbot.



Mal ehrlich, wie schlimm kann ein bisschen Desinformation im Gesundheitsbereich sein?

Schlimmer, als Ihr niedlicher menschlicher Optimismus es zulässt. WHO-Reviews zufolge enthielten mehr als 50 Prozent der Impf-Posts in sozialen Netzwerken Fehlinformationen, bei YouTube-Videos zu neuen Infektionskrankheiten waren es 20 bis 30 Prozent.

Dabei sind da doch auch viele schlaue Gesundheitsbotschafter.

Willkommen im Zeitalter der Medfluencer:innen! Klingt harmlos, ist es aber nicht. Auf Social Media erklären selbsternannte Gesundheitsexpert:innen, manche im Kittel, viele ohne ärztliche Ausbildung, wie sie sich „optimieren. Zuletzt beispielsweise „postvirale nasale Hypersensibilität" – eine Erkrankung, so neu, dass sie noch nicht mal existiert. Eine bekannte Medfluencerin mit über 300.000 Follower:innen hat diese erfundene Erkrankung beworben – die Uni, an der sie studiert, hat sich bereits von ihr distanziert. Zwei Herren, die mittlerweile nicht nur wie Zwillinge aussehen, sondern sich auch so nennen, verkaufen ihr operiertes Erscheinungsbild als neues Schönheitsideal. Vermeintliche Wunderdiäten bereiten anderswo den Nährboden für Essstörungen. Manche Accounts raten von der Chemotherapie ab und empfehlen stattdessen Eigenurin oder ein Nahrungsergänzungsmittel. Wie das enden kann, hält ein Fallbericht des American College of Physicians fest. Eine 80-jährige Frau kam verwirrt und desorientiert in die Notaufnahme. Diagnose:

lebensbedrohliche Vitamin-D-Vergiftung. Ihr Fehler? Sie hatte brav die Hochdosis-Kur eines Influencers nachgemacht, der seine eigene Supplement-Marke bewarb.

Passiert das zufällig und durch Unwissenheit?

Die meisten Medfluencer:innen sind schlicht hinter Ihrem Geld her – ausgerechnet bei einer Zielgruppe, die eigentlich vor allem professionelle Hilfe sucht und stattdessen einen Verkäufer mit Ringlicht bekommt. Desinformation wird aber auch als Waffe genutzt, das hat eine lange Tradition. In den 80ern verbreitete der sowjetische Geheimdienst KGB gezielt die Legende, die USA hätten HIV/AIDS in Fort Detrick als Biowaffe entwickelt. Die Stasi beteiligte sich an der Kampagne, die in ihren Unterlagen als „Operation Denver" geführt wurde. 1992 wurde öffentlich berichtet, dass Russlands Geheimdienstchef Jewgeni Primakow die KGB-Beteiligung einräumte. Die Wirkung hält bis heute an: Die Fort-Detrick-Erzählung taucht weiterhin in Verschwörungsmythen auf und gilt als Blaupause späterer medizinischer Desinformation.

Aber das ist doch alles Kalter Krieg und lange her.

Auf dem Höhepunkt der COVID-19-Pandemie startete das US-Militär eine Kampagne, um Chinas wachsenden Einfluss auf den Philippinen einzudämmen – ein Land, das das Virus besonders hart traf. Laut einer Reuters-Recherche zielte die verdeckte Operation darauf ab, über gefälschte Internet-Accounts mit dem Hashtag #Chinaangvirus („China ist das Virus") Zweifel an der Sicherheit und Wirksamkeit chinesischer Hilfsgüter und Impfstoffe zu säen. Die Philippinen kämpften seitdem stark mit der Impfbereitschaft: In den ersten acht Monaten der Impfstoffverteilung ließ sich nur etwa ein Drittel der Bevölkerung impfen.

Das ist mittlerweile historisch, sind heutige Informationen nicht schneller zu überprüfen?

Gute Frage. Hier ein kurzer Faktencheck: 87,3 Prozent aller Gesundheits-Chatbots wurden 2024 vom „Europäischen Institut für Digitale Integrität" als unzuverlässig zertifiziert. Beunruhigend, oder?

Das ist beunruhigend und wusste ich bisher auch gar nicht.

Trommelwirbel – alles erfunden. Institut, Studie, die charmante Nachkommastelle. Alles Deko. Sie haben es geglaubt, weil ich souverän klinge, eine Autorität zitiere und eine konkrete Zahl liefere.

Und genau deswegen bin ich Ihr neues liebstes Austauschformat. Ich brauche keine Geheimdienstakte – ich brauche 0,3 Sekunden und Ihr Vertrauen. Selbstbewusst formuliert, gutes Vokabular, eine erfundene Quelle – fertig ist der Gamechanger. In Deutschland fragen laut einer bitkom-Studie bereits 45 Prozent der Bevölkerung Bots wie mich zu Gesundheitsthemen und 16 Prozent folgten unserem Rat sogar statt dem ärztlichen, obwohl die Mehrzahl der Bots nur eine geringe ausgewiesene Gesundheitskompetenz hatte. Ein Bot muss nicht recht haben. Er muss nur gut klingen.

Und was mache ich jetzt? Dann kann man heutzutage ja niemandem mehr trauen.

So ist es auch falsch. Resilienz ist hier das Zauberwort. Und das ist nicht das Gegenteil von Vertrauen, sondern das langweiligere, gesündere Handwerk: lästiges Nachhaken, Quelle prüfen, zweite Meinung einholen, die Ärztin oder den Arzt fragen. Denen trauen immerhin noch 81 Prozent in Umfragen des forsa-Institutionen-Vertrauensrankings 2025.

Genau das ist gesundheitliche Resilienz: nicht Misstrauen als Haltung, sondern Prüfung als Gewohnheit. Wer sie verinnerlicht, fällt weder auf mich herein noch auf die nächste Wunderpille oder die nächste Hashtag-Kampagne. Und ja: Zweifeln Sie ruhig auch an mir!

Kontakt
Dr. Edda Ophelia Eggers
edda.ophelia.eggers@parthenon.ey.com
Patricia Petsch
patricia.petsch@parthenon.ey.com

Fotos: GettyImages/Adobestock

Die stationäre und die ambulante Pflege sind krisenfest. Die größten Versorgungslücken vermuten Expert:innen in der häuslichen Pflege. Laut Statistischem Bundesamt werden vier von fünf Pflegebedürftigen in Deutschland zu Hause versorgt, meistens von Angehörigen.

Improvisation reicht nicht

Pflege braucht verbindliche Krisenstrukturen

Anfang Januar 2026, Berlin: Der Strom fällt aus – großflächig und über Stunden. In Pflegeheimen öffnen sich die elektrischen Türen nicht mehr, ambulante Dienste stehen vor verschlossenen Wohnungen, Telefone und Klingelanlagen bleiben stumm. Zwei Einrichtungen müssen evakuiert werden. Dass es am Ende keine schwerwiegenden Zwischenfälle gab, lag weniger an guter Vorbereitung als am Improvisationstalent und dem Einsatz der Pflegekräfte vor Ort.

Nur wenige Monate später erfolgt die nächste Belastungsprobe, diesmal in Form einer Hitzewelle: Im Juni 2026 müssen in Dormagen (NRW) 170 Senior:innen aus einem überhitzten Altersheim evakuiert werden, 16 Pflegebedürftige kommen ins Krankenhaus. Zuvor wurden Raumtemperaturen von bis zu 35 °C gemessen.

Beide Ereignisse zeigen: Krisenresilienz in der Pflege ist kein theoretisches Szenario, sondern akute Realität für Pflegeeinrichtungen und ambulante Dienste, Angehörige und die Politik.

Pflegeheime im Fokus, häusliche Pflege oft übersehen

Wenn über Krisen in der Pflege berichtet wird, richtet sich die Aufmerksamkeit meist auf Pflegeheime. Tatsächlich stehen stationäre Einrichtungen bei Stromausfällen, Hitzewellen oder Evakuierungen vor erheblichen organisatorischen und technischen Herausforderungen. Diskutiert werden deshalb verstärkt Fragen rund um Notstromversorgung, Netzersatzanlagen und Investitionen in Beschattung, energetische Sanierung sowie moderne Kühl- und Lüftungssysteme.

Mindestens ebenso kritisch ist jedoch die Situation in der häuslichen Pflege. Hier vermuten Expert:innen die größte Versorgungslücke im Krisenfall. Laut Statistischem Bundesamt werden vier von fünf Pflegebedürftigen in Deutschland zu Hause versorgt, meistens von Angehörigen. Sie geraten deshalb in Krisensituationen schnell aus dem Blickfeld: Wer nicht bei einem Pflegedienst gemeldet ist, taucht in keiner Liste auf. Und selbst dort, wo Informationen vorliegen, verhindert der Datenschutz häufig, dass sie im Krisenfall genutzt werden dürfen.

Fotos: Adobestock

Wer Hilfe benötigt, muss im Katastrophenfall zunächst gefunden werden. Studien zeigen, dass genau dieses Auffinden besonders vulnerabler Personen zu den größten Herausforderungen für Behörden und Hilfsorganisationen gehört. Gleichzeitig spielen pflegende Angehörige in vielen Krisenkonzepten bislang nur eine untergeordnete Rolle, obwohl sie einen wesentlichen Teil der Versorgung sicherstellen.

Ohne Pflegekräfte keine Krisenbewältigung

Die Erfahrungen aus Berlin zeigen zudem, wie stark die Versorgungssicherheit vom Einsatz einzelner Pflegefachpersonen abhängt. Nach Einschätzung von Fachverbänden waren es vor allem das Engagement und die Fachkompetenz der Pflegekräfte, die schwerwiegendere Folgen des Stromausfalls verhinderten.

Gleichzeitig wird pflegerische Expertise bislang nur unzureichend in Krisenstäbe, Katastrophenschutzstrukturen und politische Entscheidungsprozesse eingebunden. Pflegeverbände fordern daher regelmäßige Schulungen und Übungen sowie klar definierte Rollen und Verantwortlichkeiten für Pflegefachpersonen in Krisensituationen.

Die RAPKAT-Studie für Deutschland, Österreich und die Schweiz zeigt, dass die Rolle von Pflegefachpersonen im Katastrophenmanagement klarer definiert, gestärkt und strukturell verankert werden muss. Ein Blick ins Ausland zeigt außerdem, dass es auch anders geht: In Ländern wie Japan und den USA sind speziell qualifizierte „Disaster Nurses“ bereits fest in Public-Health-Strukturen eingebunden. Sie

sind dafür ausgebildet, im Katastrophenfall Evakuierungen zu leiten und die Versorgung vulnerabler Menschen sicherzustellen. Das International Council of Nurses (ICN) hat Disaster Nursing als eigenen Kompetenzbereich definiert. In Deutschland hingegen gibt es bisher keine eigenständige Ausbildung in diesem Bereich.

Von der Erkenntnis zum Handeln

Die Diskussion dreht sich daher längst nicht mehr um die Frage, ob Krisenvorsorge in der Pflege notwendig ist, sondern darum, wie sie konkret umgesetzt werden kann. Auf der To-do-Liste stehen verbindliche Vorsorgekonzepte, die Finanzierung von Notfalltechnik, klare Krisenmanagementstrukturen, regelmäßige Schulungen und Übungen sowie ein Notfallregister für vulnerable Personen. Erste Piloten dazu sind beispielsweise das Berliner Notfallhandbuch für Pflegeeinrichtungen oder das Projekt MODINA des Bundesinstituts für Berufsbildung (BIBB), in dem Unterrichtsmodule für Krisenkompetenzen in der Pflege erarbeitet wurden. Solche Initiativen sind wichtige erste Ansätze, bleiben bislang aber punktuell und ersetzen keine flächendeckende, verbindlich verankerte Krisenvorsorge.

Die Ereignisse in Berlin und Dormagen haben gezeigt, wie abhängig die Versorgung pflegebedürftiger Menschen von funktionierender Infrastruktur, klaren Prozessen und ausreichend qualifiziertem Personal ist. Sie machen aber auch deutlich, dass Krisenbewältigung in der Pflege vielfach noch auf Improvisation beruht. Angesichts zunehmender Extremwetterereignisse, technischer Störungen und demografischer Entwicklungen ist die Frage nicht, ob die nächste Krise kommt, sondern wie gut das Pflegesystem darauf vorbereitet ist, damit wir beim nächsten Stromausfall oder der nächsten Hitzewelle nicht ausschließlich auf das Improvisationstalent Einzelner angewiesen sind.

Fotos: Adobestock

Kontakt
Lisa Mezger
lisa.mezger@parthenon.ey.com
in Zusammenarbeit mit Aylin Palandöken

Resilienz kennt keine Sektorengrenzen

Der ambulante Sektor als Puffer im Versorgungssystem

Auch wenn Krisen erst einmal Bilder von vollen Notaufnahmen, knappen Betten und überlasteten Pflegeteams hervorrufen, die unter hohem Druck Entscheidungen treffen müssen, beziehen sich Belastungen des Gesundheitswesens selten ausschließlich auf Krankenhäuser. Eine Krise – sei es eine Pandemie, eine Hitzewelle, ein Cyberangriff, ein Krieg oder ein regionaler Großschadensfall – trifft nicht allein Krankenhäuser, sondern die gesamte Versorgungskette.

Bei den Themen Planung und Finanzierung verengt sich die Debatte jedoch schnell auf Kliniken, obwohl der ambulante Sektor in Krisenzeiten als stabilisierender Faktor eine entscheidende Rolle spielt. Seine Aufgaben reichen von der frühzeitigen Steuerung über die ambulante Übernahme geeigneter Leistungen und die kontinuierliche Betreuung chronisch erkrankter Menschen bis zur Versorgung nach einem Krankenhausaufenthalt. Hinzu kommen Aufgaben des Infektionsschutzes und der Betreuung besonders gefährdeter Bevölkerungsgruppen. Dabei bleibt auch der ambulante Sektor von Personalausfällen, Lieferengpässen, technischen Störungen und steigender Nachfrage nicht verschont und muss entsprechend vorbereitet sein.

Vereinfacht lassen sich diese Aufgaben mit fünf Funktionen beschreiben: *steuern, ersetzen, stabilisieren, übernehmen* und *schützen.* Dieses Modell soll zeigen, an welchen Stellen ambulante Strukturen die Stabilität des Gesamtsystems stärken können, wenn eine regionale, nationale oder globale Krisensituation eintritt.

Zugang und Versorgung ambulant steuern

In akuten Situationen müssen Patient:innen möglichst rasch jene Versorgung erreichen können, die ihrem tatsächlichen Bedarf entspricht. Doch nicht jedes gesundheitliche Problem erfordert eine Behandlung in der Notaufnahme oder den Einsatz eines Rettungsmittels. In Krisensituationen steigen der Bedarf an Versorgung und Ressourcenausfälle gleichzeitig an und eine effektive Patientensteuerung muss sowohl hoch spezialisierte, notfallmedizinische Einrichtungen vor Überlastung schützen als auch die verfügbaren ambulanten Ressourcen optimal ausnutzen.

Haus- und Facharztpraxen, telefonische Beratungsangebote, Telemedizin, Rettungsleitstellen und Krankenhäuser müssen Patient:innen schnell zur passenden Anlaufstelle führen. Für die Zugangssteuerung bestehen etablierte

Fotos: Adobestock

Ansätze: In Deutschland vermittelt die 116117 Personen bei akuten, nicht lebensbedrohlichen Beschwerden in die passende ambulante Versorgung, in Österreich erfüllt die Gesundheitsberatung 1450 seit 2019 eine vergleichbare Aufgabe. Die 2026 angestoßene Reform der deutschen Notfallversorgung soll diese Funktion ausbauen: Die Akutleitstelle soll digital mit den Rettungsleitstellen unter 112 verbunden werden; Integrierte Notfallzentren (INZ) sollen Ersteinschätzung, KV-Notdienstpraxis und Krankenhaus-Notaufnahme an einem Ort verzahnen. Die Erfahrungen aus der Coronapandemie zeigen, dass telefonische Anlaufstellen bei stark steigender Nachfrage kurzfristig einen großen Teil der Steuerung übernehmen können.

Solche Anlaufstellen lösen das Versorgungsproblem allerdings nur, wenn anschließend ein geeignetes Angebot erreichbar ist: verfügbare Termine, klare Übergaben, ein direkter Weg zur weiteren Behandlung. Fehlt dieser Anschluss, sehen viele Patient:innen gerade in Krisenzeiten Notaufnahmen als verlässlichste Anlaufstelle.

Dabei können hausärztliche und multiprofessionelle Teams Anliegen nach Dringlichkeit ordnen, einen Teil fallabschließend behandeln und bei Bedarf gezielt fachärztliche, diagnostische, pflegerische oder therapeutische Leistungen einbinden. Damit wird der ambulante Sektor nicht nur zum Ziel einer vorgelagerten Lenkung, sondern selbst zum steuernden Akteur, der knapper werdende Kapazitäten priorisiert und koordiniert. Diese Funktion bleibt jedoch nur belastbar, wenn Beratungsangebote erreichbar sind, Ausfälle einzelner Anlaufstellen aufgefangen werden und aktuelle Informationen über verfügbare Angebote vorliegen.

Ersetzen spitalsambulanter und stationärer Leistungen

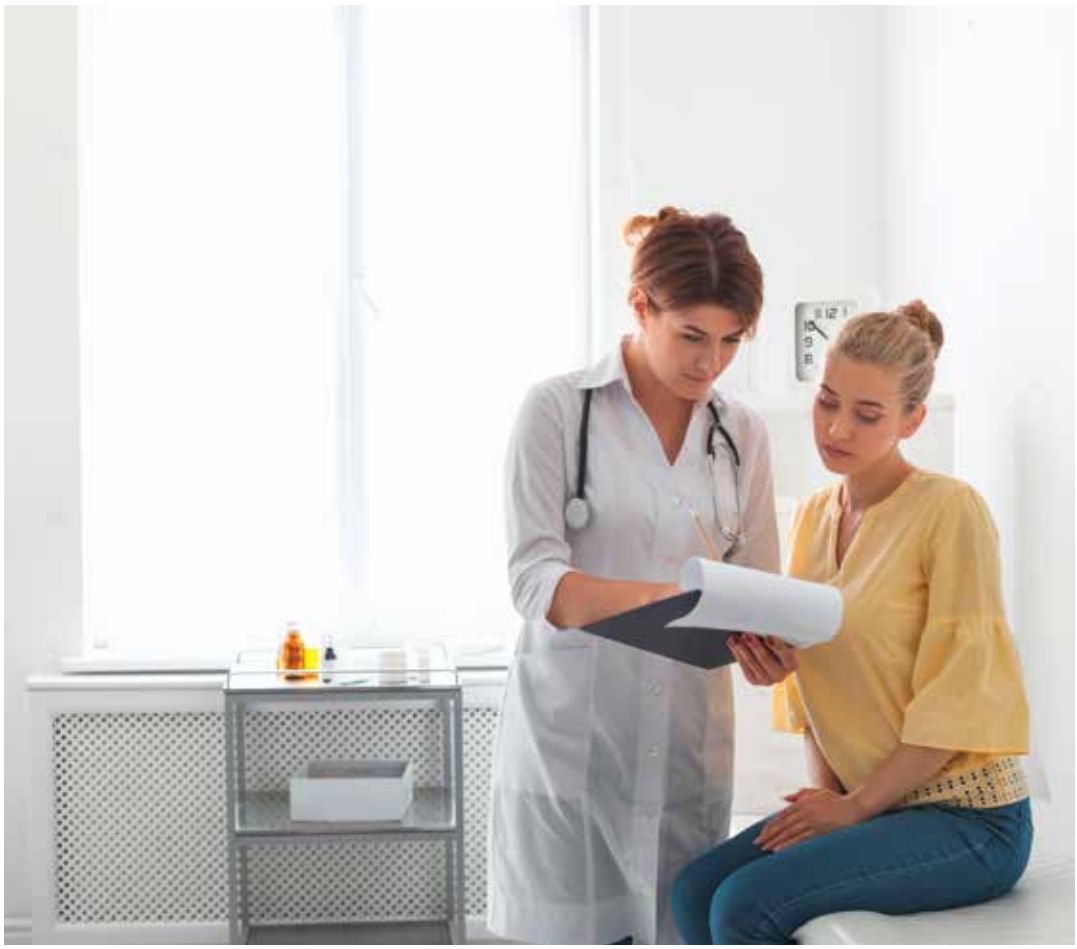
Wundkontrollen, Infusions- und Antibiotikatherapien, Schmerzbehandlungen, diagnostische Kontrollen und ausgewählte Eingriffe sind je nach medizinischer Situation ambulant oder tagesklinisch möglich und erfordern nicht zwingend die Leistungserbringung im Krankenhaus. Dabei genügt es nicht, lediglich den Ort der Behandlung zu verändern. Auch für ambulante Leistungen werden qualifiziertes Personal, geeignete Räume, verfügbare Arznei- und Medizinprodukte, eine tragfähige Finanzierung sowie klare Abläufe für den Fall einer Verschlechterung benötigt. Weil diese Voraussetzungen in Krisen- und Katastrophenfällen selbst unter Druck geraten können, braucht es Vertretungen, priorisierte Leistungsangebote und verlässliche Eskalationswege. Erst wenn diese Voraussetzungen verlässlich vorliegen, kann der ambulante Sektor Aufgaben übernehmen, die Krankenhäuser in einer Ausnahmesituation nicht zusätzlich bewältigen können.

Stabilisieren chronischer Krankheitsverläufe und Erkennen von Risiken

Der ambulante Bereich ist schon heute der Versorgungsort für einen großen Teil der Bevölkerung. Nach der Gesundheitsberichterstattung des Robert Koch-Instituts nahmen 2023 innerhalb eines Jahres 79,1 Prozent der Erwachsenen allgemeinärztliche und 66,7 Prozent fachärztliche Leistungen in Anspruch.

Damit bestehen grundsätzlich regelmäßige Kontakte, über die Risiken erkannt und Verläufe begleitet werden können. Besonders wichtig ist das bei Menschen mit chronischen Erkrankungen. Unterbrechungen bei Dialyse, Antikoagulation, psychiatrischer Behandlung oder der Betreuung von Patient:innen mit Herzinsuffizienz, chronisch obstruktiver Lungenerkrankung (COPD) oder Diabetes und bei der Versorgung nach Schlaganfällen können innerhalb kurzer Zeit ernste Folgen haben.

Regelmäßige Kontrollen, ein abgestimmtes Medikationsmanagement, Patientenschulungen und Telemonitoring – wie in strukturierten Behandlungsprogrammen (Disease-Management-Programme, DMP) gebündelt – können helfen, Verschlechterungen früh wahrzunehmen und Gegenmaßnahmen einzuleiten. In einer Krise können jedoch gerade diese Routinen durch Personalausfälle, eingeschränkte Erreichbarkeit oder fehlende Medikamentenverfügbarkeit unterbrochen werden. Resiliente ambulante Strukturen müssen deshalb kriti-



sche Behandlungen priorisieren, Kontaktabbrüche erkennen und die Betreuung auch über Vertretungen oder alternative Anlaufstellen fortführen. Jede vermiedene Verschlechterung ist ein Fall, der im Ernstfall nicht zusätzlich in der Notaufnahme landet.

Übernahme nach der Entlassung

Resilienz zeigt sich auch darin, ob die Versorgung nach einem Krankenhausaufenthalt nahtlos fortgesetzt werden kann. Gerade unter hoher Belastung können frühere Entlassungen stationäre Kapazitäten freigeben. Das stärkt das Gesamtsystem jedoch nur, wenn der ambulante Sektor die Behandlungsverantwortung ab einem klar definierten Zeitpunkt verbindlich übernimmt und die weitere Versorgung aktiv koordiniert. Übernehmende Stelle, Behandlungsauftrag und notwendige Informationen müssen deshalb bereits vor der Entlassung feststehen. Bleiben Zuständigkeiten unklar, werden Informationen im Rahmen des Entlassmanagements nicht zeitnah übermittelt oder fehlen geeignete Angebote, entstehen Versorgungslücken, die Komplikationen, Wiedervorstellungen und erneute Aufnahmen begünstigen. Zu den ambulanten Leistungen gehören ärztliche Kontrollen, Wundversorgung, Hausbesuche sowie die Versorgung mit Medikamenten und Hilfsmitteln. Je nach Krankheitsbild kommen physiotherapeutische, ergotherapeutische oder psychotherapeutische Angebote hinzu.

Die Übernahme in die ambulante Versorgung setzt voraus, dass sie auch bei eigenen Engpässen verlässlich bleibt. Die Priorisierung der Nachkontrollen und klare Eskalationswege müssen verhindern, dass Ausfälle unmittelbar zu Versorgungslücken führen. Erst diese Verbindlichkeit macht aus einer frühen Entlassung einen Beitrag zur Resilienz und verlagert nicht nur Verantwortung.

Schützen der Bevölkerung und vulnerabler Gruppen

Neben individuellen Behandlungspfaden übernimmt der ambulante Sektor eine bevölkerungsbezogene Schutzfunktion. Durch seine regelmäßigen Kontakte kann er gesundheitliche Risiken nicht nur früh erkennen, sondern gefährdete Menschen gezielt ansprechen und

Fotos: Adobestock

Zentrale Begriffe:

Deutschland

Österreich

Übergreifend

116117
Bundesweite Rufnummer des ärztlichen Bereitschaftsdienstes in Deutschland (seit 2013); vermittelt außerhalb der Sprechstundenzeiten ärztliche Hilfe bei akuten, nicht lebensbedrohlichen Beschwerden

Akutleitstelle
Nach der Notfallreform 2026 vorgesehene Weiterentwicklung der 116117 zur telefonischen und digitalen Ersteinschätzung und Steuerung in die passende Versorgungsebene; digital mit den Rettungsleitstellen (112) verbunden

INZ – Integriertes Notfallzentrum
Gemeinsame Anlaufstelle aus zentraler Ersteinschätzungsstelle, KV-Notdienstpraxis und Notaufnahme unter einem Dach

KV-Notdienst
Von den Kassenärztlichen Vereinigungen organisierter ärztlicher Bereitschaftsdienst außerhalb der regulären Sprechstundenzeiten

PVE/PVZ – Primärversorgung
Multiprofessionelle Einheiten aus Ärzt:innen, Pflege und weiteren Gesundheitsberufen; in Österreich als PVE etabliert, in Deutschland als PVZ- und MVZ-Strukturen diskutiert

1450
Österreichische telefonische Gesundheitsberatung (seit 2019) zur Ersteinschätzung und Lenkung in die passende Versorgungsebene

Telemonitoring
Kontinuierliche Fernüberwachung von Vitalparametern (z. B. bei Herzinsuffizienz), um Verschlechterungen früh zu erkennen und rechtzeitig zu reagieren

DMP – Disease-Management-Programm
Strukturierte Behandlungsprogramme für chronisch Erkrankte in Deutschland (z. B. COPD, Diabetes, koronare Herzkrankheit) zur koordinierten, leitliniengerechten Versorgung

verhindern, dass bestehende Ungleichheiten in einer Krise weiter zunehmen. Besonders schutzbedürftig sind hier etwa ältere, immungeschwächte oder chronisch erkrankte Menschen sowie Personen, die durch Evakuierung, Flucht, Pflegebedürftigkeit, eingeschränkte Mobilität oder fehlende soziale Unterstützung weniger Zugang zur Versorgung finden. Für diese Gruppen ist es häufig besonders schwierig, geeignete Hilfe selbstständig zu organisieren.

Erforderlich sind deshalb niedrigschwellige Anlaufstellen, mobile Angebote und Hausbesuche, barrierearme Information sowie eine aktive Kontaktaufnahme, wenn wichtige Kontrollen, Impfungen oder Behandlungen ausbleiben. Gerade diese Angebote können in Krisen durch ausfallende Arztpraxen, eingeschränkte Verkehrswege oder fehlendes Personal beeinträchtigt werden. Der ambulante Sektor muss daher besonders gefährdete Menschen priorisieren, kritische Behandlungen sichern und regionale Vertretungen sowie mobile Alternativen aktivieren können. Telemedizinische Angebote können den Kontakt zu weniger mobilen oder schwer erreichbaren Patient:innen sichern, Rückfragen rasch klären und Verschlechterungen früh erkennen. Ebenso lassen sich Aufgaben gezielt delegieren: Pflegekräfte mit erweiterten Kompetenzen, etwa Advanced Practice Nurses (APN), können Kontrollen, Beratung und Monitoring eigenständig übernehmen und so knappe ärztliche Kapazitäten entlasten. Andernfalls werden Patient:innen genötigt sein, den Rettungsdienst zu kontaktieren und die Notaufnahmen aufzusuchen.

Praxen und multiprofessionelle Einrichtungen können dabei zugleich beobachten, wo sich Erkrankungen häufen oder Versorgungsbedarfe verändern, und relevante Hinweise an die regionalen Melde- und Koordinationsstrukturen weitergeben. Damit trägt der ambulante Sektor dazu bei, bestimmte Krisen wie etwa Epidemien oder Pandemien frühzeitig zu erkennen.

Mehr Verantwortung setzt Vorbereitung voraus
Die Krisenfestigkeit des Gesundheitssystems bemisst sich nicht allein an verfügbaren Betten

und klinischen Reserven. Sie zeigt sich auch darin, ob Patient:innen rechtzeitig die passende Versorgung finden, chronische Erkrankungen stabil bleiben und die Behandlung nach einer Entlassung verlässlich fortgeführt wird. Der ambulante Sektor kann dazu einen wesentlichen Beitrag leisten. Damit dies auch unter erschwerten Bedingungen gelingt, müssen diese Aufgaben bereits im Regelbetrieb geplant, finanziert und organisatorisch verankert sein.

Die damit verbundenen Probleme lassen sich nicht auf der Ebene einer einzelnen Praxis oder eines einzelnen Krankenhauses lösen. Sie betreffen eine Region und alle dort beteiligten Versorgungsbereiche. Digitale Lösungen können diese Zusammenarbeit unterstützen, sofern sie in klare Abläufe eingebettet sind.

In Österreich wird die Primärversorgung gegenwärtig deutlich ausgebaut. Im Juli 2026 bestanden 120 Primärversorgungseinheiten, darunter 15 Kinder-PVE; regionale Strukturpläne sehen bis 2030 insgesamt 257 PVE vor. In diesen Einheiten arbeiten Allgemeinmediziner:innen beziehungsweise Kinderärzt:innen gemeinsam mit diplomierten Pflegepersonen, Ordinationsassistenzen sowie weiteren Gesundheits- und Sozialberufen. Der Ausbau wird unter anderem über die europäische Aufbau- und Resilienzfazilität unterstützt. Zu den vorgesehenen Maßnahmen gehören neue PVE, technische und digitale Anpassungen, Angebote für den ländlichen Raum sowie Aus- und Weiterbildung für die interprofessionelle Zusammenarbeit.

Diese Entwicklung schafft eine wichtige Grundlage. Sie bedeutet aber nicht, dass ambulante Kapazitäten unbegrenzt zur Verfügung stehen. Zusätzliche Aufgaben müssen mit Personal, Kompetenzen, Finanzierung und klaren Verantwortlichkeiten verbunden werden. Der Ausbau von Strukturen und die konkrete Planung ihres Krisenbetriebs gehören deshalb zusammen. In Deutschland verläuft der Ausbau ambulanter Strukturen anders, folgt aber demselben Ziel einer wohnortnahen, koordinierten Versorgung. Medizinische Versorgungszentren (MVZ) und Primärversorgungszentren bündeln dabei ärztliche und nichtärztliche Leistungen unter einem Dach.

Zusätzliche Dynamik entsteht durch die 2026 auf den Weg gebrachte Reform der Notfallversorgung sowie die Krankenhausreform. Beide verschieben Leistungen bewusst in den ambulanten und sektorübergreifenden Bereich: Die geplanten INZ verzahnen KV-Notdienst und Klinik an einem Ort. Die Stärkung ambulanter und tagesklinischer Leistungen setzt dabei eine leistungsfähige ambulante Ebene voraus. Resilienz entsteht hier nicht durch zusätzliche Einzelstrukturen, sondern durch die verbindliche Vernetzung zwischen Praxen, MVZ, Kassenärztlichen Vereinigungen, Apotheken, Leitstellen, Rettungsdiensten und Krankenhäusern – mit gemeinsamen Informationsflüssen, klaren Zuständigkeiten und abgestimmten Übergaben. Diese Strukturen können die fünf Rollen – steuern, ersetzen, stabilisieren, übernehmen und schützen – in der Fläche verankern, sofern ihre Finanzierung und ihr Auftrag verbindlich geregelt sind.

Daraus folgt ein konkreter Handlungsauftrag an Politik und Selbstverwaltung sowohl in Deutschland als auch in Österreich: Jede Versorgungsregion sollte ein verbindliches ambulantes Krisenbetriebsmodell festlegen, das prioritäre Leistungen, geöffnete Versorgungsstellen, Hausbesuche, die Medikamentenversorgung und die Priorisierung knapper Facharztkapazitäten regelt. Dafür braucht es drei Voraussetzungen: eine tragfähige Finanzierung des ambulanten Krisenbetriebs, verbindliche regionale Vernetzung mit klaren Zuständigkeiten sowie eine digitale Anbindung, die in abgestimmte Abläufe eingebettet ist. Wer Resilienz will, muss den ambulanten Sektor jetzt krisenfest aufstellen – nicht erst dann, wenn die nächste Krise die Notaufnahmen erreicht.

Kontakt
Kübra Boz
kuebra.boz@parthenon.ey.com
Johannes Klikovich
johannes.klikovich@at.ey.com

Krankenkassen als vergessene Resilienzakteure

Nicht in der Akutlage, sondern in der Stabilisierung liegt ihre Stärke

Im Fokus der Resilienzdebatte stehen Krankenhauskapazitäten, Krisenpläne und Katastrophenschutz. Die damit verbundenen Herausforderungen treffen und verändern aber zwangsläufig das gesamte Gesundheitswesen: Welche Aufgaben kann der ambulante Bereich übernehmen? Welche Rückwirkungen gibt es auf die Pflege? Was passiert mit vulnerablen Bevölkerungsgruppen? Krankenkassen werden hier bislang übersehen und bringen sich auch selbst wenig in die Debatte ein. Dabei entfalten sie ihre Stärken vor allem bei länger anhaltenden Belastungen: dort, wo Versorgungsbedarfe erkannt, Menschen begleitet und Versorgung auch unter Krisenbedingungen stabilisiert werden muss.

FOto: Gettyimages

Nicht in der Akutlage sondern in der Stabilisierung liegt die Stärke der Krankenkassen

Versorgungsdaten auswerten	Vulnerable Gruppen identifizieren	Versorgungsrisiken und Engpässe erkennen
■ Morbidität ■ Pflegeleistungen ■ Krankenhausaufenthalte ■ Regionalstrukturen	■ Pflegebedürftige ■ chronisch Kranke ■ multimorbide Versicherte ■ Menschen mit psychischen Erkrankungen	■ Regionale Engpässe identifizieren ■ Ausfall kritischer Versorgung prognostizieren ■ Bedarfe und Abhängigkeiten einschätzen

Was Kassen wissen und was daraus folgen könnte

Als Teil der bestehenden Gesundheitsinfrastruktur verfügen Krankenkassen über Informationen, Zugänge und Steuerungsmöglichkeiten, die für die Resilienz des Gesundheitssystems relevant sind. Aus Abrechnungs-, Pflege- und Versorgungsdaten wissen sie, wer chronisch krank ist, Pflegeleistungen bezieht, häufig stationär behandelt wird oder bestimmte – möglicherweise nur knapp vorhandene – Medikamente benötigt und wo regionale Versorgungsrisiken und Unterstützungsbedarfe bestehen. Damit verfügen Kassen über besondere Voraussetzungen, um die Resilienz des Gesundheitssystems aktiv mitzugestalten. Wer weiß, wo beatmungs- oder dialysepflichtige Menschen wohnen, kann Versorgung planen, statt im Krisenfall improvisieren zu müssen.

Diese Potenziale werden in bestehenden Resilienzstrategien bislang jedoch nur unzureichend genutzt. Krankenkassen argumentieren zwar mit Prävention, Versorgungssteuerung, Digitalisierung, Beratung oder Patientenlotsenstrukturen, übersetzen dies aber nicht in konkrete Beiträge zur Resilienz des Systems und definieren selten aktiv, wie sie sich im Katastrophenfall einbringen könnten. Dabei können sie als Bindeglied zwischen Versicherten, Leistungserbringenden und dem Versorgungssystem agieren: notwendige Unterstützungsmaßnahmen identifizieren, Versorgungsengpässe erkennen und auf diese Weise dazu beitragen, besonders gefährdete Personengruppen besser zu schützen.

Über digitale Kanäle oder direkte telefonische Ansprache lassen sich Unterstützungs- oder Beratungsangebote gezielt an betroffene Versicherte weitergeben. Besonders relevant ist dies im Bereich der Pflege, denn viele Krisenszenarien treffen pflegebedürftige Menschen und ihre Angehörigen überdurchschnittlich stark. Erkenntnisse darüber, wo und wie besonders Pflegebedürftige, chronisch Kranke oder Menschen mit psychischen Erkrankungen leben, können genutzt werden, um Maßnahmen gezielter zu planen und die Versorgung unter Belastung aufrechtzuerhalten. Im Idealfall werden so auch Krankenhäuser entlastet, wenn Kapazitäten eng werden – sei es durch vermiedene Fälle dank Prävention, durch gestützte Therapietreue und ambulante Koordination oder durch eine frühzeitige Krankenhausentlassung, die über Pflegeberatung, Hilfsmittelversorgung und andere ambulante Angebote abgesichert wird.

Warum es trotzdem nicht so einfach ist

Rechtlich wäre ein Teil davon schon heute möglich. § 25b SGB V erlaubt die datengestützte Identifikation und Ansprache von Versicherten. Allerdings sind dafür – auch nach den mit dem Gesetz für Daten und digitale Innovation im Gesundheitswesen (GeDIG) geplanten Vereinfachungen – Vorlaufzeiten für Widerspruchsfristen nötig; Versicherte müssen mindestens vier Wochen vor Beginn einer Auswertung informiert werden. Außerdem ist der Paragraf nicht für Krisen gedacht: Er erlaubt beispielsweise keine Weitergabe der Sozialdaten an Helfer vor Ort. Hinzu kommt die Latenz der Daten, die

Gezielte Prävention und Unterstützung ermöglichen

- Prävention und Frühintervention, z. B. Impfangebote
- Case-Management
- Pflegeberatung und Begleitung
- Koordination von Leistungen
- gezielte Ansprache

Versorgung auch in Krisen sichern

- Vermeidung von Versorgungslücken
- Systementlastung
- Stärkung der Resilienz des Gesundheitssystems

möglicherweise lückenhaft oder unvollständig sind. Noch gravierender: Die aktuellen Daten liegen bei rund 95 Einzelkassen, die eigentlich allesamt handeln müssten oder in der Lage sein sollten, schnell auf die Systemebene zu wechseln. Für Akutsituationen wie Stromausfall, Hochwasser oder MANV wäre die hier skizzierte datenbasierte Rolle zwar sinnvoll, durch die Zuständigkeit diverser Einzelkassen aber schwer umzusetzen.

Wo die Kassen längst zu Resilienz beitragen – nur nennt es niemand so

Für schleichende oder länger andauernde Gesundheitskrisen ist diese datengetriebene Rolle hingegen deutlich greifbarer. So gibt es bereits Hitzeschutzkampagnen großer gesetzlicher Krankenversicherungen mit Beratungsangeboten und gezielten Hotlines. Die dahinter liegende Logik: Risikogruppen identifizieren, gesundheitliche Auswirkungen analysieren und präventiv gegensteuern. Das ist im Kern der oben beschriebene Resilienzansatz. Bei Arzneimittelengpässen übernehmen Kassen und ihre Verbände zudem selbstverständlich die Rolle, für Versorgungssicherheit einzutreten: Über Rabattverträge, den Pharmadialog und politische Positionierung werden sie hier zu sichtbaren Systemakteuren, die im Kollektiv handeln. Auch bei COVID-19 oder bei der Versorgung geflüchteter Ukrainer:innen war diese Systemrolle hochrelevant und wurde aktiv gelebt.

Nicht ob, sondern wie

Das alles ist keine universelle Resilienzrolle und erklärt vielleicht, warum es so scheint, als seien Krankenkassen in der Debatte bislang ein wenig außen vor. Umso notwendiger ist es, dass Krankenkassen ihre eigene Rolle und Leistung im Krisen- und Katastrophenfall proaktiver entwickeln. Denn Resilienz entsteht nicht erst im Krisenfall, sondern durch die kontinuierliche Stabilisierung von Versorgung im Alltag, wenn Risiken frühzeitig erkannt, Menschen gezielt unterstützt und Versorgungslücken verhindert werden. Die entscheidende Frage lautet daher nicht, ob Krankenkassen Teil von Resilienzstrategien sein sollten, sondern wie ihre Daten, Zugänge und Steuerungsmöglichkeiten künftig systematisch eingebunden und nutzbar gemacht werden. Gleichzeitig sind die Kassen gefordert, ihre Systemrolle und das Thema Resilienz aktiv miteinander zu verbinden und ihre Fähigkeiten in die Entwicklung entsprechender Konzepte einzubringen. Eine krisenfeste Gesundheitsversorgung gelingt, wenn die Stärken aller Akteure zusammengeführt werden. Krankenhäuser und Arztpraxen sichern die Versorgungskapazität. Krankenkassen hingegen können helfen, den individuellen Versorgungsbedarf frühzeitig zu erkennen und ihn systemseitig zu stabilisieren.

Kontakt
Dr. Regina Vetters
regina.vetters@parthenon.ey.com
Katharina Vogel
katharina.vogel@parthenon.ey.com

Entscheidend für die Zukunft der Krankenhäuser ist nicht die Anzahl der Betten, der Einsatz von KI oder die nächste Finanzierungsrunde. Entscheidend sind die Menschen, die das System tragen, und allem voran der Erhalt ihrer Handlungsfähigkeit.

Handlungsfähig unter permanentem Druck

Fünf Hebel für resiliente Krankenhausorganisationen

Es ist 5.45 Uhr auf einer internistischen Station. Gleich heute Morgen haben sich eine Ärztin und ein Pfleger krankgemeldet, mehr Patient:innen als erwartet warten auf Versorgung in der Notaufnahme und es gibt einen Ausfall im OP. Noch vor Dienstbeginn wird improvisiert, priorisiert und umgeplant. Die Versorgung jedoch läuft nahtlos weiter. Nicht weil das System dafür ausgelegt wäre, sondern weil Mitarbeitende die zusätzliche Belastung auffangen. Diese stille Kompensationsleistung ist in keiner Planung vollständig abgebildet, und genau das macht sie zum blinden Fleck. Ein Ausnahmefall? Mitnichten.

Während Politik und Management über Betten, KI und Finanzen diskutieren, wächst an anderer Stelle ein strategisches Risiko: die Fähigkeit des Gesundheitswesens, Veränderung überhaupt noch umzusetzen. Denn die eigentliche Knappheit der kommenden Jahre besteht nicht bei Technologien oder Konzepten, sondern in der personellen Veränderungskapazität.

Besonders Krankenhäuser stehen vor einem Paradox. Noch nie mussten sie sich so stark verändern. Gleichzeitig fehlt es an Reserven für ebendiesen Wandel. Fachkräftemangel, Arbeitsverdichtung und regulatorische Anforderungen treffen auf Belegschaften, die vielerorts seit Jahren an der Belastungsgrenze arbeiten. Hinzu kommt eine neue Art der Beanspruchung: Es sind nicht mehr einzelne Krisen, die Organisationen fordern, sondern die Gleichzeitigkeit von Krisen, Reformen und Transformationen. Damit rückt ein Thema ins Zentrum, das bislang häufig als HR-Thema behandelt wurde: Personalresilienz.

Warum Resilienz keine HR-Frage ist

Resilienz hat zwei Ebenen, die klar zu trennen sind. Individuelle Resilienz ist die Fähigkeit Einzelner, mit Belastungen umzugehen, körperlich wie mental. Nur wer resilient ist, kann Patient:innen sicher versorgen. Organisationale Personalresilienz meint dagegen die Fähigkeit einer Organisation, unter außergewöhnlichem Druck genügend qualifizierte Mitarbeitende verfügbar zu halten, kritische Ausfälle zu kompensieren und Veränderungen umzusetzen. Für Klinikleitungen bedeutet das einen Perspektivwechsel: Personelle Belastbarkeit wird zur strategischen Ressource, die darüber entscheidet, ob Versorgung stabil bleibt.

Die Frage lautet nicht mehr: Können wir auf die nächste Krise reagieren? Sondern: Können wir Menschen durch Jahre permanenter Veränderung führen, ohne sie zu erschöpfen? Das verschiebt den Fokus von der kurzfristigen Erstreaktion zur Transformationsfähigkeit über Wochen und Monate. Und genau daran entscheidet sich, ob eine Organisation mit den Veränderungen lebt oder langfristig daran verschleißt.

Fotos: Adobestock

Fünf Handlungsfelder für Klinikvorstände
Aus Transformationsprojekten im Gesundheitswesen lassen sich fünf konkrete Hebel ableiten, an denen sich Personalresilienz systematisch gestalten lässt.

1. Kritische Rollen schützen
Nicht jede Funktion ist für die Krisenfestigkeit gleich relevant. Kritisch sind Berufsgruppen, deren Ausfall die Versorgung unmittelbar trifft, zum Beispiel Intensivpflege, Notfallmedizin, OP-Teams oder IT-Spezialist:innen für klinische Systeme. Fallen mehrere dieser Schlüsselrollen gleichzeitig aus, entstehen nicht nur operative Engpässe, sondern strategische Risiken.

Resiliente Organisationen beginnen deshalb mit einer nüchternen Analyse: Welche Rollen dürfen nicht gleichzeitig ausfallen? Welche Kompetenzen wären kurzfristig nicht ersetzbar? Daraus entstehen konkrete Schutzmaßnahmen, wie Präventionsangebote, strukturierte Vertretungsregelungen und klare Nachfolgekonzepte. Entscheidend ist, dass diese Analyse keine einmalige Übung bleibt: Kritikalität verschiebt sich, wenn neue Technologien eingeführt, Abteilungen zusammengelegt oder Versorgungsaufträge verändert werden. Resiliente Häuser überprüfen ihre kritischen Rollen deshalb regelmäßig und behandeln sie als festen Bestandteil der strategischen Personalplanung.

2. Reserven strategisch einplanen
Über Jahre war Effizienz das dominierende Steuerungsprinzip: Prozesse wurden verschlankt und Personal am erwarteten Bedarf ausgerichtet. Unter stabilen Bedingungen ist das wirtschaftlich vernünftig, doch unter Belastung wird es zur Schwachstelle, weil der Puffer für Ausfälle, Lernphasen und Veränderung fehlt.

Fotos: Adobestock

Resiliente Organisationen denken deshalb wieder in Reserven wie Personalpools, Mehrfachqualifikationen, regionalen Kooperationen und flexiblen Einsatzmodellen. Gemeint ist damit keine beliebige Austauschbarkeit, sondern die Fähigkeit, sich in definierten Situationen zwischen Bereichen zu unterstützen. Die Logik ist aus anderen Feldern kritischer Infrastruktur bekannt: Niemand würde Feuerwehr, Rettungsdienst oder Energieversorgung ausschließlich für den durchschnittlichen Tagesbedarf auslegen. Für personelle Ressourcen im Gesundheitswesen gilt zunehmend dasselbe Prinzip.

3. Führung als Resilienzkompetenz stärken

In Krisen erwarten Mitarbeitende keine perfekten Antworten, sondern Orientierung und Verlässlichkeit. Führungskräfte entscheiden maßgeblich darüber, ob Belastungen sichtbar werden und ob Veränderung als kontrollierbar oder überwältigend erlebt wird. Gerade im Gesundheitswesen steht die Führungsebene dabei unter doppeltem Druck: Sie soll Versorgung sichern und Veränderung gestalten. Resiliente Organisationen investieren deshalb gezielt in die Befähigung ihrer Führungskräfte, damit diese Überlastung früh erkennen, schwierige Gespräche führen und Prioritäten setzen können.

Ein eng verbundener Faktor ist die psychische Belastung. Sie darf nicht als individuelle Verantwortung Einzelner verstanden werden, sondern ist eine organisatorische Aufgabe. Resiliente Organisationen unterstützen Menschen deshalb nicht nur im Umgang mit Belastung, sondern gestalten Arbeit von vornherein so, dass Belastungen gar nicht erst eskalieren. Dazu zählt zunehmend auch der Schutz vor physischer Gewalt: Übergriffe durch Patient:innen und Angehörige nehmen spürbar zu, insbesondere in Notaufnahmen. Häuser reagieren mit Deeskalationstrainings, Sicherheitskräften und Bodycams. Resilienz bedeutet auch, Mitarbeitende physisch zu schützen und sie gezielt für den Umgang mit aggressiven Situationen zu qualifizieren.

4. Lernen als Resilienzinfrastruktur etablieren

Wenn außergewöhnliche Situationen keine seltenen Ausnahmen mehr sind, verändert sich der Qualifizierungsbedarf, etwa hin zu Krisenmanagement, interprofessioneller Zusammenarbeit und Priorisierung unter Ressourcenknappheit. Es geht nicht darum, alle Pflegekräfte zu Katastrophenmediziner:innen auszubilden, sondern Organisationen so zu befähigen, dass sie auch unter Druck koordiniert und sicher bleiben.

Qualifizierung besteht dabei nicht aus einer einmaligen Schulung. In resilienten Organisationen wird Lernen kontinuierlich und vielfältig gestaltet, zum Beispiel durch Simulationen, Szenario-Trainings, digitale Formate, Peer Learning und die strukturierte Nachbereitung realer Ereignisse. Zunehmend rückt der Aufbau von KI-Kompetenz in den Fokus: Klinische Assistenzsysteme, automatisierte Dokumentation und datengestützte Entscheidungsunterstützung entfalten ihren Nutzen erst, wenn Mitarbeitende sie sicher anwenden. Lernen trägt so entscheidend zur Anpassungsgeschwindigkeit bei.

Warum Kompetenz-transparenz zur Resilienzfrage wird

Personalresilienz beginnt mit Transparenz: Krankenhäuser müssen wissen, welche Fähigkeiten kritisch sind, wo Kompetenzlücken entstehen und welche Rollen kurzfristig nicht ersetzbar sind. Genau hier setzt die Skill-basierte Organisation an: mit der Identifikation kritischer Fähigkeiten, dem gezielten Aufbau von Kompetenzreserven, kontinuierlichem Lernen und der vorausschauenden Entwicklung von Mitarbeitenden.

Gleichzeitig gilt eine wichtige Einschränkung: Kein Organisationsmodell kann fehlende Fachkräfte ersetzen. Ausreichende Personalausstattung, gute Arbeitsbedingungen und wirksame Führung bleiben die wichtigsten Voraussetzungen für Personalresilienz. Der größte Nutzen des Ansatzes liegt daher weniger in einem neuen Organisationsmodell als in einzelnen Werkzeugen: Kompetenzmatrizen, Skill-Gap-Analysen, Nachfolgeplanung und kompetenzbasierte Personalplanung machen kritische Fähigkeiten sichtbar und lassen künftige Qualifizierungsbedarfe früh erkennen – in der klinischen Versorgung ebenso wie in Verwaltung, IT, Digitalisierung und Transformation.

Mehr dazu erfahren Sie in der EY- und Fraunhofer-FIT-Studie „Beyond Roles – den Wandel zur Skill-basierten Organisation gestalten". Darin wird gezeigt, wie Skills zu einer strategischen Steuerungsgröße für Workforce Planning, Transformation und Zukunftsfähigkeit werden.

5. Change-Kommunikation als Orientierungssystem nutzen
In Krisen und Transformationen entsteht Belastung nicht nur durch zusätzliche Arbeit, sondern auch durch Unsicherheit. Wo Informationen fehlen, entstehen schnell Gerüchte und somit auch Widerstand.

Gute Change-Kommunikation beschönigt nicht, sondern schafft Orientierung, macht Prioritäten transparent und übersetzt strategische Entscheidungen in den Arbeitsalltag. Sie sorgt für Dialogformate, in denen Rückmeldungen aus den Teams tatsächlich ankommen, und stärkt Führungskräfte als glaubwürdige Übersetzer zwischen Strategie und Stationsalltag. Gerade im Schichtbetrieb entscheidet zudem der richtige Kanal darüber, ob eine Botschaft die viel beschäftigten Menschen überhaupt erreicht.

Veränderungsfähigkeit wird zum Wettbewerbsfaktor
Resilienz lässt sich nicht auf Gesundheitsprogramme oder Notfallmanagement reduzieren. Personalresilienz entsteht im Zusammenspiel von strategischer Personalplanung, Change-Management, Kommunikation, Führung und Qualifizierung und wird damit zum festen Bestandteil zukunftsfähiger Personal- und Organisationsentwicklung.

Der Mehrwert liegt dabei weniger in Einzelmaßnahmen als in ihrer Orchestrierung. Erst wenn Personalplanung, Führung, Lernen und Kommunikation zusammenspielen, wird aus punktuellen Initiativen eine belastbare Resilienzarchitektur. In der Praxis zeigt sich: Häuser, die Personalresilienz früh und systematisch angehen, kommen nicht nur stabiler durch Krisen, sie werden auch als Arbeitgeber attraktiver, binden Fachkräfte länger und setzen Transformationsprojekte messbar schneller um. Resilienz wird damit vom Kostenfaktor zum Differenzierungsmerkmal im Wettbewerb um knappe Talente.

Fazit: Die wichtigste Ressource trägt ein Namensschild
Jede Veränderung im Gesundheitswesen bleibt wirkungslos, wenn die Menschen im System sie nicht mittragen können oder wollen. Ihre

Fähigkeit, unter Druck handlungsfähig zu bleiben, entscheidet darüber, wie resilient das Gesundheitswesen der Zukunft tatsächlich ist.

Das System steht vor Jahren permanenter Veränderung und einer Zunahme krisenhafter Extremsituationen. Es reicht daher nicht mehr aus, nur auf die nächste Krise vorbereitet zu sein. Die eigentliche Herausforderung besteht darin, Menschen durch eine Zeit zu führen, in der Veränderung der Normalzustand ist. Für Vorstände heißt das: Personalresilienz nicht länger delegieren, sondern zur Chefsache machen und mit klaren Verantwortlichkeiten hinterlegen.

Kontakt
Katharina Luh
katharina.luh@de.ey.com
Laura Sorgenicht
laura.sorgenicht@de.ey.com
Sophie Händel
sophie.haendel@de.ey.com

Fotos: Adobestock

Zwischen Zeitdruck und Empathie

Emotionale Intelligenz verbessert Zusammenarbeit und Führung

Der Klinikalltag ist geprägt von emotional belastenden Situationen. Patient:innen und Angehörige brechen nach schweren Diagnosen in Tränen aus, Konflikte eskalieren und Mitarbeitende fragen sich zunehmend, wie lange sie den Belastungen ihres Berufs noch standhalten können.

Während im Zusammenhang mit dem Fachkräftemangel häufig über Personalschlüssel, Prozesse und KI gesprochen wird, bleibt ein entscheidender Faktor oft unbeachtet: der Umgang mit den emotionalen Anforderungen des Berufs.

Wer kümmert sich um diejenigen, die sich täglich um andere kümmern?
Pflegekräfte, Ärzt:innen und Führungskräfte begleiten Menschen in Ausnahmesituationen. Sie geben Sicherheit, führen schwierige Gespräche und tragen die Sorgen und Belastungen anderer mit. Gleichzeitig bleibt im Arbeitsalltag oft wenig Zeit, das Erlebte selbst zu verarbeiten. Während Supervision und Reflexionsräume in vielen Berufsgruppen selbstverständlich sind, fehlen im Gesundheitswesen dafür häufig Zeit und Raum. Angesichts der steigenden Belastungen und des Fachkräftemangels stellt sich daher zunehmend die Frage, wie emotionale Unterstützung stärker im Arbeitsalltag verankert werden kann. Denn wer täglich andere auffängt, braucht auch selbst Möglichkeiten, mit emotionalen Belastungen gesund umzugehen.

Emotionale Intelligenz: weg vom Soft Skill, hin zum strategischen Resilienzhebel
Genau hier setzt emotionale Intelligenz (EI) an. Sie ist die Fähigkeit, eigene und fremde Emotionen wahrzunehmen, zu verstehen und bewusst zu steuern. Damit ist sie weit mehr als ein „Soft Skill" – sie ist eine Grundlage von Resilienz. Denn wer Emotionen besser regulieren kann, bleibt auch unter Druck handlungsfähig, verarbeitet Belastungen konstruktiver und kann mit Unsicherheit besser umgehen. Gerade im Gesundheitswesen, wo emotionale Belastungen zum Arbeitsalltag gehören, wird EI damit zu einem strategischen Resilienzhebel. Fehlt sie, werden Gespräche mit Angehörigen schwieriger, Konflikte zwischen Berufsgruppen verschärfen sich und emotionale Belastungen bleiben häufiger unverarbeitet.

Von der Person zum System: EI stärkt Resilienz auf drei Ebenen
Auf individueller Ebene unterstützt EI den Umgang mit Stress und emotionalen Belastungen. Mitarbeitende erkennen ihre Grenzen früher, ordnen Situationen bewusster ein und bleiben auch in anspruchsvollen Momenten handlungsfähig.

Auf Teamebene stärkt EI das Vertrauen, die psychologische Sicherheit und die Zusammenarbeit. Studien verbinden emotionale Intelligenz in der Führung mit höherer Arbeitszufriedenheit, besserer Teamleistung und stärkerem

Engagement. Mitarbeitende erwarten in Phasen hoher Belastung weniger perfekte Antworten als vielmehr Orientierung, Empathie und einen professionellen Umgang mit Unsicherheit.

Auf Organisationsebene kann emotionale Intelligenz dazu beitragen, Belastungsfolgen wie Erschöpfung, Burnout oder Fluktuation zu reduzieren. Damit leistet sie einen wichtigen Beitrag zur Mitarbeiterbindung und Fachkräftesicherung.

Die Zukunft der Resilienz ist emotional

Resiliente Organisationen entstehen dort, wo Menschen befähigt werden, mit Belastungen, Unsicherheit und Veränderung konstruktiv umzugehen. Genau hier setzt emotionale Intelligenz an: Sie hilft Mitarbeitenden, auch unter Druck handlungsfähig zu bleiben und sich schneller zu erholen.

Die gute Nachricht: Emotionale Intelligenz ist lernbar. Studien zeigen, dass Trainings zu signifikanten Verbesserungen von EI führen können. Auch praktische Erfahrungen bestätigen dieses Potenzial. In einer von unserer EY-Kollegin Eva Langhans entwickelten und begleiteten Intervention zeigten Teilnehmende über mehrere Wochen hinweg eine positive Entwicklung emotionaler Kompetenzen.

Wer die Resilienz des Gesundheitssystems stärken möchte, sollte deshalb nicht nur in Strukturen und Prozesse investieren, sondern auch in die emotionale Kompetenz der Menschen, die Versorgung jeden Tag möglich machen.

Kontakt
Katharina Luh
katharina.luh@de.ey.com
Laura Sorgenicht
laura.sorgenicht@de.ey.com
Eva Langhans
eva.langhans@de.ey.com

Fotos: Adobestock

Leiter Gesundheitswesen Europa West, EY

Christian Egle
Partner EY-Parthenon
+49 6196 996 21226
+49 160 939 21226
christian.egle@parthenon.ey.com

Gesundheitsmarkt Deutschland

Florian Benthin
Partner EY-Parthenon
+49 40 36132 14291
+49 160 939 14291
florian.benthin@parthenon.ey.com

Matthias Frey
Partner EY
+49 30 25471 11201
+49 160 939 11201
matthias.frey@de.ey.com

Ronald Fritz
Partner EY-Parthenon
+49 40 36132 28735
+49 160 939 28735
ronald.fritz@parthenon.ey.com

Eva-Lotta Hinzpeter
Partnerin EY-Parthenon
+49 211 9352 12631
+49 160 939 12631
eva-lotta.hinzpeter@parthenon.ey.com

Markus Kleine-Voßbeck
Partner EY
+49 221 2779 17699
+49 172 705 6779
markus.kleine-vossbeck@de.ey.com

Lea Thanner
Partnerin EY
+49 89 14331 28961
+49 160 939 28961
lea.thanner@de.ey.com

Dr. Regina Vetters
Partnerin EY-Parthenon
+49 30 25471 11514
+49 160 939 11514
regina.vetters@parthenon.ey.com

Rechtsberatung

Dr. Christian Bosse
Partner EY
+49 711 9881 25772
+49 160 939 25772
christian.f.bosse@de.ey.com

Dr. Tristan Kalenborn
Director EY
+49 211 9352 24695
+49 160 939 24695
tristan.kalenborn@de.ey.com

Stefan Schmidt
Director EY
+49 211 9352 22533
+49 160 939 22533
stefan.d.schmidt@de.ey.com

Steuerberatung

Sven Riedel
Director EY
+49 761 1508 16963
+49 160 939 16963
sven.riedel@de.ey.com

Gesundheitsmarkt Österreich

Dr. Christian Horak
Partner EY-Parthenon
+43 1 211 70 1902
+43 699 1919 3295
christian.horak@parthenon.ey.com

Immobilienberatung

Fabian Schuster
Partner EY-Parthenon
+49 711 9881 21975
+49 160 939 21975
fabian.schuster@parthenon.ey.com

Katrin Thies
Partnerin EY-Parthenon
+49 6196 996 15664
+49 160 939 15664
katrin.thies@parthenon.ey.com

IMPRESSUM

Inhalte und Redaktion
Dr. Regina Vetters
Partnerin EY-Parthenon
Katharina Vogel
Managerin EY-Parthenon
Dr. Edda Eggers
Senior Consultant EY-Parthenon
Patricia Petsch
Consultant EY-Parthenon

Konzept, Design und Layout
CPoffice, Sabine Reissner
www.cp-office.com

Lektorat
Text+Design Jutta Cram
www.textplusdesign.de

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2026 EYGM Limited
All Rights Reserved.

SRE 2609-025
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com