02/2022

Hartmannbund
Verband der Ärztinnen und Ärzte Deutschlands e. V.

# Hartmannbund Magazin

## Der unsichtbare Feind

Was Cyberangriffe für Praxen und Kliniken bedeuten

# Editorial

**Dr. Klaus Reinhardt**
*Vorsitzender des Hartmannbundes Verband der Ärztinnen und Ärzte Deutschlands*

liebe Kolleginnen,
liebe Kollegen,

niemand bezweifelt, dass wir die Corona-Pandemie weiterhin intensiv im Blick behalten müssen. Pläne für den Herbst sind Pflicht, Virus-Varianten sind zu beobachten, mögliche Entwicklungen zu prognostizieren und die „Nebenwirkungen" der Pandemie-Bekämpfungsmaßnahmen konsequent aufzuarbeiten, gerade zu Letzterem hat sich auch der Deutsche Ärztetag in Bremen klar positioniert. Aber im gleichen Maße, in dem wir uns dieser Verantwortung bewusst sind, entwickelt sich inzwischen das Gefühl, dass andere essenzielle Felder der Gesundheitspolitik möglicherweise schon bald ebenfalls in die Kategorie „Kollateralschäden" eingeordnet werden müssen. Long Covid droht in gewisser Weise auch dem deutschen Gesundheitssystem.

Es ist absolut nachvollziehbar, dass die Bewältigung der Pandemie in den vergangenen zwei Jahren allen Beteiligten ein hohes Maß an politischer und administrativer Konzentration abverlangt hat. Das ändert aber nichts an der – auch von den Koalitionären zu Recht festgestellten – dringenden Notwendigkeit, Strukturveränderungen des Gesundheitssystems in Angriff zu nehmen.

Einen Leitfaden für die anstehenden „Hausaufgaben" bietet der Koalitionsvertrag der Ampel. Neben den immer offensichtlicher werdenden Defiziten im Bereich der Digitalisierung des Gesundheitswesens, den Themen Krankenhausplanung und -finanzierung, Notfallversorgung oder etwa dem Öffentlichen Gesundheitsdienst warten eine Vielzahl an Herausforderungen. So duldet zum Beispiel die auch vom Bundesrat einhellig geforderte Einführung erlösunabhängiger Vorhaltepauschalen für die Kliniken auf Grundlage von Empfehlungen einer kürzlich eingesetzten Regierungskommission keinen Aufschub. Auch im ambulanten Bereich stehen Entscheidungen an, Konzepte sind zu erarbeiten. So ist die GOÄ-Reform längst überfällig. Hier haben wir als Ärzteschaft unsere Hausaufgaben gemacht! Und auch für eine angemessene Anpassung der vertragsärztlichen Honorierung in Bezug auf die Preissteigerungen sowie den Fachkräftemangel ist es höchste Zeit.

Dabei gilt nach wie vor: Wir stehen der Politik bei der Gestaltung der Reformvorhaben mit unserer Expertise zur Seite. Dieses Angebot und dieser Anspruch gelten ausdrücklich nicht nur für einen bisweilen etwas orientierungslos wirkenden Gesundheitsminister, sondern auch und gerade für das Parlament, das ja schlussendlich das letzte Wort hat. Wir werden in unserer Gesellschaft rückblickend sicher viele durch die Pandemie verursachte Einschnitte resümieren. Eine Corona-Delle auf der Reformbaustelle könnte noch weitgehend vermieden werden.

Mit kollegialen Grüßen,

Ihr

# Inhalt

PASSWORT

**„Als Angreifer brauche ich nur einmal zu gewinnen, als Verteidiger muss ich das immer“**
Eben noch mitten in der Digitalisierung, findet sich das Lukaskrankenhaus in Neuss im Jahr 2016 plötzlich auf dem Entwicklungsstand der Schwarzwaldklinik wieder. Der Klinikbetrieb ist nur noch mit Stift und Papier zu bewältigen. Was mit ungewöhnlich langsamen Geräten in der einen Abteilung beginnt, mit Druckerproblemen oder Fehlermeldungen der Planungssoftware in der anderen, stellt sich bald als ausgewachsener Cyber-Angriff heraus. Um die sensiblen Patientendaten zu schützen und weitere Schäden zu verhindern, fährt das Krankenhaus fast die gesamte IT herunter. Die Folgen sind drastisch – die Notaufnahme wird ausgesetzt, es ist kein Zugriff auf digitale Patientenakten möglich, Medikamente können nicht mehr bestellt und die Strahlentherapie für Krebspatienten muss ausgesetzt werden. Cyber-Angriffe bedrohen inzwischen längst regelmäßig auch die Strukturen im Gesundheitswesen und gefährden im Ernstfall auch Menschenleben. Nicht nur Krankenhäuser, sondern auch Arztpraxen sind Opfer von Attacken. Wo die Gefahren lauern, wie man sich schützen kann und vieles Spannende mehr lesen Sie in unserer Titelgeschichte.

Cyber-Attacken im Gesundheitssystem – Die unterschätzte Gefahr

# „Als Angreifer brauche ich nur einmal zu gewinnen, als Verteidiger muss ich das immer“




*Es geht langsam los, der Zeitensprung ist dann umso heftiger: Eben noch mitten in der Digitalisierung, findet sich das Lukaskrankenhaus in Neuss im Jahr 2016 plötzlich auf dem Entwicklungsstand der Schwarzwaldklinik wieder. Der Klinikbetrieb ist nur noch mit Stift und Papier zu bewältigen. Was mit ungewöhnlich langsamen Geräten in der einen Abteilung beginnt, mit Druckerproblemen oder Fehlermeldungen der Planungssoftware in der anderen, stellt sich bald als ausgewachsener Cyber-Angriff heraus, der im Krankenhausnetzwerk Daten verschlüsselt. Um die sensiblen Patientendaten zu schützen und weitere Schäden zu verhindern, fährt das Krankenhaus fast die gesamte IT herunter. Die Folgen sind drastisch – die Notaufnahme wird ausgesetzt, es ist kein Zugriff auf digitale Patientenakten möglich, Medikamente können nicht mehr bestellt und die Strahlentherapie für Krebspatienten muss ausgesetzt werden. Beim zuständigen Landeskriminalamt fragt man sich, ob eine Mordkommission eingerichtet werden muss, falls durch die Ransomware-Attacke und deren Auswirkungen auf die Patientenversorgung ein Mensch sterben sollte. Vom Vorzeigekrankenhaus der Digitalisierung ist das Lukaskrankenhaus nun selbst zu einem Notfall geworden. Cyber-Angriffe bedrohen inzwischen längst regelmäßig auch die Strukturen im Gesundheitswesen und gefährden im Ernstfall auch Menschenleben. Nicht nur Krankenhäuser, sondern auch Arztpraxen sind Opfer von Attacken. Hier und da werden die Gefahren offensichtlich trotzdem noch immer unterschätzt.*

Die Art und Weise, wie sich im Frühjahr 2016 die Ransomware im Krankenhausnetzwerk ausbreitet, ist damals noch unbekannt. Es dauert Tage, bis das Lukaskrankenhaus wieder im Normalbetrieb laufen kann. Menschen kommen nicht zu Schaden. Aber die Öffentlichkeit verfolgt das Geschehen aufmerksam. Seitdem werden immer wieder Cyber-Angriffe bekannt, die Krankenhäuser, aber auch Praxen und weitere Akteure des Gesundheitswesens treffen. Zunehmende Digitalisierung und Vernetzung sorgen nicht nur für mehr Effizienz und medizinischen Fortschritt. Es zeigt sich, dass diese auch Risiken bergen. Kein IT-System ist absolut sicher, wenn auch konsequente Sicherheitsmaßnahmen die Wahrscheinlichkeit eines erfolgreichen Angriffes minimieren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet in den vergangenen Jahren einen Anstieg von IT-Sicherheitsvorfällen bei registrierten Betreibern der kritischen Infrastrukturen (KRITIS). Während eine erfolgreiche Attacke von Cyber-Kriminellen in der Industrie oder im produzierenden Gewerbe zu beträchtlichen Schäden, finanziellen Einbußen und Betriebsausfall führen kann, stehen im Gesundheitswesen auch Menschenleben auf dem Spiel. Wie also steht es um die Informationssicherheit im Gesundheitswesen, wo ein Großteil der Prozesse heute ohne Digitalisierung kaum vorstellbar ist – sind Praxen und Krankenhäuser ausreichend gewappnet, um Schaden von der Praxisroutine sowie den Patientinnen und Patienten abzuwehren, um sensible Daten zu sichern?

### *Kritische Infrastruktur mit besonderer Verantwortung*

Aufgrund ihrer in vielerlei Hinsicht enormen Verantwortung müssen Einrichtungen des Gesundheitswesens besondere Sorgfalt bei der Absicherung ihrer IT-Systeme walten lassen. Seit dem BSI-Gesetz und 2015 mit dem IT-Sicherheitsgesetz haben Krankenhäuser mit 30 000 vollstationären Patienten pro Jahr – als Teil der kritischen Infrastrukturen – die Verpflichtung, technische und organisatorische IT-Sicherheitsmaßnahmen nach dem „Stand der Technik“ umzusetzen und diese dem BSI alle zwei Jahre nachzuweisen. Doch nicht nur KRITIS-Häuser erfüllen eine wichtige Funktion für die Bevölkerung, weshalb das Aufrechterhalten der stationären medizinischen Versorgung unerlässlich ist. Das trifft auch auf Einrichtungen unterhalb des KRITIS-Schwellenwertes zu. Auch diese müssen sich mit der Bedrohung durch Cyberkriminalität auseinandersetzen. IT-Sicherheit rückt also auch hier immer mehr in den Fokus.

Mit dem Krankenhauszukunftsgesetz (KHZG) von 2020 richtete der Bund sich deshalb an diese Zielgruppe. Mit dem Investitionsprogramm für Krankenhäuser sollte die Digitalisierung vorangetrieben werden. Mindestens 15 Prozent der jeweiligen Fördersumme für bewilligte Projekte mussten dabei für die Verbesserung der IT-Sicherheit verwendet werden. Die Idee: Sicherheit soll bei der Digitalisierung von Anfang an mitgedacht werden. Seit Januar diesen Jahres gilt mit dem IT-Sicherheitsgesetz 2.0, dass auch alle Nicht-KRITIS-Häuser den branchenspezifischen Sicherheitsstandard für Gesundheitsversorgung im Krankenhaus erfüllen müssen. Zwar entfällt bei ihnen die Nachweisplicht gegenüber dem BSI. Schadensersatzforderungen und Haftungsrisiken aber treffen die Betreiber trotzdem, falls ein Sicherheitsvorfall durch nicht ausreichend aufgerüstete IT-Technik eintritt. Das kann teuer werden. Bislang konnten Bußgelder von maximal 100 000 Euro erhoben werden, mit der Gesetzesänderung sind es nun bis zu 20 Millionen Euro.

Und die niedergelassenen Ärztinnen und Ärzte? Arztpraxen zählen nicht zur kritischen Infrastruktur, aber Informationssicherheit geht auch sie etwas an: Die Kommunikation mit Patienten

*Heinz-Theo Rey (KBV): Die Bereitschaft der Krankenkassen, Infrastrukturleistungen entsprechend zu refinanzieren, war bis jetzt sehr bescheiden.*

kann online stattfinden, Patientendaten werden digital gespeichert, die Terminvergabe erfolgt häufig übers Internet. Das Digitale-Versorgung-Gesetz forderte deshalb von der ärztlichen Selbstverwaltung verbindlich geltende IT-Sicherheitsstandards. Die Kassenärztliche Bundesvereinigung (KBV) hat mit Einvernehmen des BSI daher eine IT-Sicherheitsrichtlinie erarbeitet, die entsprechend der aktuellen Bedrohungslage und neuen technischen Möglichkeiten regelmäßig angepasst werden soll. Praxisinhaberinnen und -inhaber erhalten durch sie eine Orientierung, welche Sicherheitsvorkehrungen zu treffen sind, um Datenmissbrauch zu verhindern. Seit April 2021 wird diese Richtlinie nun in Etappen umgesetzt, für die Einführung der letzten Maßnahmen haben mittlere und große Praxen bis Juli dieses Jahres Zeit. Mittlerweile sollten in allen Praxen die Basisanforderungen zum Alltag gehören. Dazu zählen beispielsweise der Einsatz aktueller Virenschutzprogramme, das Abmelden beziehungsweise Sperren eines Gerätes, sobald es von der Person nicht mehr genutzt wird, und die Nutzung von Firewalls.

### *„Wer nichts tut, spielt mit seiner Existenz“*

Die gesetzlichen Vorgaben sind also klar. Aber wie klappt es mit der Umsetzung? „In dem Moment, in dem man IT nutzt und ans Internet angeschlossen ist, wird man angegriffen. Diese Erkenntnis ist bei Praxispersonal und Praxisinhabern stellenweise gar nicht vorhanden“, beschreibt Heinz-Theo Rey, Dezernent für IT und Infrastruktur bei der KBV, seinen Eindruck. Sorglosigkeit, Unachtsamkeit, das passt nicht so recht zum Thema Datenschutz und Informationssicherheit. „Der Gedanke ist oft: Die IT wird es schon richten oder es ist ja noch immer gut gegangen. Es braucht nur eine E-Mail mit Anhang zu kommen und es wird nicht lange nachgedacht. Man macht einen Doppelklick und schon ist man infiziert.“ Tatsächlich

## Risikofaktoren

- Surfen im Internet
- E-Mail-Anhänge
- Private USB-Sticks
- Schwache Passwörter
- Alle vernetzten Geräte wie Computer, Drucker, Fax, Telefon, medizinische Geräte
- Veraltete Virenschutzprogramme
- Patienten und Personal nutzen das W-Lan der Praxis oder des Krankenhauses

spiegelt diese Einschätzung gut die Realität wider. Das aktuelle Bundeslagebild zum Thema Cybercrime, den das Bundeskriminalamt (BKA) im Mai veröffentlicht hat, greift genau diesen Punkt auf: Im vergangenen Jahr zählte das sogenannte Phishing erneut zu den Haupteintrittsvektoren für Schadsoftware und war die Ursache dafür, dass es, wie das BKA schreibt, zu einem massenhaften Abgriff sensibler personenbezogener Daten kam. Schadsoftware werde häufig über maliziöse Dokumente als E-Mail-Anlage verteilt. Das Phänomen ist kein neues. Und dennoch sind mit dem Beginn der Corona-Pandemie die Phishing-Zahlen, auch im Gesundheitswesen, stark gestiegen. Kein Grund also, die IT-Sicherheit schleifen zu lassen. Eigentlich. „Die KBV hat Schwierigkeiten, Ärzten diese Dramatik klarzumachen. Es gibt natürlich Ärzte, die gut aufgestellt sind. Aber wenn sie nichts tun, spielen sie mit Ihrer Existenz! Das kommt leider nicht bei allen an“, sagt Rey.

Wie es tatsächlich in den Praxen aussieht, wie gut – oder eben auch nicht – die Ärztinnen und Ärzte ausgerüstet sind, um ihre Daten zu schützen, darüber kann die KBV keine Auskunft geben. Die Ärzteschaft hat ihr gegenüber keine Meldepflicht. Weder, was Cyberangriffe auf Praxen, noch was die Umsetzung der IT-Sicherheitsrichtlinie betrifft. Anders als in KRITIS-Häusern wird keine regelmäßige Überprüfung der Sicherheitsstandards durchgeführt. Es liegt allein in der Verantwortung der Praxisinhaber, die verbindliche KBV-Richtlinie tatsächlich auch umzusetzen. Und während das KHZG gut als Anschubfinanzierung für die IT-Sicherheit von Krankenhäusern diente, fehlt ein ähnlicher Anreiz für Niedergelassene, in ihre IT zu investieren. „Die Bereitschaft der Krankenkassen, Infrastrukturleistungen entsprechend zu refinanzieren, war bis jetzt sehr bescheiden. Das ist jedoch dringend erforderlich“, urteilt Rey. Verhandlungen zwischen KBV und GKV-Spitzenverband dazu laufen noch.





Sich in falscher Sicherheit wähnend, unvorbereitet für den Notfall und nachlässig im Umgang mit Passwörtern – recht verheerend fiel auch 2019 der Branchenreport „Cyberrisiken bei Ärzten und Apothekern“ aus. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hatte eine repräsentative Forsa-Umfrage zu den Cyberrisiken im Gesundheitswesen in Auftrag gegeben. Unter anderem 200 Mitarbeiter von Arztpraxen, die für die Internetsicherheit zuständig waren, nahmen daran teil. Ein Ergebnis lautete: Der Großteil von ihnen, 80 Prozent, war davon überzeugt, ihre Praxis ausreichend geschützt zu haben. Nur 17 Prozent sagten, dass das Risiko ihrer Arztpraxis, Opfer von Cyberkriminalität zu werden, eher beziehungsweise sehr hoch sei. Neben dieser Umfrage hatte der GDV auch einen IT-Spezialisten 25 Arztpraxen überprüfen lassen. Mit Hilfe von Penetrationstests machte der Experte sich Ende 2018 auf die Suche nach Sicherheitslücken in den Praxisnetzwerken. Das Ergebnis stand im direkten Kontrast zur recht positiven Einschätzung der Umfrage: 21 der 25 teilnehmenden Praxen hatten ein hohes oder sehr hohes Risiko, Opfer eines internen Angriffs zu werden.

### *Bewusstsein für Risiken noch nicht sehr ausgeprägt*

Michael Wiesner war es, der die Penetrationstests damals durchgeführt hatte. Der Informationssicherheitsexperte berät seit mehr als 25 Jahren Unternehmen. Eine der Fokusbranchen seines Beratungsunternehmens ist das Gesundheitswesen. Außerdem ist er Sprecher der AG KRITIS, einer unabhängigen Arbeitsgruppe, deren Ziel die Versorgungssicherheit der Bevölkerung ist. Dass Wiesner im Rahmen der GDV-Studie erfolgreich Praxen hacken konnte, war für ihn keineswegs ein Ereignis mit Seltenheitswert. Das Bewusstsein für Cyberrisiken sei bei vielen Ärzten – sowohl in Praxen als auch in Krankenhäusern – noch nicht sehr ausgeprägt. Wiesner erinnert sich an einen Live-Hack vor etwa sieben Jahren. 25 000 Patientendaten – Namen und Geburtsdaten der Patientinnen sowie

Foto: Uwe Klissing

*Michael Wiesner: Maximal zehn Minuten sind die Zeitspanne, in der nach Feststellen einer Cyber-Attacke noch Schaden abgewendet werden kann*

Befundfotos – einer gynäkologischen Gemeinschaftspraxis konnte er frei im Internet finden. Er schüttelt den Kopf und lacht ungläubig, als er davon erzählt. Er attestiert dem Gesundheitswesen Nachholbedarf, wenn es um die Informationssicherheit geht.

„Tatsächlich ist es so, dass eine Arztpraxis sicherlich nicht zwingend Angst davor zu haben braucht, Opfer eines gezielten Hackerangriffs zu werden. Aber es gibt eben auch die ungezielten Angriffe, die relativ automatisiert ablaufen und natürlich Praxen treffen können. Dagegen kann man sich mit einfachen Mitteln schützen“, erklärt er. Firewall, Zutrittskontrollsysteme, Endpoint-Security und ein schlüssiges Security-Konzept, das beispielsweise regelmäßige Updates, Mitarbeiterschulungen und ausgefeilte Passworte beinhaltet, gehören für ihn zum Standard. „Das sind grundlegende Maßnahmen. Wenn ich die erfülle, habe ich ein sehr großes Maß an Grundsicherheit. Das reicht für Praxen meist auch schon aus“, erklärt Wiesner. Die Furcht vor zu hohen Ausgaben lässt er nicht gelten. Er schätzt, dass Praxisinhaber mit einem vierstelligen Betrag schon sehr viel erreichen können. All dies entspreche im Grunde genommen auch den Empfehlungen der KBV in ihrer IT-Sicherheitsrichtlinie. Nur: „Standards oder Richtlinien sind immer nur ein Anfang. Sie definieren auf einer sehr generischen Linie eine Anforderung, die erfüllt werden muss.“ Für Wiesner liegt das Problem darin, dass diese Anforderungen nach Stand der Technik umgesetzt werden müssen – und viele das nicht machen. „Im KRITIS-Bereich wird das überprüft. Wird eine Abweichung gefunden, muss nachjustiert werden. Da wurden jetzt die Bußgelder erhöht, deswegen wird das auch mehr befolgt. Denn man muss leider sagen: Ohne Bußgeldandrohung wird kaum etwas gemacht. Bei den IT-Sicherheitsrichtlinien ist das genauso. Zwar gibt es konkrete Anforderungen, aber wie diese letztendlich umgesetzt werden, ob das nach Stand der Technik erfolgt, prüft im Moment keiner.“

## Bundeslagebild Cybercrime 2021

- Die Zahl der erfassten Cyberstraftaten steigt weiterhin an. Im Jahr 2021 ist sie um mehr als 12 Prozent gestiegen.
- Die Aufklärungsquote liegt bei knapp unter 30 Prozent.
- Das Bedrohungspotential von Ransomware ist auch im vergangenen Jahr deutlich gestiegen. Zudem verursacht Ransomware weiterhin das höchste Schadenspotential im Bereich Cybercrime. Im internationalen Vergleich ist Deutschland überdurchschnittlich häufig von Ransomware-Angriffen betroffen.
- Cyberkriminelle haben neben öffentlichen Einrichtungen, dem Gesundheitswesen, dem Bildungssektor sowie KRITIS nahezu jede Branche angegriffen.
- Cybercrime verursacht Schäden in Milliardenhöhe. Betrug der jährliche Schaden 2019 noch rund 5,3 Milliarden Euro, waren es 2021 bereits etwa 24,3 Milliarden Euro.

Dafür entdecken immer mehr die Vorteile von Cyberversicherungen für sich. Seit 2017 sind Cyberversicherungen ein großes Thema beim GDV, seither haben rund 40 GDV-Mitglieder Versicherungen im Angebot. Zwar liegt dem GDV keine genaue Statistik vor, doch eine Tendenz ist schon erkennbar: Die Zahl der Verträge und Beiträge über alle Branchen hinweg steigt, gleichzeitig steigt auch die Zahl der Schäden durch Cyberangriffe und deren Aufwand. Gut möglich, dass unter den Neu-Versicherten auch Ärzte und Krankenhäuser zu finden sind. Für Anja Käfer-Rohrbach, stellvertretende GDV-Hauptgeschäftsführerin, ist das mit dem zunehmenden Cyberrisiko auch nicht verwunderlich: „Ärzte und Krankenhäuser können ohne IT nicht arbeiten und sollten sich gegen jedes Risiko, das besteht, absichern." Im Falle eines vermuteten Cyberangriffs werden beispielsweise schnellstmöglich IT-Forensik-Experten zur Analyse, Beweissicherung und Schadensbegrenzung vermittelt und die Kosten dafür übernommen. Was sie außerdem feststellt ist, dass langsam ein Wandel einsetzt, wenn es darum geht, das eigene Unternehmen vor Cyberangriffen schützen zu wollen. „Über alle Branchen hinweg gibt es die Tendenz, dass Großunternehmen durchaus früh erkannt haben, dass für sie in dieser Hinsicht ein Risiko besteht und sie sich dem auch gewidmet haben. Die kleinen Unternehmen beginnen erst jetzt, nachzuziehen", sagt Anja Käfer-Rohrbach.

### *Präventive Maßnahmen sind nur ein Teil der Lösung*

Ein Umdenken ist dringend nötig. Das Bundeslagebild „Cybercrime" vom BKA macht es deutlich – nicht nur KRITIS-Einrichtungen sind von Cyberkriminalität betroffen, nahezu jede Branche wird zum Ziel von Cyber-Attacken. „Bis vor ein paar Jahren gab es immer noch Unternehmen, die sagten, sie seien von Cyberangriffen nicht betroffen, weil sie zu unbedeutend seien. In dieser Kategorie finden sich auch viele Ärzte. Das ist heute nicht mehr so. Die Zahlen zeigen, es hat sich von ‚ich bin so klein, mich betrifft das nicht' zu ‚gerade mich betrifft es' entwickelt. Denn je weniger ich vorbereitet bin, umso häufiger werde ich Opfer von Attacken. Das ist leider die neue Realität", sagt Thomas Schumacher; der beim Beratungsunternehmen Accenture den Bereich Security im deutschsprachigen Raum leitet. Gerade im Mittelstand werde das Thema Cyberangriffe immer präsenter. Das zeigt auch eine repräsentative Bitkom-Studie. 88 Prozent der befragten Unternehmen aus allen Branchen gaben an, 2021 von Cyberangriffen betroffen gewesen zu sein, 12 Prozent vermuteten solch einen Vorfall. 2019 berichteten nur 75 Prozent aller Unternehmen von einer Cyber-Attacke.

Für Schumacher besteht die Lösung darin, sich als Unternehmen aktiv mit der Bedrohungssituation auseinanderzusetzen und eine nachhaltige, aufs Unternehmen zugeschnittene Sicherheits-Strategie zu erarbeiten. Die aktuellen Zahlen legen nahe, dass es keine Frage ist, ob man mit Cyberkriminalität in Berührung kommt, sondern wann. „Die Kunst ist es, sich von Anfang an der Gefahr bewusst zu sein und sie einzukalkulieren. Wenn Sie einen Plan haben, kann ein Angriff trotzdem noch passieren, aber er ist dann nur halb so schlimm. Wenn Sie überhaupt nicht drüber nachdenken und es trifft Sie, dann haben Sie ein Problem", erklärt Schumacher. Dabei ist es wichtig, nicht nur Augenmerk auf technische Lösungen zu legen. Ein hundertprozentiger Schutz vor Cyberangriffen wird nicht möglich sein, deshalb sollte das Thema ganzheitlich angegangen werden. Es ist wichtig, dass Sicherheit schon bei Prozessen und Mitarbeitern mitgedacht wird und man erst am Ende auf technische Unterstützung setzt.

Das sieht auch Michael Wiesner so. Bei Penetrationstests in Krankenhäusern ist er immer wieder erfolgreich. „Das überrascht mich überhaupt nicht, weil Informationssicherheit nicht ganzheitlich betrachtet wird. Als Angreifer gelangen wir über eine Schwachstelle im Betriebssystem, Windows zum Beispiel, in ein Netzwerk. Nehmen wir ein kleines Krankenhaus, dort gibt es vielleicht 300 Systeme und davon sind 299 aktuell, eins aber nicht. Das reicht mir." Sich zum Schutz hermetisch gegenüber der Außenwelt abzuschotten, ist aber nicht realistisch. Es wird immer Schnittstellen geben, über die man die Kommunikation zum Internet zulässt. Zum Beispiel, wenn Befunde per E-Mail beim Arzt eingehen. Zwar gibt es für alles technische Lösungen, Michael Wiesner befürwortet auch Machine Learning-Programme, um Anomalien im Krankenhausnetz durch Cyber-Attacken aufzuspüren. Aber er weist auch darauf hin, dass kleineren Häusern für ausgefeilte Informationssicherheit auf Stand der Technik oft das Budget und das Personal fehlt. Bei Penetrationstests stellt er häufig fest, dass dadurch die Fähigkeiten stark eingeschränkt sind, auf Angriffe richtig zu reagieren. Damit katapultiert man sich im Ernstfall ins Aus. Denn bei einem Cyberangriff zählt vor allem eins: So wenig Zeit wie möglich zu verlieren. Maximal zehn Minuten gibt Wiesner als Zeitspanne an, in der nach Feststellen einer Cyber-Attacke noch Schaden abgewendet werden kann. Indem beispielsweise der Angreifer im Netzwerk eingeschlossen und daran gehindert wird, in andere Bereiche vorzudringen. „Mit jeder weiteren Minute steigt die Wahrscheinlichkeit, dass etwas passiert." Detektive und reaktive Fähigkeiten – also einen Angreifer zu erkennen, sobald er im Netzwerk ist, und schnell und routiniert nach zuvor festgelegtem Plan darauf antworten zu können – seien deshalb wichtige Voraussetzungen, um Krankenhäuser sicher betreiben zu können. Denn allein durch präventive Maßnahmen wie beispielsweise das Einspielen aller Sicherheitsupdates seien längst nicht alle Schwachstellen im Netzwerk zu beseitigen. Informationssicherheit auf die leichte Schulter zu nehmen oder sich auf bisher Erreichtes zu verlassen, kann deshalb nicht im Sinn von Verantwortlichen in Praxen und Krankenhäusern sein. Wiesner sagt dazu: „Eine Schwachstelle zu finden, ist nicht schwierig und es gilt: Als Angreifer brauche ich nur einmal zu gewinnen, als Verteidiger muss ich das immer."

## Schutz vor Cyberangriffen

Unterschied IT-Sicherheit und Informationssicherheit => IT-Sicherheit ist Teil der Informationssicherheit. Darunter versteht man den Schutz von Informationen durch Informationstechnologie (IT), es betrifft also alle technischen Aspekte. Der Begriff Informationssicherheit hingegen ist weiter gefasst. Darunter fallen ebenso personelle und organisatorische Aspekte. Um sich vor einem Cyberangriff zu schützen, stehen technische und organisatorische Maßnahmen zur Verfügung. Dazu zählen:

- Virenscanner
- Firewalls nach Stand der Technik
- Regelmäßige Sicherheits-Updates
- Systematische Datensicherung
- Passwortgeschützte Zugänge für Mitarbeiterinnen und Mitarbeiter
- Verschlüsselung sensibler Daten
- Verschlüsselter E-Mail-Verkehr
- Zutrittskontrollsysteme
- Penetrationstests
- Security-Konzept
- Schulung von Mitarbeiterinnen und Mitarbeitern





Beispiele von Angriffen aufs Gesundheitswesen

# Auch Software-Hersteller war schon betroffen




### LUKASKRANKENHAUS IN NEUSS

Eine kompromittierte E-Mail verursachte im Februar 2016 einen Stillstand des digitalen Klinikalltags. Nach Fehlermeldungen hatte sich die Klinikleitung dazu entschlossen, das gesamte Krankenhausnetz herunterzufahren. Der Blackout selbst dauert fünf Tage. Mehr als 800 Endgeräte waren betroffen. Befallen waren auch Server und Datenspeicher. Die komplette IT war über einen Monat lang nicht funktionsfähig. Im Anschluss musste das gesamte System modernisiert werden. Kosten für externe IT-Sicherheitsexperten betrugen fast eine Million Euro. Die Patientenversorgung auf den Stationen war gesichert, nicht dringende Operationen wurden aber verschoben und in den ersten 36 Stunden konnten keine Notfälle aufgenommen werden. Es handelte sich um einen Ransomware-Angriff, der nicht zielgerichtet war. Ziel war es, Patientendaten zu verschlüsseln. Durch schnelles Eingreifen, Herunterfahren der Systeme und Backup-Lösungen konnte dies verhindert werden. Auf die Erpressung sind die Verantwortlichen nicht eingegangen. Die damalige Geschäftsführung ging mit diesem Vorfall offensiv an die Öffentlichkeit, um mehr für diese Thematik zu sensibilisieren.

### UNIVERSITÄTSKLINIKUM DÜSSELDORF

Im September 2020 fiel nach einem Cyberangriff das Computer- und IT-System der Klinik aus. Ursache war eine Schwachstelle in der Software Citrix. Etwa 30 Server der Uniklinik waren verschlüsselt worden. Die Notaufnahme musste für 13 Tage schließen. Eigentliches Ziel der Attacke war jedoch offenbar die Heinrich-Heine-Universität in Düsseldorf, wie ein Erpresserschreiben andeutete. Die Polizei nahm Kontakt mit den Tätern auf, teilte mit, dass statt der Universität ein Krankenhaus getroffen wurde und dadurch Patienten gefährdet seien. Die Erpresser händigten daraufhin den digitalen Schlüssel aus, der die Daten wieder freigab.

### MEDATIXX

Der Praxissoftware-Hersteller, dessen Produkte mehr als 28 Prozent aller niedergelassenen Ärztinnen und Ärzte nutzen, war im November 2021 von einer Ransomware-Attacke betroffen, wichtige Teile des internen IT-Systems wurden dadurch lahmgelegt. Das Unternehmen gab bekannt, dass es sich mit hoher Wahrscheinlichkeit um einen Angriff auf medatixx handelte. Die Kunden und somit die Funktionalität der Praxis-Verwaltungssysteme seien dadurch nicht betroffen.

### MEDIZIN CAMPUS BODENSEE

Zwei Häuser – das Klinikum Friedrichshafen und die Klinik Tettnang – des Klinikverbunds wurden im Januar dieses Jahres attackiert. Die IT-Infrastruktur wurde heruntergefahren. Die Folgen davon sind auch noch Monate nach dem Angriff zu spüren, eine komplette Wiederherstellung der Netzwerkstruktur ist noch nicht abgeschlossen – während Patienten schon seit einiger Zeit wieder digital aufgenommen und auch abgerechnet werden können, sind die beiden Krankenhäuser erst seit Mai nun nicht mehr nur telefonisch und per Fax, sondern auch wieder per E-Mail zu erreichen. Die Grundversorgung der Patientinnen und Patienten sei in beiden Häusern sichergestellt, einige Wochen nach dem Sicherheitsvorfall konnten auch wieder Notfallpatienten versorgt und geplante notwendige Operationen durchgeführt werden.


Grafik: Photon photo/shutterstock.com

## So wird angegriffen

# Von Ransomsoftware bis Drive-by-Exploits

**Ransomware** Ransomware ist eine Form von Malware, die von Cyberkriminellen zu Erpressungszwecken angewendet wird. Sie zählt aktuell zu den häufigsten Attacken aus dem Internet. In der Regel gelangt Ransomware über E-Mails in Praxen oder Krankenhäuser. Mit dem Klick auf einen Link oder einen Anhang in dieser E-Mail wird der Angriff gestartet. Ransomware, die mehr Know-How erfordert, nutzt auch unsichere Fernzugriffsverbindungen. Beim Angriff selbst werden Benutzer aus dem eigenen System ausgesperrt oder Daten verschlüsselt. Ein Zugriff auf diese ist erst wieder möglich, wenn die Hacker nach Erhalt eines Lösegeldes (Englisch: ransom) einen Schlüssel für die Entschlüsselung bereitstellen. Selbst, wenn die geforderte Geldsumme entsprechend der Anweisungen an die Erpresser gezahlt wurde, gibt es keine Sicherheit dafür, dass der Zugriff auf die eigenen Daten tatsächlich wieder möglich ist. Eine weitere Gefahr: Bevor die Daten beim Cyberangriff verschlüsselt werden, können die Hacker diese auch kopieren und abfließen lassen. Die Erpresser drohen dann damit, sensible Daten zu veröffentlichen.

**DoS-Angriff** Denial of Service, heißt so viel wie außer Betrieb setzen. Ein Server wird dabei mit so vielen Anfragen bombardiert, dass das System darauf nicht mehr reagieren kann und im schlimmsten Fall zusammenbricht.

**(D)DoS-Angriff** Distributed Denial of Service, verteilte DoS-Attacken. Eine hohe Anzahl von verschiedenen Rechner greift in koordinierter Weise an.

**Phishing-Attacke** Über gefälschte Webseiten, E-Mails oder Kurznachrichten versucht der Angreifer, persönliche Daten eines Internetnutzers zu erhalten. Das Wort setzt sich im Englischen zusammen aus Password und fishing. Im Deutschen heißt es so viel wie: Nach Passwörtern angeln.

**Social Engineering-Angriffe** Durch gezielte Täuschung wird unberechtigter Zugang zu IT-Systemen erlangt. Das können beispielsweise gezielte E-Mails oder Anrufe an Mitarbeiterinnen und Mitarbeiter sein, durch die vermeintlich im Auftrag des Vorgesetzten bestimmte Informationen abgefragt werden oder die Aufforderung erteilt wird, Schadprogramme zu installieren.

**CEO-Fraud** Das ist ein gezielter Social Engineering-Angriff, bei dem der Angreifer zuvor erbeutete Identitätsdaten wie Telefonnummern, E-Mail-Adressen oder Passwörter nutzt. Damit gibt er sich beispielsweise als Geschäftsführung aus.

**Drive-by-Exploits** Bestimmte Webseiten, die manipuliert wurden, damit Anwender sich beim Besuch mit einem Schadcode infizieren.






## Hartmannbund-Blitzumfrage

# Jede fünfte Praxis war schon Opfer einer Cyber-Attacke

Die Arbeitsabläufe in den Arztpraxen sind inzwischen ohne digitale Daten und funktionierende Informationstechnik kaum noch denkbar. Täglich wird der Datenaustausch über das Internet genutzt und erst nach und nach rückt dabei ins Bewusstsein: Cyberkriminalität betrifft nicht nur große Wirtschaftsunternehmen oder Krankenhaus-Ketten. Hacker interessieren sich auch immer mehr für die „kleinen" Arztpraxen. Und auch hier kann es dann ganz schnell um große Beträge gehen – nicht selten durch Erpressung.

Im Rahmen einer Blitzumfrage hat der Hartmannbund einen Blick auf die Erfahrungswerte der niedergelassenen Ärztinnen und Ärzte im Umgang mit Cyberkriminalität geworfen, wollte wissen, wie sie die tägliche Herausforderung erleben, die Datensicherheit in der eigenen Praxis zu gewährleisten. Im Ergebnis zeigte sich: Die Befragten sind sich des Risikos bewusst, auch selbst Opfer einer Attacke durch Cyberkriminalität werden zu können. Bei der Einschätzung, ob sich die Praxen ausreichend geschützt und auf einen möglichen Ausfall ihres IT-Systems vorbereitet fühlen, gehen die Meinungen jedoch auseinander.

Immerhin 20 Prozent der knapp 300 Umfrageteilnehmer gaben an, schon einmal Opfer einer Cyber-Attacke gewesen zu sein. Dabei wurde von jedem Zweiten das Öffnen einer Spam-Mail oder angehängter Dateien als Ursache benannt. Ein Viertel der Betroffenen konnte den Weg des Angriffs nicht nachvollziehen. Die dabei entstandenen Schäden wurden als unterschiedlich „gravierend" empfunden. Von „gering" über „mittel" bis „schwerwiegend" hielten sich die Einschätzungen die Waage. Die Hälfte der betroffenen Praxen beklagte dabei einen Ausfall des IT-Systems. Dabei war in den meisten Fällen die gesamte Telematikinfrastruktur der Praxis oder zumindest das Praxisverwaltungssystem betroffen, was in fast allen Fällen zum Erliegen der Praxis führte.

Die meisten Praxen funktionieren voll digital und werden – was die IT-Sicherheit betrifft – in 70 Prozent der Fälle von professionellen IT-Firmen betreut. Durch die Zusatzbelastung an digitalen Daten steigen auch die Ansprüche an das IT-System. 75 Prozent der schon einmal attackierten Praxen haben nach der Attacke weiter in ihre IT-Sicherheit investiert. Insgesamt haben sich 25 Prozent aller Befragten gegen durch Cyberangriffe verursachte Schäden versichert.

Sind die Krankenhäuser gut aufgestellt?

# „Es ist ein ständiges Wettrüsten“

***Das Gesundheitswesen steht im Fokus von Cyberkriminellen. Vor allem Cyberangriffe auf Krankenhäuser werden regelmäßig öffentlich gemacht. Die beiden stellvertretenden Vorsitzenden des Bundesverbands der Krankenhaus IT-Leiterinnen/ Leiter (KH-IT), Lars Forchheim und Thorsten Schütz, bewerten im Gespräch mit dem Hartmannbund Magazin die aktuelle Sicherheitslage, sagen was sich verändert hat und verraten, ob das Thema Informationssicherheit nach ihrer Einschätzung die notwendige Beachtung bei Entscheidungsträgern findet.***

*Hartmannbund Magazin: Die Zahl der Cyberangriffe steigt immer weiter. Wie ist Ihre Einschätzung, sind Krankenhäuser gut aufgestellt, um darauf entsprechend reagieren zu können?*
**Lars Forchheim**: Hat sich die Sicherheitslage in den letzten Jahren wirklich verändert oder ist das Risiko für einen Angriff merklich gestiegen? Wenn man ehrlich ist, steigt das Risiko nicht. Die Lage bleibt konstant.

*Ist das so?*
**F**: Dass eine Software eine Lücke haben kann, ist nichts Neues. Was sich wesentlich geändert hat, ist, dass heute viel mehr Systeme mit dem Internet verbunden sind und dadurch diese Lücken offensiver von außen angreifbar sind. In diesem Bereich hat das Thema an Relevanz gewonnen. Jedes IT-System hat eine Lücke. Die Frage ist: Wie gehe ich mit solchen Informationssicherheitsrisiken um?

**Thorsten Schütz**: Ich glaube auch, dass die Bedrohungslage gar nicht so sehr gestiegen ist. Es ist ein stetes Wettrüsten. Neu ist die gestiegene Abhängigkeit von der IT im Krankenhaus. Wenn man zehn Jahre zurückblickt, dann konnte man mit einem vorübergehenden Ausfall deutlich besser leben als heutzutage. Viele Krankenhäuser haben es in den letzten Jahren geschafft, ihre Patientenakte, die sie innerhalb des Hauses führen, von Papier auf digital zu überführen. Spätestens, wenn ich dann noch Arzneimittel ausschließlich digital dokumentiere, habe ich ein großes Problem – weil die Daten nicht mehr parallel auf Papier zur Verfügung stehen, wenn die IT ausfällt.

**F**: Auch die Wahrnehmung dafür ist gestiegen. Es wird über Fälle berichtet, wo Sicherheitslücken angegriffen wurden. Dadurch, dass Fälle durch die Gesetzgebung meldepflichtig sind, erhält das Thema Informationssicherheit einen anderen Stellenwert in der Öffentlichkeit.

*Wo sehen Sie die größten Risiken für Krankenhäuser?*
**S**: Aus meiner Sicht sind es zwei Sachen. Zum einen sind es die Zufallstreffer. Es passiert einfach, dass Krankenhäuser zufällig von Ransomware-Attacken getroffen werden, die weltweit unterwegs sind. Zum anderen werden regelmäßig gravierende Sicherheitslücken aufgedeckt wie bei Exchange oder bei Citrix. Diese werden gezielt ausgenutzt, das ist auch schon in Deutschland vorgekommen.

**F**: Bei allen Sicherheitsvorfällen in Krankenhäusern gab es auch immer eine Verkettung verschiedener Dinge. Es gab nicht nur eine große Lücke, über die ein Angriff erfolgreich ausgeführt werden konnte. Nehmen wir zum Beispiel die Log4J-Sache im letzten Jahr. Das war eine Java-Lücke, die jedem bekannt war – aber es gab für manche Applikationen einfach noch keine Updates. Es gab keine Lösungen, wie man die Software hätte schützen können, weil der Software-Hersteller das erst einmal selber herausfinden musste. In dieser Zeit ist die Software weiterhin im Betrieb und jeder, der draußen unterwegs ist, kann diese Lücke dann nutzen.

**S**: Das Problem ist die Vielzahl von ständig neu aufgedeckten Sicherheitslücken, aber auch die Überforderung in vielen Bereichen, die Lücken zu schließen und diese Komplexität überhaupt bewältigen zu können. Das konnte man gut im vergangenen Jahr beobachten. Einrichtungen, die zur kritischen Infrastruktur gehören, erhalten Warnmeldungen vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Im März 2021 hat das BSI erstmalig die Warnstufe Rot ausgerufen, wegen der Exchange-Mail-Server-Lücke. Alle wussten, das ist absolut brisant – Mailserver hat jeder, auch wenn nicht jeder Outlook Web Access nutzt, was in diesem Fall betroffen war. Es ging durch die Medien, alle waren informiert. Sechs Monate später, im November 2021, waren aber immer noch 12 000 Mailserver nicht geschützt. Im Januar 2022 wurde das nochmals untersucht und auf Anhieb eine zweistellige Anzahl von Mailservern in Verwaltungen gefunden, die immer noch die gleiche Sicherheitslücke aufwiesen.

*Und wie kann mehr Sicherheit erreicht werden?*
**F**: Wir können die Gefahren abtrennen. Gibt es Medizintechnik oder auch andere Software, die gerade nicht durch Updates gesichert werden kann, ist die einzige und wirksamste Maßnahme: Das Gerät darf nicht ins Internet kommunizieren oder nur über eine Firewall mit entsprechendem Regelwerk. Das machen alle so, egal ob im Krankenhaus oder in der Industrie. Wenn wir aber über die größte Schwachstelle im System sprechen, dann möchte ich einmal hervorheben: Das ist der Mensch.

**S**: Da würde ich widersprechen. Wenn ein IT-Sicherheitssystem allumfassend gut abgesichert ist, dann sollte der Einzelne eigentlich gar kein so großes Gefahrenpotential darstellen. Man darf dem End-Anwender eigentlich nicht allein auferlegen, dass er eine E-Mail als richtig oder falsch erkennt. Das ist immer schwieriger zu erkennen und man muss den Anwender hier vor sich selbst schützen. Die Technik kann heute schon sehr viel abnehmen. Es gibt zunehmend Mechanismen, die eingehende E-Mails so gut vorab scannen, dass dem Anwender nicht mehr die letzte Kontrolle überlassen werden muss. Natürlich ist es wichtig, dass Anwender trotzdem nicht auf alles klicken.





*Haben Gesetze, Richtlinien oder Anreize wie das Krankenhauszukunftsgesetz (KHZG) dazu geführt, dass Informationssicherheit in Krankenhäusern nun besser dasteht oder besteht noch Handlungspotential?*
**S**: Das hängt auch von der Größe ab. Man kann viel vorgeben als Gesetzgeber. Und wir merken, dass die größeren Krankenhäuser durchaus eine Chance haben, das umzusetzen, weil sie die entsprechende Manpower haben. Die kleineren haben aber damit zu tun, überhaupt ihre Systemlandschaft in all der Komplexität am Laufen zu halten. Es ist ähnlich wie in den Arztpraxen, wo die KBV-Richtlinie zwar Vorgaben macht, der einzelne Arzt aber möglicherweise überfordert ist, diese umzusetzen und sich dann auf Dienstleister verlässt. Ich glaube, die Vorgaben sind an sich richtig und würden sie in der Komplexität komplett umgesetzt und eingehalten, bräuchte man sich wahrscheinlich deutlich weniger Sorgen machen. Allein die Umsetzung und das dauerhafte Nachhalten ist für viele Häuser aber eine Herausforderung und wird auch budgettechnisch nicht abgebildet. Weder vonseiten der Kassen noch der Länder gibt es im Investitionsplan oder auch im Budgetplan explizite Positionen zur IT-Sicherheit.

*Stellt Fachkräftemangel in Ihrer Branche ein großes Problem dar?*
**F**: Je mehr IT entsteht und benötigt wird, desto mehr Personal braucht man auch. Und das ist schwer zu finden. Ist ein Mangel vorhanden? Ich würde sagen, das KHZG hat die Entwicklung begünstigt. Wir haben immer gesagt: Wir würden mehr Maßnahmen umsetzen, wenn wir mehr Geld hätten. Jetzt haben wir das Geld, aber wir haben nicht das nötige Personal dafür.

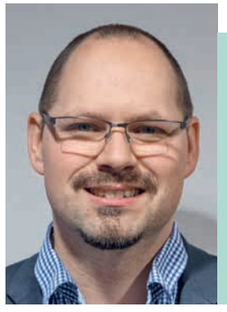
*Wird dem Thema Informationssicherheit überall ausreichend Bedeutung beigemessen oder gibt es durchaus noch Verbesserungspotential?*
**S**: Ich glaube, allen ist bewusst, dass ein IT-Sicherheitsvorfall mit hohen Ausfällen verbunden sein kann. So wie ich es wahrnehme, ist das durchaus in der obersten Ebene angekommen.

**F**: Das Thema Informationssicherheit ist angekommen. Bei der Frage, wer am Ende die Umsetzung macht, passiert oft Folgendes: Wir sprechen von Informationssicherheit, sehr oft wird IT-Sicherheit daraus gemacht. Und in dieser Schublade landet das Thema dann meistens auch. Im Krankenhaus darf man aber nicht vergessen, dass Informationstechnik nicht nur die IT betrifft. Die Haustechnik ist auch beteiligt, genauso die Medizintechnik. Informationssicherheit ist am Ende eine Organisationsaufgabe. Und beim Organisationsversagen haftet die Geschäftsführung, der Vorstand, die Geschäftsleitung. Spätestens da wird jedem bewusst, welche Bedeutung das Thema hat.

*Unserem Gespräch entnehme ich, dass Sie die aktuelle Situation grundsätzlich eher positiv einschätzen. Gibt es dennoch Hürden, die noch überwunden werden müssen?*
**F**: Es gibt genügend Regularien, die definieren, was zu tun ist. Das ist in Ordnung. Das, was an vielen Stellen fehlt, ist das Wie. Jedes Mal, wenn Sicherheitslücken auftreten, soll es die Informationssicherheit lösen. Aber wie soll etwas konkret gemacht werden und wer soll es machen? Das sind Fragen, die am Ende offenbleiben.

## Thorsten Schütz

Der stellvertretende Vorsitzende des KH-IT ist Arzt mit Zusatzbezeichnung „Medizinische Informatik“ und Certified Healthcare CIO. Im Klinikum und Seniorenzentrum Itzehoe samt angeschlossenen MVZs leitet Schütz den Bereich IT und Betriebsorganisation.



## Lars Forchheim

Der Diplom-Wirtschaftsinformatiker ist ebenfalls stellvertretender Vorsitzender des KH-IT. Als Chief Information Officer (CIO) der ANregiomed gKU ist er für Strategie, Changemanagement, Betrieb und Prozessorganisation für drei Krankenhäuser, eine Praxisklinik und sechs MVZs im Landkreis Ansbach und in der Stadt Ansbach verantwortlich.

Interview mit Carsten Meywirth, Leiter der Abteilung „Cybercrime“ im Bundeskriminalamt

# „Gerade im Gesundheitssektor besteht ein erhöhtes Erpressungspotential“

***Die Zahl der Cyberangriffe steigt und damit auch die Gefahr von Unternehmen, Opfer von kriminellen Tätergruppen zu werden. Im Interview mit dem Hartmannbund Magazin erläutert Carsten Meywirth, Leiter der Abteilung Cybercrime im Bundeskriminalamt, ob sich das Vorgehen der Angreifer im Gesundheitswesen von anderen Branchen unterscheidet, warum Cyberkriminalität zunimmt und wieso sich Betroffene häufig scheuen, den Angriff bei der Polizei zu melden.***

*Hartmannbund Magazin: Im aktuellen Bundeslagebild Cybercrime 2021 heißt es, dass das Bedrohungspotential durch Ransomware deutlich angestiegen ist und es der Modus Operandi mit dem höchsten Schadenspotential im Bereich Cybercrime bleibt. Wie gehen die Täter vor?*

**Carsten Meywirth**: Im Wesentlichen gehen die Täter auf zwei Arten vor. Sie können sich Zugangsdaten wie E-Mail-Adresse oder Passwort zu einzelnen Opfern im Internet auf entsprechenden Portalen kaufen. Bei den Zugängen weiß man aber nicht, ob das eine Privatperson ist oder eine Anwaltskanzlei, eine Arztpraxis oder ein Dax-Unternehmen. Vorwiegend verfolgen die Täter aber eine andere Methode. Sie produzieren eine Nachricht und adressieren sie massenhaft an tausende E-Mailadressen. Sie greifen hierbei ein Narrativ auf, das gesellschaftliche Aktualität besitzt, beispielsweise die Corona-Pandemie oder sie nutzen bekannte Marken wie Amazon, Apple, Microsoft. Das soll den Empfänger dazu verleiten, auf einen angehängten Link oder ein angehängtes Dokument zu klicken. Wenn das geschieht, wird der Schadcode heruntergeladen, der dann das Einfallstor der Täter ist. Sind die Täter einmal im System, beginnt die Selektion, das sogenannte Big Game Hunting. Die Tätergruppierungen durchsuchen alles, um zu erfahren, was das für ein Unternehmen ist – wie viel Umsatz macht es, wie viele Mitarbeiter sind dort angestellt, wie hoch sind Einnahmen.

*Spielt es für Cyberkriminelle eine Rolle, in welcher Branche sie zuschlagen? Gibt es spezielle Präferenzen?*

**Meywirth**: Nein. Den Tätergruppierungen ist im Prinzip egal, ob es sich um ein Krankenhaus oder mittelständisches Unternehmen handelt. Es geht einfach nur um die Höhe des Lösegeldes, das sie erzielen können. Sie gehen an die Schmerzgrenze dessen, was das Opfer gerade noch bereit ist zu zahlen, um den Betriebsausfall zu umgehen. Wenn die Täter sehen, bei dem Netzwerk handelt es sich zum Beispiel um ein Krankenhaus, dann vermuten sie ein hohes Erpressungspotential mit entsprechenden Erfolgsaussichten – weil bei einem Betriebsausfall auch sehr kritische Prozesse wie die Notfallversorgung nicht mehr sichergestellt werden können. Das würden sie dann vielleicht erst einmal einer kleineren Arztpraxis vorziehen. Häufig sind die Täter Wochen oder Monate in den Netzwerken unterwegs, schauen sich sehr genau um und exfiltrieren dann auch Daten. Wir nennen das Double Extortion, eine doppelte Erpressung, weil die Unternehmen mit den Daten noch einmal erpresst werden. Gerade im Gesundheitssektor sind das sensible Daten und es besteht ein erhöhtes Erpressungspotential für das Opfer. Es wird ihnen beispielsweise gedroht, diese Daten auf einem Portal zu veröffentlichen, wenn das Unternehmen das Lösegeld nicht zahlt. Eine andere Möglichkeit ist es, die Daten zu verschlüsseln.

*Cybercrime läuft also im Gesundheitswesen nach dem gleichen Schema ab wie in anderen Wirtschaftszweigen auch. Aber was führt dazu, dass die Zahl der Ransomware-Angriffe steigt?*

**Meywirth**: Für das Gesundheitswesen wie für alle anderen Branchen gilt: Seit 2015 erleben wir eine Verdopplung der Straftaten. 2021 haben wir zusätzlich die Steigerung von 12 Prozent. Hintergrund ist, dass bis 2015 einzelne Gruppierungen im Wesentlichen eine Tat von A bis Z selbst begangen haben. Seither stellen wir fest, dass sich eine sehr effiziente Underground Economy etabliert hat, eine illegale Dienstleistungswirtschaft, die von der Struktur, den Leistungen wie Kauf und Verkauf vergleichbar ist mit dem normalen Onlinehandel. Es können dort Schadcodes und spezielle Dienste gekauft oder Hosting-Provider gemietet werden. Wir nennen das Crime-as-a-Service. Dazu kommt der Megatrend Digitalisierung, der 2020 durch die Corona-Pandemie einen zusätzlichen Schub erfahren hat. Es musste sehr schnell auf remote Infrastrukturen umgestellt werden, wir mussten ins Homeoffice, Firmen hatten Arbeitsprozesse außerhalb des physischen Netzwerks zu legen. Nach wie vor verzeichnen wir aber auch eine sehr geringe Aufklärungsquote von unter 30 Prozent. Diese Entwicklungen haben dazu geführt, dass Täter immer mehr Angriffsflächen und eine immer größere Wahrscheinlichkeit für illegale Profite erkannt haben.

*Warum wird denn nur einer von zehn Cyberangriffen bei der Polizei gemeldet?*

**Meywirth**: Es ranken sich gewisse Mythen um dieses Thema. Die Unternehmen glauben, dass wir deren gesamte IT einsammeln und einbehalten. Dass wir, wenn wir einmal Zugänge zu den Informationen aus dem Unternehmen haben, auch nach anderen Straftaten wie Steuerdelikten oder Betrugsdelikten suchen. Und dass wir ihre Bemühungen nachhaltig stören, den Betrieb wiederaufzunehmen. Das stimmt natürlich nicht. Zusätzlich ist die Angst vor einem Reputationsverlust groß, dass durch eine Anzeige die Öffentlichkeit davon erfährt und man sich für den erfolgten Cyberangriff rechtfertigen muss. Ich stelle in den vergangenen Jahren allerdings eine wachsende Bereitschaft fest, Anzeige zu erstatten. Das liegt an den spezialisierten Cybercrime-Dienststellen in den Landeskriminalämtern, die sogenannten ZAC – Zentrale Ansprechstellen von Cybercrime.

*An wen kann man sich wenden, wenn man Opfer eines Cyberangriffs geworden ist?*

**Meywirth**: KRITIS-Unternehmen haben eine Meldeverpflichtung gegenüber dem BSI. Wir sitzen mit dem BSI und anderen Behörden im Nationalen Cyber-Abwehrzentrum und beraten dort über diese herausragenden Fälle und das Vorgehen. Das Bundeskriminalamt, also meine Abteilung „Cybercrime“, ist zuständig für die Ermittlung bei Cyberangriffen auf Kritische Infrastrukturen und Bundeseinrichtungen. Wir haben mit der Quick Reaction Force eine Aufrufeinheit aufgebaut, die 24/7 in Bereitschaft ist und die erste Maßnahmen bei Cybereingriffen einleitet. Kleinere Unternehmen wie Arztpraxen oder Apotheken sollten sich im jeweiligen Bundesland bei der ZAC beim Landeskriminalamt melden. Auch diese sind rund um die Uhr erreichbar.

*Wie lange muss denn vor Ort ermittelt werden?*

**Meywirth**: Das muss im ersten Moment nicht unbedingt vor Ort ablaufen. Das Opfer befindet sich in einer Chaos-Phase und muss mit oberster Priorität den Betrieb wiederherstellen. Dabei können wir ihm nicht direkt helfen, das ist Aufgabe von qualifizierten Mitigations-Dienstleistern. Wir kooperieren mit ihnen und sprechen ab, wann wir Daten erhalten können, die es uns ermöglichen, Ermittlungen aufzunehmen. Diese Kooperation selbst ist sehr einvernehmlich. Wir beraten das Unternehmen dahingehend, wie der Fall einzuschätzen ist, welche Gruppierung dahintersteckt, wie diese in der Vergangenheit vorgegangen ist und wie bei Lösegeldverhandlungen vorzugehen ist. Das kann man zunächst auch alles fernmündlich besprechen, Maßnahmen vor Ort wären dann in Absprache mit dem Mitigations-Dienstleister möglich.

*Was raten Sie Betroffenen – sollen sie auf die Erpressung eingehen?*

**Meywirth**: Wir empfehlen jedem, kein Lösegeld zu zahlen. Einfach, weil nicht klar ist, mit wem da verhandelt wird. Sie wissen nur, dass das keine seriösen Geschäftspartner, sondern Verbrecher sind. Sie wissen nicht, ob die Schlüssel, wenn sie denn geliefert werden, tatsächlich effektiv eingesetzt werden können. Sie wissen nicht, ob die Täter mit Nachforderungen kommen. Es ist in jedem Fall eine Investition in eine illegale Dienstleistungswirtschaft. Die Täter werden durch Lösegeldzahlung vielmehr ermutigt, wiederzukommen. Weil sie wissen, es ist schon einmal gezahlt worden und die Wahrscheinlichkeit hoch ist, dass es wieder geschieht.

*Wie ist Ihre Prognose für die Zukunft? Hat man eine Chance gegen hochprofessionell organisierte Cyberkriminelle?*

**Meywirth**: Es ist zunächst einmal für Unternehmen wie für private Akteure wichtig, eine gute Vorkehrung zu treffen. Es sollte also ein möglichst hohes Level an IT-Sicherheit vorhanden sein. Ich glaube, da ist in Deutschland viel in puncto Sicherheit aufzuholen, insbesondere bei kleineren Unternehmen, die auch im Gesundheitssektor zu finden sind. Wir wissen natürlich, dass selbst das höchste IT-Sicherheitsniveau nicht ausreichend ist, um Kompromittierungen zu entgehen. Bei Ransomware-Angriffen kommt es entscheidend darauf an, ob sich ein Mitarbeiter findet, der auf einen Schadcode klickt oder nicht. Da müssen neben IT-Sicherheitsmaßnahmen entsprechende Ausbildungsmaßnahmen erfolgen. Aber wir brauchen auch eine effektive Strafverfolgung, um die Täter abschrecken zu können. Ich halte es für geboten, was die Cybercrime-Bekämpfung anbelangt, für ein möglichst hohes Abschreckungsniveau zu sorgen. Und das steigt mit den Täterermittlungen, die wir durchführen, und der Anzahl der Täter-Infrastrukturen, die wir zerstören.

Foto: Bundeskriminalamt

## Carsten Meywirth

Carsten Meywirth ist Leiter der Abteilung „Cybercrime“ im Bundeskriminalamt (BKA). Diese wurde im April 2020 eingerichtet. Kriminalbeamten, Analysten und IT-Experten arbeiten zusammen, um deutschlandweit und international Cyberkriminalität zu bekämpfen. Im Januar 2021 war die Abteilung daran beteiligt, die Infrastruktur der Schadsoftware Emotet nachhaltig zu zerschlagen. Diese galt als die gefährlichste Schadsoftware weltweit. Diesen April konnte das BKA den weltweit größten illegalen Darknet-Marktplatz „Hydra Market“ sicherstellen und schließen.

Foto: GreenTech/shutterstock.com

Wie können Attacken verhindert werden, welche Rolle spielen medizinische Geräte und der Mensch?

# Forschen für mehr Sicherheit

***Es herrscht Konsens darüber, dass die Informationssicherheit des Gesundheitswesens mit zunehmender Digitalisierung durch immer mehr Cyberangriffe unter Druck gerät. Wie können unberechtigte Zugriffe auf Krankenhausysteme verhindert werden, welche Rolle spielen medizinische Geräte und der Mensch dabei? Mit diesen Fragen setzt sich die Wissenschaft auseinander, um Menschenleben und Patientendaten künftig in Krankenhäusern noch besser schützen zu können. Wir stellen drei Forschungsprojekte vor.***

Ein diffuses Gefühl. Das war die Ausgangssituation für das Projekt „MITSicherheit.NRW“. Das Wissen darüber, dass es zwar Schwachstellen der IT-Sicherheit im medizinischen Kontext gibt, aber nicht, in welchem Ausmaß diese Schwachstellen tatsächlich auftreten und welche Bedeutung das hat. Das sollte mit dem vom Land Nordrhein-Westfalen und der Europäischen Union geförderten Forschungsvorhaben genauer untersucht und dokumentiert werden. Damit aus dem diffusen Gefühl am Ende Handlungsempfehlungen formuliert werden können, um sich gegen Cyberangriffe zu schützen. Christoph Saatjohann, Doktorand im Labor für IT-Sicherheit an der FH Münster, promoviert zum Thema „IT-Sicherheit in der Medizin“ und forschte am Verbundprojekt, bei dem auch die Ruhr-Universität Bochum und Medizintechnikunternehmen beteiligt waren.

Cyberangriffe beeinträchtigen nicht nur die Krankenhausnetzwerke, sie stellen auch ein Bedrohungspotential für Medizingeräte dar. Was passiert eigentlich, wenn medizinische Geräte Ziel eines Cyberangriffs werden? Eine Prognose in der IT-Sicherheits-Community lautet, dass in Zukunft speziellere Angriffe auf medizinische Geräte durchaus in den Fokus rücken können. Die Motivation der Hacker wäre eine ähnliche wie heute: Geld. Zum einen hätten Täter die Möglichkeit, Hersteller, Praxen oder Krankenhäuser zu erpressen, wenn ein weit verbreitetes Gerät wie ein Herzschrittmacher beziehungsweise sein Home-Monitoring-System gehackt werden. Auch Aktien-Short-Selling wäre denkbar. Eine Investmentgesellschaft wettet beispielsweise darauf, dass der Aktienkurs eines Medizinproduktherstellers in den kommenden Monaten sinken wird. Durch Cyberangriffe können Sicherheitslücken beim medizinischen Gerät festgestellt werden, was dann öffentlichkeitswirksam publik gemacht wird – und so tatsächlich zum Absturz des Aktienkurses führt. Ähnlich spielte sich das beim Herzschrittmacherhersteller St. Jude bereits vor einigen Jahren ab. Und als letztes Beispiel gibt Saatjohan noch gezielte Angriffe auf High-Profile-Personen wie hochrangige Politiker an. Aus Sorge vor einem Angriff dieser Art, ließ der damalige US-Vizepräsident Dick Cheney deshalb die Funkschnittstelle seines Herzschrittmachers deaktivieren.






### *Medizintechnik vor Angriffen schützen*

Im Krankenhausalltag ist dies alles kein Thema. Hier geht es vielmehr darum, Medizintechnik vor Cyberangriffen zu schützen. Deshalb haben die Forscher eine Art Scanner entwickelt, der im laufenden Krankenhausbetrieb die IT-Infrastruktur überprüfen kann – gibt es Probleme auf Rechnern und medizinischen Geräten oder Schwachstellen im Krankenhausnetz? Das ist neu, zuverlässige Scanner, wie sie bei Penetrationstests benutzt werden, gab es bisher noch nicht für medizinische Geräte. Einen weiteren Scanner, den Large-Scale-Scanner, entwickelte das Forschungsteam für ein zweites Projekt innerhalb von „MITSicherheit.NRW“. Mit diesem konnten im Internet zahlreiche Angriffspunkte, also medizinische Geräte, identifiziert werden. Das Ergebnis war deutlicher, als Saatjohann sich das im Vorfeld vorgestellt hatte: Im Dezember 2020 berichteten er und seine Kollegen, dass gut 200 Telematikinfrastruktur (TI)-Konnektoren in Praxen offen übers Internet erreichbar waren, ebenso Röntgenbildarchive. Das lag an der schwachen IT-Sicherung in den Praxen, die, wie Saatjohann ausdrücklich betont, nichts mit der TI zu tun hatten. Das brachte viel Aufmerksamkeit, auch die Tagesschau berichtete. Die Sicherheitslücken wurden dokumentiert, und über das BSI und die Gematik an die entsprechenden Hersteller weitergereicht. Dort wurden die Probleme ernst genommen und versucht, diese abzustellen. Für Saatjohann ist das ein gutes Gefühl, dass er mit seiner Forschung etwas zum Positiven verändern konnte.

„Der Großteil der Angriffe, die im Moment stattfinden, wird noch durch Standardsoftware ermöglicht, die nicht, oder selten, aktualisiert wird – durch alte Systeme wie Windows XP, Windows 7, die in den Krankenhäusern und Arztpraxen noch laufen. Aber in Zukunft muss man sich schon die Frage stellen, was mit den medizinischen Geräten, was mit den medizinischen Protokollen wie DICOM und HL7 ist. Die sind vom Standard her oft unsicher, hier muss etwas getan werden“, erzählt Saatjohann. DICOM und HL7 sind die häufigsten medizinischen Netzwerkprotokolle, die in ganz Deutschland und auch weltweit in Krankenhäusern im Einsatz sind. Und das schon seit Mitte der 1980-er Jahre. Es war also klar, dass es hier Standardprobleme geben musste. Immerhin wurden sie entwickelt, als es noch nicht das Internet von heute gab und somit an aktuelle Cyberangriffsmodelle noch nicht zu denken war. Eine Analyse der Wissenschaftler ergab, dass diese Annahme tatsächlich zutraf: In beiden Protokollen, die dem Datenaustausch dienen, wurden große sicherheitstechnische Probleme, mehrere 100 Sicherheitslücken festgestellt. Es steht fest, dass DICOM und HL7 trotz ihrer Sicherheitslücken noch länger Bestandteil im Krankenhausalltag sein werden. „Jetzt lautet die Frage: Wie sichere ich Geräte trotzdem ab, auch wenn es hier Probleme gibt mit Protokollen oder mit der Software, was kann ich als Krankenhaus tun?“ Das soll die Forschung in Zukunft beantworten.

### *Faktor Mensch: Für den Ernstfall gewappnet sein*

Ende 2021 ist „MITSicherheit.NRW“ nach drei Jahren abgeschlossen worden, die Ergebnisse wurden Anfang Mai dieses Jahres vorgestellt. Saatjohann beschäftigt sich im Nachfolgeprojekt „MedMax“ nun mit den Fragen, wie das Krankenhaus, das per se aus IT-technischer Sicht eine unsichere Umgebung ist, auf Cyberangriffe und –angriffsversuche reagieren soll. Reine Prävention genügt für den Schutz von Krankenhäusern nicht mehr, es müssen neue technische Lösungen und prozessuale Aspekte gefunden werden, um Cyberangriffe rechtzeitig zu erkennen und darauf zu reagieren. „Die Frage lautet nicht, ob ein Hacker-Angriff kommt. Die Gefahr ist da, es werden Krankenhäuser angegriffen werden. Man weiß nur nicht, welche und wann. Das heißt, alle Krankenhäuser müssen dafür gewappnet sein. Technisch natürlich, aber auch menschlich müssen sie darauf vorbereitet sein“, sagt Saatjohann. Es bleibt also noch viel zu forschen.

Der Faktor Mensch nahm in der Forschung von Dr. Christian Dresen einen wichtigen Part ein. Mittlerweile ist der Informatiker beim Beratungsunternehmen Accenture im Bereich Security im Gesundheitswesen tätig. In seiner Doktorarbeit, die er im vergangenen Jahr an der FH Münster schrieb, beschäftigte er sich damit, wie ein Cyberangriff das Patientenwohl beeinflussen kann. Für die Studie, die er in Kooperation mit der Ruhr-Universität Bochum durchführte, kreierte er ein Worst-Case-Szenario, für das es noch kein Beispiel in der realen Welt gab: Ein Cyberangriff auf der Intensivstation. Dresen sorgte dafür, dass nach und nach alle Vitalmonitore verrücktspielten und einen kritisch zu niedrigen Blutdruck anzeigten. Natürlich nicht auf einer Station, sondern im Trainingszentrum des Universitätsklinikums Münster. Eine Pflegekraft sollte eine Nachtschicht mit drei Schauspiel-Patienten betreuen. Eine Kollegin war ebenfalls anwesend. Diese war in die Studie eingeweiht. Die Aufgabe für die Pflegekraft lautete, die Patientendaten am Monitor zu überwachen und eine Infusion zu setzen. Ziel des Experiments war es, herauszufinden, wie mit der Cyber-Attacke umgegangen wird. Ist die Pflegekraft in der Lage, beim Abgleich eines klinischen Bildes vom Patienten mit dem eines manipulierten Bildes vom Monitor zu erkennen, dass etwas nicht stimmt? Dass den Geräten nicht zu trauen ist?

Etwas mehr als die Hälfte der 20 Pflegekräfte habe gemerkt, dass die Monitore falsche Werte anzeigten. Dass dies aber die Folgen eines Cyberangriffs waren, darauf kamen viele nicht. Sie vertrauten auf ihren Instinkt, weil sie sich beispielsweise mit dem Patienten unterhalten konnten, obwohl das nach den Werten auf dem Monitor nicht der Fall hätte sein können. Besonders routinierte Pflegekräfte konnten sich besser von den Monitoren lösen, auf den Gesundheitszustand des Patienten achten, so alles besser überblicken und schließlich die richtigen Entscheidungen treffen. Vielen half der konstruktive Austausch mit der Kollegin. Es kam allerdings auch zu einigen Maßnahmen, die das Leben der Patienten gefährdet hätten. „Am Ende haben wir alle darüber aufgeklärt, was passiert ist. Und ausnahmslos alle haben zwei Dinge gesagt. Erstens: Das war gar nicht in meinem Mindset. Jetzt glaube ich, das ich das in so einer Situation eher erkennen kann. Und zweitens: Es wäre super, in so einer Situation etwas an die Hand zu bekommen“, erläutert Dresen das Studienergebnis. Das Pflegepersonal auf solche Ausnahmefälle vorzubereiten, ihnen eine Richtlinie zur Verfügung zu stellen und sie nicht allein zu lassen, das habe eine große Auswirkung auf die Sicherheit im Klinikalltag. Und für Dresen ist gerade das eine Schlüsselstelle, an der sich in einer Ausnahmesituation viel entscheiden kann: „Die Awareness und die Mitarbeiter sind ein wichtiger Teil der Cyber-Resilienz. Im Endeffekt sind sie es, die verhindern, dass ein Cyberangriff Patientenwohl gefährdet oder zumindest können sie die Situation verbessern.“

Dass es in bestimmten Situationen besonders auf Mitarbeiter ankommt, steht auch im Mittelpunkt von „KISK: Kompetenzorientierte und stellenspezifische IT-Sicherheit für MitarbeiterInnen in Krankenhäusern“. Denn menschliche Fehler machen Cyberangriffe oft erst möglich. Das vom Bundesministerium für Gesundheit geförderte Verbundprojekt ist im Dezember 2021 gestartet und wird bis November 2024 maßgeschneiderte Sicherheitstrainings für verschiedene Berufsprofile an Krankenhäusern ausarbeiten. Die Projektleitung nimmt die Universität Göttingen ein. Weiterhin beteiligt sind das Universitätsmedizin Göttingen, die Universität Hohenheim und 13 assoziierte Partnerkrankenhäuser. „Am Lehrstuhl für

Informationssicherheit und Compliance beschäftigen wir uns intensiv mit dem Thema, wie man Mitarbeiterverhalten dahingehend verbessern und die Mitarbeiter kompetent machen kann, dass sie in verschiedenen Situationen mit Gefahrenpotential wirklich informationssicher reagieren können“, erklärt Projektleiterin Kristin Masuch, Postdoc am Lehrstuhl „Juniorprofessur für Informationssicherheit und Compliance“. Sie sollen nicht nur wissen, welche Gefahren in ihrem Arbeitsbereich vorkommen können, sondern auch die Gefahr im Ernstfall tatsächlich erkennen und entsprechend handeln können. Wie soll also reagiert werden, wenn eine Phishing-Mail im Postfach ist?

### *Krankenhaus als untypischer Angriffsort*

In Kooperation mit der Wirtschaftspädagogik an der Universität Hohenheim haben die Wissenschaftlerinnen und Wissenschaftler festgestellt, dass aktuelle Informationssicherheitstraining nicht die Vielfalt abbilden, die notwendig ist, um die Kompetenz der Mitarbeiterinnen und Mitarbeiter zu steigern. „Gerade im Krankenhauskontext sind die Informationssicherheitstrainings, die aktuell dort angeboten werden – wenn sie überhaupt angeboten werden –, sehr generisch und nicht unbedingt auf diesen Bereich, sondern eher auf andere Wirtschaftsunternehmen zugeschnitten. Sie sprechen dementsprechend nicht zwangsläufig die Jobprofile an, die in einem Krankenhaus existieren. Als Konsequenz erfahren die Mitarbeiter vielleicht nicht, welche Gefahren es in ihrem speziellen Job gibt und wie sie darauf reagieren müssen“, sagt Kristin Masuch. Unterscheiden sich Wirtschaftsunternehmen im Alltag so deutlich vom Klinikalltag? Natürlich gibt es in Krankenhäusern auch typische Büroarbeitsplätze. Doch zusätzlich gibt es eben auch diverse weitere Jobprofile, in denen Personen beispielsweise hauptsächlich Patientenkontakt haben oder im Labor arbeiten – Ärzte, Pflegepersonal, eventuell auch medizinisch-technische Assistenten. Vielleicht haben sie auch keinen eigenen Zugang zu einem Rechner oder dieser steht in einem Zimmer, zu dem auch andere Personen Zutritt haben. Die Art, wie Angriffe durchgeführt werden, um Patienten- oder Kundendaten zu stehlen, kann sich also komplett voneinander unterscheiden, erklärt Kristin Masuch. Während man mit festem Büroarbeitsplatz Opfer von gezielten Phishing-Angriffen über E-Mails oder Telefon werden kann, wird der Angreifer im Krankenhaus vielleicht eher anders vorgehen.

Um mehr über die verschiedenen Berufsprofile und die jeweils spezifischen Gefahrensituationen im Krankenhaus zu erfahren, werden derzeit Interviews mit Informationssicherheitsbeauftragten der verschiedenen Krankenhäuser geführt. Das Ziel ist es, anhand dieser Informationen ein Training für jede Berufsgruppe zu konzipieren. Es soll nicht ein Training für alle Mitarbeiter geben, so wie es aktuell noch der Fall ist. Stattdessen soll jeder entsprechend seines Anforderungsprofils so trainiert werden, dass es handlungsnah ist und den tatsächlichen Arbeitsalltag samt den Gefahren, die dort vorkommen können, widerspiegelt. Um den Erfolg dieser Trainings zu überprüfen, werden auch passende Kompetenzmessinstrumente entwickelt. Mit diesen soll im Verlauf des Projektes drei Mal ermittelt werden, welche Wissenslücken die Mitarbeiter zum Beispiel aufweisen. So erfahren die Wissenschaftler am Ende, wenn die Informationssicherheitstrainings im Krankenhaus durchgeführt werden, ob dadurch die Mitarbeiterkompetenz wirklich verbessert wird.

Nun ändern sich die Strategien und Charakteristiken von Cyberangriffen ständig – wie steht es da um die langfristige Wirksamkeit der Trainings, die erarbeitet werden sollen? Kristin Masuch sieht trotz der Schnelllebigkeit in der Informationssicherheit kein Hindernis dafür, dass die Trainings auch in Jahren noch aktuell sein werden. Die Berufsbilder werden sich in Zukunft nicht gravierend ändern, zudem werde sich bemüht, künftige Entwicklungen im Klinikalltag zu berücksichtigen. Dreh- und Angelpunkt der Trainings sei es, dem Personal Wissen zu vermitteln, wo im jeweiligen Beruf Sicherheitsrisiken bestehen, mit welchen wichtigen Werte sie zu tun haben, auf die es Angreifer abgesehen haben könnten, und wie mit Problemen umgegangen werden soll. Dadurch ist das Personal in der Lage, erlernte Fähigkeiten auch auf andere Angriffe übertragen zu können und zu verstehen, wo weitere Risiken bestehen, erklärt Masuch.

Das Interesse von Krankenhäusern, am Projekt teilzunehmen, war übrigens groß, erzählt die Projektleiterin. Wer nicht mehr bei KISK teilnehmen kann, wird nach Abschluss des Projekts vielleicht trotzdem davon profitieren können: Ein Katalog mit den Trainings für die verschiedenen Anforderungsprofile soll veröffentlicht werden und für alle frei zugänglich sein. Dieser soll anderen Krankenhäusern dann als Vorlage dienen, sich und ihre Mitarbeiterinnen und Mitarbeiter cybersicher aufzustellen.


Foto: Daniell Li

*Kristin Masuch*
*Chair of Information Security and Compliance*


Foto: privat

*Christian Dresen*


Foto: privat

*Christoph Saatjohann*





Prävention, Detektion und Reaktion

# Die Polizei rät zum Dreiklang

***Das Landeskriminalamt Berlin empfiehlt einen „Dreiklang“ aus Prävention, Detektion und Reaktion, um sich gegen Cybercrime zu schützen.***

## ▶ PRÄVENTION

Ein ganzheitliches Sicherheitskonzept ist notwendig. Der Ist-Zustand des Unternehmens oder der Organisation sollte festgestellt und die wichtigsten Informationen und Daten identifiziert werden. Darunter werden alle Daten verstanden, die für den Weiterbetrieb des Unternehmens unabdingbar sind. Ein sehr wichtiger Baustein der Prävention ist ein auf das jeweilige Unternehmen angepasstes Backup-Konzept, das diese Daten absichern soll. Das Backup sollte getrennt vom laufenden IT-System aufbewahrt werden (sogenanntes kaltes Backup) und über einen längeren Zeitraum zurückreichen. Des Weiteren sollten Mitarbeiterinnen und Mitarbeiter regelmäßig, unregelmäßig und kreativ sensibilisiert werden. Eine einmalige Schulung oder Erinnerungs-E-Mails mit identischem Inhalt im Abstand einiger Wochen wird wenig Effekt haben. Es sollten sich immer neue Methoden zur Mitarbeiterschulung angeboten werden, um sich der unberechenbaren Herangehensweise von Tätern anzunähern. Es sollte nicht vergessen werden: Die Cyberkriminellen zielen deutlich auf den Menschen als Schwachstelle der IT-Infrastruktur. Deshalb ist eine entsprechende Fehlerkultur im Unternehmen wichtig. Eine schnelle adäquate Reaktion ohne Furcht vor Konsequenzen kann Schäden erheblich minimieren.

## ▶ DETEKTION

Das ganzheitliche Sicherheitskonzept sollte umgesetzt, regelmäßig überprüft und angepasst werden. Sicherheitsstandards sind regelmäßig zu kontrollieren und Verstöße zu sanktionieren.

## ▶ REAKTION

Es werden vorher konzipierte und möglichst eingeübte Handlungsketten umgesetzt. Dazu gehört die Alarmierung der Entscheider, IT-Verantwortlichen sowie – wenn vorhanden – weitere Personen des Krisenstabs.

Foto: Ajdin Kamber/shutterstock.com


## Was ist im Falle eines Angriffs zu tun?

# Bei einem Cyberangriff zählt jede Minute

***Bei einem Cyberangriff zählt jede Minute – nicht nur, um die IT-Sicherheit wiederherzustellen und so möglichst Schaden durch die Attacke abzuwenden oder kleinzuhalten. Auch für Praxisinhaber und Krankenhausbetreiber gilt es, keine Zeit zu verlieren und alle erforderlichen Schritte jenseits der IT-Sicherheit einzuleiten. Nur so können erhebliche Geldbußen durch Aufsichtsbehörden vermieden werden. Was muss bei einem Sicherheitsvorfall beachtet werden? Und wer sollte auf welche Weise darüber informiert werden? Rechtsanwalt Alexander Helle erklärt, worauf es ankommt.***

***Ich bin von einem Cyberangriff betroffen. Was muss ich jetzt tun?***

Im Idealfall ist man auf diesen Fall vorbereitet und befolgt einen Notfallplan, bei dem klar ist, welche Punkte abzuarbeiten und welche IT-Experten zu benachrichtigen sind. Nach einem solchen Notfallplan kann es sinnvoll sein alle Programme bzw. potenziell betroffene Rechner abzuschalten, um den Schaden eines Cyberangriffs zu minimieren. Aber sobald der Angriff als solcher unterbrochen ist und festgestellt wird, dass der Datenschutz verletzt wurde, muss der Verantwortliche – also der Praxisinhaber oder in Krankenhäusern die Geschäftsführung – den Sicherheitsvorfall der zuständigen Aufsichtsbehörde melden. Und das, wie es in der Datenschutzgrundverordnung Artikel 33, Absatz 1 steht, unverzüglich binnen 72 Stunden. Jede Verzögerung muss begründet werden. Die genannten Fristen gelten auch an Feiertagen und am Wochenende. Die 72 Stunden beginnen mit Kenntnis der Datenschutzverletzung. Zudem besteht nach Artikel 33, Absatz 5 eine interne Dokumentationspflicht. Das heißt, der Verantwortliche muss den Vorfall und alle eingeleiteten Maßnahmen protokollieren, auch damit dies der Aufsichtsbehörde nachgewiesen werden kann.

***Es wurden Patientendaten verschlüsselt. Muss ich die Betroffenen informieren?***

Die betroffenen Patienten sind ebenfalls unverzüglich zu informieren. Auch das steht in der Datenschutzgrundverordnung, Artikel 34, Absatz 1: „Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.“ Was heißt unverzüglich? Nach der Datenschutzgrundverordnung ist hier keine exakte Frist definiert. In der deutschen Rechtsprechung ist das Wort „unverzüglich“ umgangssprachlich definiert als „kurzfristig, ohne schuldhaftes Zögern“, was wiederum etwa eine Woche bedeutet. Die Frage ist nun, wer alles benachrichtigt werden muss, und das in nachvollziehbarer Weise. Konnte der Cyberangriff unterbrochen werden, sind möglicherweise nicht der gesamte Datensatz und somit nicht alle Patienten betroffen. Idealerweise können das die IT-Experten feststellen und ab diesem Zeitpunkt – also mit Kenntnis der Datenverletzung für die betroffene Person – beginnt die Frist für die Benachrichtigung. Kann nicht eindeutig identifiziert werden, welche Patientendaten kompromittiert sind, sollten alle Patienten informiert werden, dass ihre Daten betroffen sein könnten.

***Wie sollen die Patienten von dem Vorfall benachrichtigt werden?***

Das muss auf sicherem Weg erfolgen, also kommt nur ein Telefonat oder ein verschlossener Brief infrage. Per E-Mail ist es schwierig, da diese meist (noch) nicht Ende-zu-Ende-verschlüsselt sind bzw. die Server der Emailanbieter im Ausland (bspw. USA) stehen. Eine Alternative ist eine E-Mail mit einem verschlüsselten Anhang, wobei sich hierbei die Frage stellt, wie der Empfänger den digitalen Schlüssel erhält. Generell bietet sich deshalb eher ein Serienbrief an, der an alle Patientinnen und Patienten verschickt werden kann und in dem kurz über den Vorfall und die bisher erfolgten Maßnahmen berichtet wird. Auch wenn dies nicht zwingend per Einschreiben erfolgen muss, wäre dies aus Beweisgründen aber sicherlich sinnvoll.

***Welche juristischen Folgen können auf mich zukommen?***

Zum einen wird die Datenschutzaufsichtsbehörde den Vorfall genau prüfen. Wurden die Daten nach außen abgesichert? Lag ein Datenschutzkonzept vor, wurde sich an einschlägige Standards hinsichtlich der IT-Sicherheit gehalten wie beispielsweise regelmäßige Updates der IT-Systeme? Hat die Aufsichtsbehörde etwas am Vorgehen oder am Sicherheitsmanagement auszusetzen, wird ein entsprechendes Bußgeld verhängt. Dazu zählt übrigens auch, wenn der zuständige Landesdatenschutzbeauftragte nicht rechtzeitig oder nicht vollständig informiert wurde. Nach Datenschutzgrundverordnung Artikel 83, Absatz 4 können auf Verstöße Geldbußen von bis zu 10 000 000 Euro verhängt werden, wobei hier ein erheblicher Ermessenspielraum (im Prinzip 0 Euro bis 10 Mio. Euro) gegeben ist.

Zum anderen besteht die Möglichkeit, dass die betroffene Person, deren Daten publik geworden sind, dadurch einen materiellen oder immateriellen Schaden erleidet. Diese betroffene Person hat dann möglicherweise gegenüber demjenigen, der sein System nicht vernünftig geschützt hat, einen Anspruch auf Schadenersatz.

Wurden alle Verpflichtungen erfüllt, besteht Spielraum, bezogen auf das „Ob“ und natürlich die Höhe einer etwaigen Geldbuße. Keine Software ist hundertprozentig sicher, das ist technisch nicht möglich. Ein Cyberangriff kann jederzeit vorkommen. Das wird auch von den Aufsichtsbehörden berücksichtigt.

Foto: Michael Danner


## Alexander Helle

Alexander Helle ist Fachanwalt für Medizin- und Arbeitsrecht sowie zertifizierter Datenschutzbeauftragter. Er ist am Berliner Standort der Anwaltskanzlei Meyer-Köring tätig.






## 126. Deutscher Ärztetag in Bremen

# Das Ringen um Prävention, Digitalisierung und GOÄ

***Es war der emotionalste Moment der feierlichen Eröffnung des 126. Deutschen Ärztetages: Minutenlanger Applaus der 250 Delegierten für Andriy Bazylevych, Vorstandsmitglied der Ukrainian Medical Association und Präsident der Weltförderation Ukrainischer Ärztlicher Vereinigungen, der vom Präsidenten der Bundesärztekammer, Dr. Klaus Reinhardt, in der Bremer „Glocke“ herzlich begrüßt wurde.***

Ein klares Zeichen der Solidarität, die auch in der Rede des BÄK-Präsidenten besonderen Ausdruck fand. Ansonsten gab es unmissverständliche Botschaften an die Politik, vor allem in Richtung von Bundesgesundheitsminister Prof. Karl Lauterbach, der sich von der ersten Reihe aus davon überzeugen konnte, dass die deutsche Ärzteschaft klar formulierte Erwartungshaltungen mit Blick auf die zentralen Herausforderungen der deutschen Gesundheitspolitik hat.

Dazu gehörten – analog zum Krankenhauszukunftsgesetz – die Forderung nach einem „Praxiszukunftsgesetz“ zur Finanzierung digitaler Vernetzungsprojekte, der Appell zur Eindämmung von Private Equity als wichtige Maßnahme gegen die fortschreitende Kommerzialisierung in der Medizin oder etwa die Mahnung, der Prävention mehr Gewicht in der Gesundheitspolitik einzuräumen. Ein Gastgeschenk gab es für den Minister auch. Reinhardt übergab ihm die gebundene „Erstausgabe“ der novellierten GOÄ. Auf dieser Basis, davon zeigte sich der BÄK-Präsident überzeugt, sollte einer zeitnahen politischen Umsetzung nichts mehr im Wege stehen. Der Minister kündigte eine „unvoreingenommene Prüfung“ an.

Im Mittelpunkt der vier Bremer Tage standen die aktuell zentralen Mammutaufgaben der Gesundheitspolitik, die die Entsandten der Kammern aus ganz Deutschland derzeit beschäftigen. Dazu gehörten u. a. als Schwerpunktthema die Auswirkungen der Corona-Pandemie auf Kinder und Jugendliche. Die Jüngsten hätten einen hohen Preis bezahlt. Vereinsamung, Bildungsdefizite, häusliche Gewalt: Das seien nur einige der Folgen, unter denen sie litten. Jetzt gelte es, umfangreiche Unterstützungs- und Hilfspakete zu schnüren und Kinder und Jugendliche bei allen künftigen Corona-Maßnahmen in den Mittelpunkt zu stellen.

Als Lehre aus der Corona-Pandemie wurde auch die Einführung eines bundesweiten zentralen Impfregisters gefordert. Mit dem Register sollen sowohl valide Daten über die Impfquote ermittelt als auch Erkenntnisse über die Sicherheit und Wirksamkeit von Impfstoffen gewonnen werden. In einem weiteren Beschluss sprach sich der Ärztetag klar gegen Impfungen in Apotheken aus.


*Gehör und Aufmerksamkeit verschafften sich die Studierenden gemeinsam mit den Assistenzärztinnen und -ärzten des Verbandes. Vor dem Plenarsaal machten sie aus ihrer jeweiligen Perspektive mit einer symbolischen Aktion auf Missstände im Klinikalltag aufmerksam. Bei den Delegierten stießen sie mit ihrer Aktion auf offene Ohren, auch BÄK-Präsident und Hartmannbund-Vorsitzender Dr. Klaus Reinhardt war begeistert.*

Der Deutsche Ärztetag hat den Verordnungsgeber dann nochmals explizit aufgefordert, die Reform der Gebührenordnung für Ärzte (GOÄ) jetzt umzusetzen. Die Bundesärztekammer, der Verband der Privaten Krankenversicherung und die Beihilfe hätten hierfür in jahrelanger intensiver Arbeit einen gemeinsamen Vorschlag entwickelt. Sollte der Verordnungsgeber die GOÄneu nicht bis zum 31.12.2022 in Kraft setzen, fordern die Abgeordneten die Bundesärztekammer auf, die Ärzteschaft über die rechtskonforme Möglichkeit der Anwendung besonderer Honorarvereinbarungen (sog. Abdingung) mit höheren Steigerungsfaktoren als dem 2,3-fachen Regelsteigerungssatz zu informieren.

Auch ein klares Signal in der Telematik-Frage wurde gesendet. In vielen Beschlüssen wurden das BMG und die gematik aufgefordert, die Serien von Pleiten, Pech und Pannen zu beenden und die kommenden Anwendungen e-Rezept und e-AU erst einzuführen, wenn es aussagekräftige, erfolgreich abgeschlossene Feldtests gäbe. Der BÄK-Vorstand hat zudem ein Kalkulationstool vorgestellt, mit dem der im Krankenhaus tatsächlich anfallende Bedarf an ärztlicher Leistung errechnet werden kann. Darin einbezogen seien sämtliche Leistungen, die Klinikärztinnen und -ärzte in ihrem Alltag erbringen.

Die Zusatzbezeichnung Homöopathie wird in der (Muster-)Weiterbildungsordnung (MWBO) gestrichen: Das wurde mit großer Mehrheit beschlossen. Wissenschaftliche Studien, die einen evidenzbasierten Einsatz der Homöopathie belegen, fehlten, hieß es zur Begründung. Heiß diskutiert wurde auch die Frage, wie Fehlzeiten in der Weiterbildung fair anerkannt werden können. Der Antrag des BÄK-Vorstandes wurde schließlich angenommen. „Grundsätzlich“ können demnach längere Fehlzeiten anerkannt werden. Die Abgeordneten forderten zudem die Klinikleitungen in einem Antrag aus den Reihen des Hartmannbund auf, die Qualität des Praktischen Jahres (PJ) zu priorisieren. In diesem Zusammenhang dürften Medizinstudierende im PJ nicht mit pflegerischen, sondern mit ärztlichen Aufgaben betraut werden. Auch müssten diese eine einheitliche angemessene Aufwandsentschädigung erhalten.

Hinsichtlich des steigenden Kommerzialisierungsdrucks wurde ein Maßnahmenkatalog für die ambulante und stationäre Versorgung beschlossen. Darin fordert die Ärzteschaft unter anderem, die Gründung von Medizinischen Versorgungszentren (MVZ) durch Krankenhäuser an einen fachlichen, räumlichen und regionalen Bezug zu deren Versorgungsauftrag zu koppeln. An die Klinikleitungen wurde die Forderung adressiert, den ökonomischen Druck auf die Ärzteschaft sowie bürokratische Aufgaben zu reduzieren.

Der 127. Ärztetag in Essen im kommenden Jahr heißt übrigens weiterhin „Deutscher Ärztetag“. Ein emotional diskutierter Antrag, eine gendergerechte Sprache in der Namensgebung umzusetzen, wurde mehrheitlich abgelehnt. Auf gendersensible Formulierungen u. a. in Anträgen muss in Zukunft hingegen geachtet werden. Weitere Beschlüsse, Bilder und Videos vom Ärztetag finden Sie unter: ***www.hartmannbund.de/daet_2022***

Erste Positionierungen der Beteiligten

# Ambulantisierung im Konsens?

***Im Mai 2022 wurden die Mitglieder der „Regierungskommission für eine moderne und bedarfsgerechte Krankenhausversorgung“ benannt. Die Expertenkommission soll Empfehlungen und Leitplanken für eine Krankenhausreform vorlegen. Ein gewichtiger Auftrag der Reform-Agenda lautet, die Möglichkeiten einer „Ambulantisierung“ der medizinischen Versorgung umfänglich auszuloten.***

Der Koalitionsvertrag der Ampel-Koalition sieht in diesem Zusammenhang vor, „zügig für geeignete Leistungen eine sektorengleiche Vergütung durch sogenannte Hybrid-DRG“ umzusetzen, um die Ambulantisierung von unnötig stationär erbrachten Leistungen zu fördern. Laut einem Gutachten des IGES Instituts können viele der medizinischen Leistungen, die derzeit stationär erbracht werden, auch ambulant angeboten werden. Ärzteschaft, Krankenhäuser und Krankenversicherungen haben sich zur „Ambulantisierung“ positioniert.

### *Empfehlungen als Reformen-Grundlage*

Die im Koalitionsvertrag vorgesehene „Regierungskommission für eine moderne und bedarfsgerechte Krankenhausversorgung“ ist mit 15 Expertinnen und Experten aus der Versorgung (Pflege und Medizin), der Ökonomie, der Rechtswissenschaften und einem an das BMG angebundenen Koordinator, Professor Dr. Tom Bschor, Facharzt für Psychiatrie und Psychotherapie und langjähriger Chefarzt der Abteilung für Psychiatrie der Schlosspark-Klinik Berlin und stellvertretender Vorsitzender der Berliner Gesellschaft für Psychiatrie und Neurologie, besetzt. Die Empfehlungen der Kommission sollen Grundlage der Reformen im stationären Bereich ab dem Jahr 2023 werden. Die letzte „wirklich große“ Reform liege 20 Jahre zurück, erklärte Bundesgesundheitsminister Lauterbach Anfang Mai vor der Presse. Die Krankenhausreform sei für ihn neben der Digitalisierung ein zentraler Bereich. Die Kommission solle zunächst aber ohne direkte Beteiligung der Krankenkassen oder der Krankenhausgesellschaft selbst arbeiten. Sie sei eine „wissenschaftsorientierte Kommission“. „Die beteiligten Krankenhäuser, Krankenhausgesellschaft, Krankenkassen aber auch die Länder werden natürlich im Rahmen der Arbeit dieser Kommission angehört“, versicherte der Minister.

Die Regierung der letzten Legislaturperiode aus Union und SPD hatte mit dem MDK-Reformgesetz von 2020 die Kassenärztliche Bundesvereinigung (KBV), den GKV-Spitzenverband und die Deutsche Krankenhausgesellschaft (DKG) dazu verpflichtet, den AOP-Katalog (Katalog ambulant durchführbarer Operationen und sonstiger stationsersetzender Eingriffe im Krankenhaus) zu überarbeiten und ein Vergütungssystem auf Basis des Einheitlichen Bewertungsmaßstabs (EBM) zu erarbeiten. Der EBM regelt die Höhe der Honorare in der ambulanten Versorgung der niedergelassenen Ärzte.

Das im Auftrag von KBV, GKV-Spitzenverband und DKG erstellte Gutachten des IGES Instituts sieht für 2.476 medizinische Leistungen (gemäß Operationen- und Prozedurenschlüssel – OPS) grundsätzlich Ambulantisierungspotential und damit die Möglichkeit den AOP-Katalog, auszubauen – „ein Plus um 86 % auf insgesamt 5.355 Leistungen“. Die vom IGES-Institut für eine Erweiterung des AOP-Katalogs empfohlenen Operationen und Prozeduren wurden im Jahr 2019 insgesamt rund 15 Mio. Mal zur vollstationären Behandlung von Patienten durchgeführt. Das sind mehr als ein Viertel aller etwa 58 Mio. vollstationär erfolgten Leistungen. Am häufigsten waren diagnostische Maßnahmen, die gut sieben Millionen Mal stationär vorkamen, überwiegend die Endoskopie, meist von Magen und Darm. Je nach patientenindividueller Situation, also dem Behandlungskontext, könnten diese Leistungen zukünftig teilweise ambulant durchgeführt werden.

Die Gutachter empfehlen ergänzend ein Prüfverfahren, im Gutachten Kontextprüfung genannt, zu implementieren, mit dem Kliniken fallindividuell begründen können, warum sie Patienten, wenn nötig, doch stationär behandeln. Gründe dafür könnten erhöhte Krankheitsschwere, altersbedingte Risiken, soziale Begleitumstände oder erhöhte Betreuungsbedarfe der Patienten sein, also der jeweilige Behandlungskontext. Eine ambulante Durchführung entfällt auch, wenn eine AOP-Leistung nur eine ausschließlich stationär mögliche Behandlung begleitet.

### *Neuer Bereich ideal für Hybrid-DRGs*

Die Nutzung ambulanter Potenziale werde aus Sicht der DKG wesentliche Voraussetzung sein, um dauerhaft eine wirtschaftliche und qualitativ hochwertige Versorgung in Deutschland gewährleisten zu können, sagte Dr. Gerald Gaß, Vorstandsvorsitzender der DKG, anlässlich der Veröffentlichung des IGES-Gutachtens. „Wir begrüßen das Ergebnis des Gutachtens zur Anpassung und Erweiterung des AOP-Katalogs und unterstützen den Ansatz, dass deutlich über eine reine Anpassung des Katalogs hinausgegangen wurde. Wir sind überzeugt, dass die Nutzung der ambulanten Potenziale der Krankenhäuser in Zukunft ein echter Mehrwert für die Patientenversorgung sein wird.“ Ein solcher klinisch-ambulanter Leistungsbereich an den Krankenhäusern könne ideal mit den im Koalitionsvertrag angesprochenen Hybrid-DRGs vergütet werden. „Damit werden starke Anreize für eine Ambulantisierung bisher vollstationärer Leistungen gesetzt und allein medizinische Aspekte bei der patientenindividuellen Wahl des Behandlungsortes in den Mittelpunkt gestellt“, so Gaß.

Auf dem DRG-Forum Mitte März zeigte sich Gaß „zutiefst“ davon überzeugt, „dass wir in den kommenden Jahren noch stärker vor allem natürlich in den Flächenländern, in den Regionen auf die Situation zulaufen, dass die medizintechnische Infrastruktur und die breite Interdisziplinarität, die man braucht um gute Patientenbehandlungen zu machen, dass die in erster Linie an Krankenhausstandorten konzentriert und vorgehalten werden kann.“ Das heiße aber nicht, dass dort nur Krankenhaus-Mitarbeiterinnen und -Mitarbeiter tätig sein müssten. Gaß könne sich sehr gut vorstellen, dass diese medizintechnische Infrastruktur daneben noch viel stärker als das bisher der Fall sei, auch gemeinsam genutzt werden könne. Falls notwendig, könne man dann das Institut für das Entgeltsystem im Krankenhaus (InEK) beauftragen, für solche Fälle Hybrid-DRGs zu entwickeln. Ein weiterer Vorteil dabei: „Bei gleicher Vergütung für die ambulant oder stationär erbrachte Leistung gibt es vermutlich keine Diskussionen mit dem Medizinischen Dienst.“

Bei der Reform des AOP-Katalogs sehe er die Möglichkeit, die berühmten „gleich langen Spieße“ von ambulantem und stationärem Sektor endlich einmal Wirklichkeit werden zu lassen, so der Vorstandsvorsitzende der Kassenärztlichen Bundesvereinigung, Dr. Andreas Gassen. „Mein Petitum war und ist: Wer gemäß Kriterienkatalog über die personellen, räumlichen und technischen Voraussetzungen verfügt, der darf mitmachen, egal, ob Krankenhausarzt oder -ärztin oder niedergelassen. Was nicht sein kann, ist, den Leistungskatalog unter dem Aspekt des Bestandsschutzes für Krankenhäuser zu definieren. Auch müsse der Facharztstandard gegeben sein.

### *Postoperative Pflegekapazitäten fehlen*

Der Berufsverband der Deutschen Chirurgen (BDC) plädierte im April 2022 dafür, die Aufnahme von Eingriffen in einen neu zu definierenden ambulanten Leistungskatalog lediglich auf Behandlungen zu beschränken, die „in der Regel“ ambulant durchgeführt werden könnten. Eine Ausweitung des ambulanten Leistungskataloges in der Breite, wie es im IGES-Institut dargestellt wird, lehnt der BDC ab. Das überschreite den gesetzlichen Auftrag und wäre zudem mit einem „unüberschaubaren Prüfaufwand“ im stationären Bereich verbunden, erklärte Hans-Joachim Meyer, Präsident des BDC. Das deutsche Gesundheitssystem sei infrastrukturell auf eine solche Ambulantisierungswelle nicht vorbereitet. Es mangele beispielsweise an Pflegekapazitäten für die postoperative Betreuung von Patienten zu Hause. Die Selbstverwaltung solle nun zunächst alle in der Regel ambulant zu erbringenden Eingriffe identifizieren und in den AOP-Katalog überführen.

Der AOK-Bundesverband hat jüngst einen einheitlichen Ordnungsrahmen für das ambulante Operieren gefordert. „Viele Behandlungen, die bisher im Krankenhaus stattfinden, sind auch ambulant gut durchführbar – da sind sich alle Akteure im Gesundheitswesen einig“, sagte Sabine Richard, Geschäftsführerin Versorgung im AOK-Bundesverband. Problematisch sei jedoch, „dass bei diesem Thema gerade zwei Prozesse völlig ohne Abstimmung parallel laufen“. Gemeint sind der gesetzliche Auftrag der letzten Bundesregierung zu einer Überarbeitung des AOP-Katalogs und des Vergütungssystems durch Krankenkassen, Ärzteschaft und Krankenhäuser auf der einen Seite und der Plan Hybrid-DRGs umzusetzen der jetzigen Bundesregierung auf der anderen Seite. Die AOK-Expertin forderte einen Stopp der noch von der Großen Koalition angestoßenen AOP-Reform. „Nötig sind eine gute sektorenübergreifende Versorgungsplanung, wie sie ja auch im Koalitionsvertrag vorgesehen ist, und ein wirtschaftliches, sektorengleiches Vergütungssystem auf einer klaren vertraglichen Grundlage“, unterstrich Richard. Der Fokus müsse dabei auf den Leistungen liegen, die heute noch unnötigerweise im Krankenhaus erbracht würden.

Allerdings, darauf wird auch in der gesundheitspolitischen Diskussion hingewiesen, müsste die Regierungskoalition zunächst Hybrid-DRGs definieren, und auch, inwieweit diese zu einer sektorenübergreifenden Versorgung führen oder aber in den getrennten Bereichen nach gleicher Vergütung erfolgen soll. In diesen Fragen gründet sich unter anderem der nach wie vor schwelende Konflikt zwischen Krankenhäusern und Vertragsärzteschaft.

*Ein klinisch-ambulanter Leistungsbereich an den Krankenhäusern könne ein Gewinn sein.*

Foto: imageFlow/shutterstock.com

POLITIK

Opt-in oder Opt-out?

# Sinnvolle Maßstäbe für ein überfälliges Gesundheitsdatennutzungsgesetz

***„Trotz der großen Potenziale, die mit der Digitalisierung für die Verbesserung der Versorgung sowie die Weiterentwicklung des Gesundheitswesens verbunden werden, liegt Deutschland im internationalen Vergleich weit hinter anderen europäischen Ländern zurück“, heißt es im Jahresgutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands 2022 der Expertenkommission Forschung und Innovation (EFI). Die Gründe hierfür seien „vielschichtig“; unter anderem werden „Abwägungen und Sorgen bezüglich des Datenschutzes“ genannt.***

Insbesondere bei der elektronischen Patientenakte (ePA), dem „Kernelement eines digitalisierten Gesundheitssystems“, wird noch über das Zugriffsmanagement und Zustimmungsverfahren für die Nutzung der Gesundheitsdaten diskutiert. Die Expertenkommission spricht sich für eine bessere Nutzung von Gesundheitsdaten insbesondere in der Forschung und Entwicklung aus. Der 126. Deutsche Ärztetag hat die Bundesregierung am 27. Mai aufgefordert, das im Koalitionsvertrag von SPD, Bündnis 90/Die Grünen und FDP angekündigte Gesundheitsdatennutzungsgesetz zügig zu entwickeln und die Ärzteschaft aktiv in den Prozess einzubeziehen.

„Eine digitale Infrastruktur, die alle Akteure des Gesundheitssystems miteinander vernetzt und die einen sicheren, organisationsübergreifenden Informations- und Datenaustausch ermöglicht, ist Grundlage für eine erfolgreiche Digitalisierung“, wird im EFI-Gutachten erklärt, das am 9. März 2022 veröffentlicht und an Bundesforschungsministerin Bettina Stark-Watzinger MdB (FDP) übergeben wurde. In Deutschland soll die Telematik-Infrastruktur (TI), die „Datenautobahn des Gesundheitswesens“, diese Aufgaben erfüllen. Sie besteht aus dezentralen Komponenten wie beispielsweise Kartenlesegeräten sowie zentralen Hardware- und Software-Komponenten, zu denen u. a. der sichere E-Mail-Dienst Kommunikation im Medizinwesen (KIM) gehört. Diese Komponenten und Dienste sollen die technische Plattform für die Vernetzung von Akteuren und für das Angebot von Fachanwendungen – wie z. B. der elektronischen Patientenakte (ePA) – bereitstellen. Die ePA soll die „wichtigsten gesundheitsrelevanten Informationen von Versicherten in einem digitalen Dokumentationssystem“ erfassen und diese Informationen Leistungserbringern fach-, einrichtungs- und sektorenübergreifend zur Verfügung stellen.

*Für die Einrichtung der ePA etc. ist derzeit im Patientendaten-Schutzgesetz ein mehrstufiges Zustimmungsverfahren (Opt-in-Verfahren) durch die Versicherten vorgesehen.*

Grafik: PopTika/shutterstock.com

### *Im Spannungsverhältnis zwischen IT-Sicherheit und Datenschutz*

Die Fachanwendungen, Komponenten und Dienste der TI werden entsprechend den gesetzlichen Vorgaben – dies umfasst auch die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) – spezifiziert. Die Einhaltung der gesetzlichen Grundlagen bzgl. der Fachanwendungen, Komponenten und Dienste der TI wird durch die gesetzlich geforderte Einbindung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bei der Erstellung der technischen Vorgaben durch die gematik sichergestellt. Die gematik GmbH ist für den Aufbau, Betrieb und die Weiterentwicklung der TI verantwortlich. Gesellschafter sind das Bundesministerium für Gesundheit (BMG) sowie die Spitzenverbände des deutschen Gesundheitswesens, darunter die KBV, die Bundesärztekammer, der GKV-Spitzenverband, die Deutsche Krankenhausgesellschaft und der Deutsche Apothekerverband.

„Bei Gesundheitsdaten handelt es sich häufig um sensible personenbezogene Daten“, wird im EFI-Gutachten erläutert. Deshalb bestehe im Gesundheitswesen mehr als in anderen Bereichen ein Spannungsverhältnis zwischen IT-Sicherheit und Datenschutz auf der einen und den Potenzialen der Datennutzung auf der anderen Seite. Gemäß Artikel 9 der Europäischen Datenschutz-Grundverordnung (DSGVO) ist bei der Erhebung, Weitergabe und Nutzung personenbezogener Gesundheitsdaten besondere Sorgfalt geboten. „Hierin wird oft ein nicht unerhebliches Hemmnis für die Digitalisierung im Gesundheitswesen gesehen“, so das EFI-Gutachten.

Die DGSVO erlaube allerdings Regelungsspielräume auf nationaler Ebene, argumentieren die Autoren. „So zeigt ein Blick auf andere europäische Länder wie Estland und Dänemark, dass die DSGVO allein keinen Hinderungsgrund für die Datenverwendung im Gesundheitswesen darstellt.“ Dort würden DSGVO-konforme Opt-out-Regelungen die Weitergabe und Nutzung von Daten aus elektronischen Patientenakten für Forschungszwecke erlauben. „In Deutschland fehlen vergleichbare Regelungen bislang“, wird bemängelt.

Für die Einrichtung der ePA und die Zuteilung von Datenbearbeitungsrechten ist derzeit im Patientendaten-Schutzgesetz ein mehrstufiges Zustimmungsverfahren (Opt-in-Verfahren) durch die Versicherten vorgesehen. Im Ampel-Koalitionsvertrag ist die Einführung eines Opt-out-Verfahrens geplant: „Alle Versicherten bekommen DSGVO-konform eine ePA zur Verfügung gestellt; ihre Nutzung ist freiwillig (opt-out)“. Dies bedeutet, dass Patientinnen und Patienten der Nutzung der ePA aktiv widersprechen müssten. Im EFI-Gutachten wird dies als „zielführende Anpassung“ gesehen; das Opt-in-Verfahren sei „umständlich“ und trüge mit der fehlenden Bekanntheit der ePA dazu bei, dass sich nur wenige Versicherte für die Einrichtung der ePA entscheiden würden und diese dadurch nicht flächendeckend in die Anwendung gelange.

### *Ärztetag spricht sich für Opt-Out-Verfahren aus*

Auch der 126. Deutsche Ärztetag hat sich nachdrücklich für ein sogenanntes Opt-Out-Verfahren bei der elektronischen Patientenakte (ePA) ausgesprochen. Ziel müsse es sein, den Verbreitungsgrad der Akte zu erhöhen. Die ePA müsse die Sicherheit der Patientendaten gewährleisten und einen sicheren und einfachen Zugriff auf die in der ePA abgelegten Daten sicherstellen. Die Abgeordneten sprachen sich dafür aus, dass statt der bisher vorgesehenen expliziten Datenfreigabe für jeden Arzt alle an der Behandlung beteiligten Ärztinnen und Ärzte zunächst vollen Zugriff auf die Daten in der ePA erhalten sollten – es sei denn, der Patient schränkt die Zugriffsrechte explizit ein.

„Durch den unmittelbaren und ortsunabhängigen Zugang zu strukturierten Informationen kann eine ePA eine bedarfsgerechtere und besser koordinierte Versorgung ermöglichen“, heißt es in dem EFI-Gutachten. Um jedoch die mit den ePA-Daten verbundenen Potenziale heben zu können, sollte nach Ansicht der Autoren für Versicherte auch die Möglichkeit der Freigabe der Daten – insbesondere für Forschungszwecke, aber auch für den Datenaustausch zwischen Versorgung und Forschung – möglichst niedrigschwellig ausgestaltet werden. Die Autoren des Gutachtens sehen zudem die „Vielzahl an Landesdatenschutzgesetzen, die von den Landesdatenschutzbeauftragten im Hinblick auf die Weitergabe und Nutzung von Gesundheitsdaten für Forschungszwecke unterschiedlich ausgelegt werden“ als Hemmnis für die Digitalisierung. Dies trüge zu Rechtsunsicherheit bei und verzögere die Durchführung von datenabhängigen Forschungsprojekten. Auch die Delegierten des Deutschen Ärztetags stehen einer Nutzung medizinischer Daten für Forschungszwecke grundsätzlich positiv gegenüber – vorausgesetzt, diese zielt auf eine Verbesserung der Versorgung ab. Eine Datenfrei- und -weitergabe dürfe allerdings nur freiwillig erfolgen.

### *Alles- oder Nichts-Prinzip*

Der Bundesdatenschutzbeauftragte Kelber beanstandete unterdessen in seinem 30. Tätigkeitsbericht für das Jahr 2021, dass das Zugriffsmanagement auf die ePA „mit europarechtlichen Vorgaben nicht vereinbar“ sei. Die nationalen gesetzlichen Vorgaben sähen vor, dass Zugriffe nur nach dem „Alles- oder Nichts-Prinzip“ möglich seien. Versicherte, die kein eigenes geeignetes Endgerät besitzen oder keines nutzen wollen, könnten lediglich beim Leistungserbringer, z. B. in der ärztlichen Praxis, auf Kategorien von Dokumenten beschränkte Zugriffsrechte erteilen oder einem Dritten mit einem geeigneten technischen Gerät Vertretungsrechte einräumen, müssten dabei aber dieser Person gegenüber alle Daten offenlegen. „Außerdem werden diejenigen, die weder ein geeignetes Endgerät nutzen können oder wollen, noch die Vertreterlösung für sich in Anspruch nehmen möchten, auf Dauer auch keinen Einblick in ihre eigene, von ihnen selbst zu führende ePA haben.“ Die gesetzlichen Vorgaben würden die Souveränität der Versicherten „empfindlich“ beschneiden und einen Verstoß gegen die für die Verarbeitung personenbezogener Daten geltenden Grundsätze darstellen.

Vor dem Hintergrund der bestehenden Hemmnisse bei der Weitergabe und Nutzung von Gesundheitsdaten befürwortet die Expertenkommission ausdrücklich das im Koalitionsvertrag angekündigte Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung von Gesundheitsdaten. „Mit einem Gesundheitsdatennutzungsgesetz müssen die rechtlichen, organisatorischen und infrastrukturellen Rahmenbedingungen eindeutig festgelegt sein“, forderte auch der Deutsche Ärztetag. Aus Sicht der Abgeordneten müsse das Gesetz zudem das Risiko einer Re-Identifizierung bei aktuell anonymisierten Daten sowie einer unrechtmäßigen Re-Identifizierung bei pseudonymisierten Daten weitestgehend minimieren. Darüber hinaus bedürfe es einer Strategie zur Interoperabilität aller relevanten Gesundheitsdaten, um die Qualität und Vergleichbarkeit der Daten sicherzustellen.

Künstliche Intelligenz: Fragen und Entscheidungen

# Nur Ärzte können das „gesamtbiografische Krankheitsbild“ verorten

***Aufgrund der vielseitigen Einsatzmöglichkeiten und der sich stetig erweiternden technologischen Entwicklungen würden KI-Systeme in der Medizin „ein sehr bedeutsames und zugleich außerordentlich dynamisches Gebiet mit dem Potential einer weiteren Verbesserung der Gesundheitsversorgung“ darstellen. Politik und Institutionen auf nationaler und europäischer Ebene befassen sich derzeit mit der Nutzung der Künstlichen Intelligenz (KI) und dafür erforderlicher rechtlichen Ausgestaltungen.***

Im Fokus der Stellungnahme der Zentralen Ethikkommission stehen KI-basierte Datenverarbeitungssysteme, die Ärztinnen und Ärzte bei ihrer Entscheidungsfindung unterstützen sollen – sog. „Clinical Decision Support Systems“ (CDSS), von denen sich viele noch in der Erprobungsphase, andere aber bereits im klinischen Einsatz befinden würden. Die ZEKO begrüßt in ihrer Stellungnahme den Einsatz von CDSS – vorausgesetzt, diese würden dazu beitragen, die Qualität und Effektivität der Patientenversorgung zu verbessern. „Bereits jetzt können CDSS durch den Einsatz moderner Methoden der Datenverarbeitung bei bestimmten Teilaufgaben Ergebnisse erzielen, die mit denen von Ärztinnen und Ärzten vergleichbar sind oder diese sogar übertreffen.“ Der Einsatz von KI in der Medizin wecke aber auch Ängste.

Mögliche und teilweise auch schon realisierte klinische Anwendungsbeispiele/-felder für CDSS gebe es in diagnostischen, therapeutischen, prognostischen und prädiktiven Zusammenhängen, wird in dem Papier erklärt. „CDSS in der Diagnostik sind etwa für die radiologische Bildgebung entwickelt worden, wo auffällige Bereiche (z. B. suspekte Areale in Mammographien) in Bildern detektiert und markiert werden.“ Auch für die klinische Diagnostik in der Dermatologie befänden sich bereits CDSS für die Beurteilung der Malignität von Hautläsionen in der Anwendung. Hinsichtlich des Einsatzes von CDSS im therapeutischen Bereich ständen z. B. Anwendungen zur Verfügung, die die präoperative Therapieplanung sowie das intraoperative Vorgehen unterstützten.

### *Verantwortung kann nicht abgegeben werden*

Ein in ethischer Hinsicht „besonders umstrittenes Feld“ bietet der Stellungnahme zufolge der Einsatz von CDSS, die Aussagen zur klinischen Prognose von Patientinnen und Patienten treffen. Umstritten sei hier insbesondere, auf welchen Daten eine Prognose – insbesondere auch angesichts der zum Teil erheblichen Streuung individueller klinischer Verläufe – erfolge und welche Rolle hier etwa auch gesundheitsökonomische Parameter spielen könnten. Noch einen Schritt weiter als die Prognose gehe der Einsatz von CDSS bei der Prädiktion von Krankheiten, die bei gesunden Menschen ansetze und Dispositionen und Empfänglichkeiten (Suszeptibilitäten) für bestimmte Erkrankungen aufdecken wolle. „Die Prädiktion geschieht auf der Basis oft schwer interpretierbarer statistischer Wahrscheinlichkeiten, die weniger auf Methoden der deduktiven Kausalitätsermittlung als auf induktiven Kausalitätsannahmen aus Korrelationsanalysen beruhen und damit zu Fehlschlüssen führen können“, bemängelt der ZEKO.

„Beim Einsatz von KI liegt die Verantwortung und Rechenschaftspflicht für Diagnose, Indikationsstellung und Therapie nach wie vor beim Arzt beziehungsweise bei der Ärztin. Diese Verantwortung kann nicht an ein CDSS abgetreten werden“, hebt der Vorsitzende der ZEKO, Prof. Dr. jur. Jochen Taupitz, hervor. Optimale Behandlungsergebnisse würden insbesondere erzielt, wenn CDSS und ärztliches Erfahrungswissen zusammenwirkten. „Nur Ärztinnen und Ärzte vermögen das Krankheitsbild gesamtbiographisch zu verorten und auch psychische sowie emotionale Faktoren zu berücksichtigen, die sowohl für die Diagnose Gewicht haben als auch für eine angemessene Therapie ausschlaggebend sein können“, wird in der Stellungnahme betont.

*An erster Stelle bei der Regulierung müssen die Gesundheit der Menschen und der Schutz ihrer elementaren Grundrechte stehen.*

Grafik: Have a nice ... Photo/shutterstock.com

In einer Stellungnahme zur „Entscheidungsunterstützung ärztlicher Tätigkeit durch Künstliche Intelligenz“ der Zentralen Ethikkommission (ZEKO) bei der Bundesärztekammer (BÄK) wird nicht nur der aktuelle Entwicklungsstand Künstlicher Intelligenz (KI) skizziert sondern auch die mit dem Einsatz von KI für die ärztliche Tätigkeit verbundenen Fragen aus medizinischer, ethischer und rechtlicher Perspektive beleuchtet. Vor einem Jahr (April 2021) wurde zudem von der EU-Kommission ein Vorschlag für einen ersten Rechtsrahmen vorgelegt, „um sicherzustellen, dass KI-Systeme, die in der EU verwendet werden, sicher, transparent, ethisch, unparteiisch und unter menschlicher Kontrolle sind“. Am 16. März 2022 befasste sich der Digitalausschuss des Deutschen Bundestages mit dem „Bericht der Bundesregierung zum Verhandlungsstand zur EU-Verordnung für künstliche Intelligenz (KI)“.

### *Rechtlicher Rahmen muss geschaffen werden*

Der Vorschlag für eine „Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zu Änderung bestimmter Rechtsakten der Union“ der EU-Kommission soll darauf abzielen, „einen Rechtsrahmen für eine vertrauenswürdige KI zu schaffen, damit das zweite Ziel für den Aufbau eines Ökosystems für Vertrauen umgesetzt werden kann“. „KI sollte ein Instrument sein, das als positive Kraft für die Gesellschaft im Dienst der Menschen steht und das letztlich zu einem größeren Wohlbefinden der Menschen beiträgt“, heißt es in dem Verordnungsvorschlag. KI-Systeme sollen nach vier Risikostufen eingeteilt werden:

1. **Unzulässiges Risiko:** Alles, was als eindeutige Bedrohung für EU-Bürger angesehen wird, wird verboten: von der behördlichen Bewertung des sozialen Verhaltens (Social Scoring) bis hin zu Spielzeug mit Sprachassistent, das Kinder zu riskantem Verhalten verleitet.
2. **Hohes Risiko:** u.a. Kritische Infrastrukturen (z. B. im Verkehr), Sicherheitskomponenten von Produkten (z. B. eine KI-Anwendung für die roboterassistierte Chirurgie). Alle Systeme werden sorgfältig geprüft, bevor sie in Verkehr gebracht werden — und auch während ihres gesamten Lebenszyklus.
3. **Begrenztes Risiko:** Für KI-Systeme wie „Chatbots“ gelten minimale Transparenzverpflichtungen
4. **Minimales Risiko:** Kostenlose Nutzung von Anwendungen wie KI-gestützten Videospielen oder Spamfiltern.

Die Beauftragte der Bundesregierung für die Digitale Wirtschaft und Start-ups, Anna Christmann (Bündnis 90/Die Grünen), sagte im Ausschuss, die Stellungnahme der Bundesregierung solle zeitnah nach Brüssel übersandt werden. Sie begrüße die Zielsetzung der Verordnung, insbesondere, dass gemeinsame europäische Werte festgelegt werden und, dass der KI-Standort Europa gestärkt werde und Rechtssicherheit geschaffen werde. Schlüssel zum Erfolg seien eine verlässliche Regulierung, Vertrauen aufzubauen und einen eigenen, erfolgreichen Weg im Umgang mit der Technologie zu entwickeln.

### *Ein Ökosystem für Vertrauen*

Der TÜV-Verband hatte in einer Stellungnahme im September 2021 konkrete Nachbesserungen am EU-Regulierungsentwurf für Künstliche Intelligenz gefordert. Aus Sicht des TÜV-Verbands ist der vorliegende Regelungsentwurf „nicht hinreichend ambitioniert und bleibt hinter dem eigenen Anspruch der EU-Kommission zurück, ein ‚Ökosystem für Vertrauen‘ zu schaffen“. Ein Ökosystem für Vertrauen könne nur durch ein Primat der Sicherheit von KI bei der Ausgestaltung des Regulierungsrahmens geschaffen werden. „Bei der Regulierung von Künstlicher Intelligenz müssen die Gesundheit der Menschen und der Schutz ihrer elementaren Grundrechte an erster Stelle stehen“, sagt Dr. Joachim Bühler, Geschäftsführer des TÜV-Verbands. „Bei der Zuordnung von KI-Systemen in die vier vorgesehenen Risikoklassen von minimal bis unannehmbar und den damit verbundenen Anforderungen an die Sicherheit und deren Überprüfung sind Verbesserungen notwendig.“

Die Kernforderungen des TÜV-Verbands zusammengefasst:

1. Risikoklassen nachvollziehbar herleiten und effektiven Rechtsgüterschutz priorisieren: Insbesondere fehle es an nachvollziehbaren Kriterien, von welchen KI-Systemen ein besonders hohes Risiko („high-risk“) ausgeht.
2. Unabhängige Drittprüfung bei high-risk KI-Systemen durchgehend vorsehen.
3. Risikoadäquate Klassifizierungsvorschriften für „high-risk“ Anwendungen einführen: Auch die bereits regulierten Produktbereiche sollen einer KI-risikospezifischen Neubewertung unterzogen werden.
4. Risiken für schützenswerte Rechtsgüter müssen alleiniger Maßstab zur Ergänzung der Liste der high-risk KI-Systeme sein: Sofern Leib und Leben oder zum Beispiel die Privatsphäre der Menschen gefährdet sind, muss das KI-System als high-risk klassifiziert werden.
5. Einspruchsmöglichkeiten gegen Entscheidungen notifizierter Stellen konkretisieren und europaweit einheitlich regeln.

POLITIK

## Kontrollierte Cannabis-Freigabe in Vorbereitung

# „Wir wollen den Dealer arbeitslos machen“

***Der Koalitionsvertrag bis 2025 sieht vor, eine kontrollierte Abgabe von Cannabis an Erwachsene in lizenzierten Geschäften einzuführen. Bundesgesundheitsminister Professor Dr. Karl Lauterbach MdB (SPD) kündigte am 4. Mai 2022 an, die Cannabis-Legalisierung neben weiteren gesundheitspolitischen Reformen über den Sommer „mit Kraft“ auf den Weg bringen zu wollen. Der Bundesdrogenbeauftragte Burkhard Blienert (SPD) teilte kurze Zeit später mit, gemeinsam mit dem Bundesgesundheitsministerium und weiteren Ressorts „einen gründlichen Konsultationsprozess“ zu starten.***

Zudem übte der Bundeshaushaltsausschuss mit einer vorläufigen Sperre von einer Million Euro des Etats für die Öffentlichkeitsarbeit des Gesundheitsministeriums Druck aus, noch dieses Jahr die Cannabis-Legalisierung auf den Weg zu bringen. Ein Gesetzentwurf soll, so der Bundesgesundheitsminister, in der zweiten Jahreshälfte folgen.

Der Umgang mit Cannabis ist in Deutschland im Betäubungsmittelgesetz (BtMG) festgelegt. In diesem ist Cannabis in Anlage I als „nicht verkehrsfähig“ eingestuft. Somit ist jeglicher Besitz von Cannabis und Cannabisprodukten (Haschisch, Marihuana) illegal und somit strafbar. Laut § 29 ff. des BtMG wird mit einer Freiheitsstrafe von bis zu fünf Jahren oder mit einer Geldstrafe bestraft, wer: „Betäubungsmittel unerlaubt anbaut, herstellt, mit ihnen Handel treibt, sie, ohne Handel zu treiben, einführt, ausführt, veräußert, abgibt, sonst in den Verkehr bringt, erwirbt oder sich in sonstiger Weise verschafft.“ Der Konsum einer illegalen Droge ist in Deutschland hingegen nicht strafbar. „Da dem Konsum aber in der Regel der Besitz vorausgeht, machen sich Menschen, die kiffen, meist doch strafbar“, so die Bundeszentrale für gesundheitliche Aufklärung (BZgA).

„Der Koalitionsvertrag 2021 bis 2025 zwischen SPD, Bündnis 90/Die Grünen und FDP sieht vor, eine kontrollierte Abgabe von Cannabis an Erwachsene zu Genusszwecken in lizenzierten Geschäften einzuführen“, heißt in einer Antwort der Bundesregierung auf eine Kleine Anfrage der CDU/CSU-Fraktion im Februar 2022 (Bundestagsdrucksache Nr. 20/653). „Dadurch soll die Qualität kontrolliert, die Weitergabe verunreinigter Substanzen verhindert und der Jugendschutz gewährleistet werden.“ Eine Evaluierung des Gesetzes auf gesellschaftliche Auswirkungen solle nach vier Jahren erfolgen. Vorrangiges Ziel und Leitgedanke des Gesetzgebungsvorhabens werde daher sein, für einen bestmöglichen Gesundheitsschutz der Konsumentinnen und Konsumenten zu sorgen sowie den Kinder- und Jugendschutz sicherzustellen. Zum aktuellen Zeitpunkt könne noch keine Aussage zur konkreten Ausgestaltung des Gesetzentwurfes getroffen werden. Die Klärung spezifischer Fragen werde im Rahmen der Erstellung des Gesetzesentwurfes der Bundesregierung erfolgen. „Ich war immer ein Gegner der Cannabis-Legalisierung, habe aber meine Position vor rund einem Jahr revidiert“, erklärte Lauterbach. Seiner Meinung nach seien die Gefahren einer Nicht-Legalisierung größer.

„Wir wollen hier ein Gesamtkonzept verfolgen“, erklärte Bundesjustizminister Dr. Marco Buschmann MdB (FDP) am 11. Mai 2022 im Deutschen Bundestag bei einer Befragung der Bundesregierung. „Wir wollen dafür sorgen, dass wir – ich darf es mal so flapsig sagen – den Dealer arbeitslos machen. Wir wollen dafür sorgen, dass sich die Konsumenten auf vernünftige Produktqualität verlassen können, und wir wollen dafür sorgen, dass Missbrauch dadurch vermieden wird, dass wir qualifizierte Verkaufsstellen haben.“ Er gab zur Umsetzung zu bedenken: „Wenn man einen solchen Gesetzentwurf vorlegt, braucht dieser ja schon ein paar Monate, um durch das Parlament zu kommen. Mein persönliches Ziel ist, dass wir im nächsten Jahr so weit sind, dass vielleicht der erste legale Joint verkauft werden kann.“

Fachliche Vorbereitungen sind laut dem Bundesdrogenbeauftragten im Mai gestartet. „Es geht darum, das Wissen und die Erfahrungen zu bündeln, aber auch Einwände und Vorbehalte sehr offen anzusprechen“, sagte er der Deutschen Presse-Agentur. In die weiteren Vorbereitungen sollten auch die Länder, Kommunen, Verbände, Wissenschaft und die Zivilgesellschaft eingebunden werden. „Kaum ein anderes drogenpolitisches Thema beschäftigt die Menschen seit Jahrzehnten so sehr wie Cannabis“, betonte Blienert. „Wir alle wissen, wie komplex dieses Vorhaben ist.“ Bis zum Herbst solle daher mit führenden Expertinnen und Experten über die relevantesten Fragen zum Gesundheitsschutz, zu Anbau, Lieferketten und zur Besteuerung diskutiert werden. „So unterstützen wir den Gesetzgebungsprozess fachlich und politisch durch ein gutes Fundament.“

Im Fokus der Beratungen sollten Blienert zufolge die Bereiche Jugend- und Gesundheitsschutz stehen. „Denn am Ende sollen in Deutschland natürlich nicht mehr, sondern weniger Jugendliche Cannabis konsumieren.“ Auch internationale Erfahrungen, etwa aus Kanada, sollten genau angeschaut werden. Dort war Cannabis 2018 mit dem politisch erklärten Ziel legalisiert worden, das zuvor illegale Geschäft zu kontrollieren und zu regulieren. „Mit dem Koalitionsvertrag haben wir uns auf einen Paradigmenwechsel in der Drogen- und Suchtpolitik verständigt: weniger Repression, mehr Schutz und Hilfe.“

Der Haushaltsausschuss im Deutschen Bundestag hat vom Etat für die Öffentlichkeitsarbeit vom Bundesgesundheitsministerium eine Million Euro mit einer Sperre belegt. Die Sperre soll bis zur Vorlage eines Gesetzentwurfs für ein Cannabiskontrollgesetz gelten, heißt es in der Beschlussempfehlung des Haushaltsausschusses vom 11. Mai 2022 (Bundestagsdrucksache 20/1614). Die Mittel seien „verbindlich zur Cannabisprävention zu verwenden“. Die Aufhebung der Sperre bedürfe der Einwilligung des Haushaltsausschusses des Deutschen Bundestages. Mit dem Sperrvermerk sei für das Bundesgesundheitsministerium ein finanzieller Anreiz geschaffen worden, den angekündigten Entwurf auch wirklich in diesem Jahr vorzulegen, so Karsten Klein MdB (FDP), Mitglied im Haushaltsausschuss und Berichterstatter seiner Fraktion für diese Thematik.

In einem gemeinsamen Positionspapier zur kontrollierten Abgaben von Cannabis vom 23. Februar 2022 fordern fünf deutsche Sucht-Fachgesellschaften den Gesetzgeber auf, geeignete Maßnahmen zu ergreifen, welche die gesundheitlichen und sozialen Folgeschäden mindern, die bei einer Ausweitung des Cannabiskonsums erwartbar wären. Falls sich nun, wie angekündigt, eine politische Verständigung erfolgen sollte, richten sie fünf zentrale Forderungen an die politischen Entscheidungsträger. Die Forderungen zusammengefasst:

- Priorisierung und Ausbau des Jugendschutzes, Prävention des problematischen Konsums durch strukturelle Maßnahmen, wie begrenzte Öffnungszeiten und Anzahl der Verkaufsstellen, Legale Abgabe von Cannabis oberhalb des 18. Lebensjahrs (Vorschlag: ab dem 21. Lebensjahr), Mengenbegrenzung beim Verkauf, Werbeverbot, Anbau und Betrieb durch staatliche Stellen.
- Mit der Einführung legaler Verkaufswege muss illegaler Handel konsequent unterbunden werden.
- Der Steuersatz muss eine Komponente des Wirkstoffgehaltes beinhalten, es darf nicht ausschließlich nach Gewicht (Gramm) besteuert werden. Parallel zu den steigenden Steuereinnahmen durch den Verkauf von Cannabis zu Rauschzwecken und in vergleichbarerer Größenordnung müssen dem Gesundheitsbereich zusätzliche Mittel zukommen zur verbesserten Prävention, Früherkennung, Frühintervention, Beratung, Begleitung und Behandlung sowie der Versorgungs- und Therapieforschung im Bereich cannabisbezogener Störungen.
- Umfassende Begleitforschung und Ausbau des Drogen- und Gesundheitsmonitorings in Deutschland, um gesundheitliche, soziale und rechtliche Entwicklungen präziser abzuschätzen.
- Etablierung einer interdisziplinären Gruppe von Expertinnen und Experten, die die Regierung bei der Umsetzung der neuen Regulierungen zur kontrollierten Cannabisabgabe berät.

Unterzeichner des Positionspapiers sind die Deutsche Gesellschaft für Suchtforschung und Suchttherapie (DG-Sucht), die Deutsche Gesellschaft für Suchtmedizin (DGS), die Deutsche Gesellschaft für Suchtpsychologie (dgsps) und die Deutsche Hauptstelle für Suchtfragen (DHS).

Foto: DvorakPhoto/shutterstock.com

*Bis zum Herbst soll mit führenden Expertinnen und Experten über die relevantesten Fragen zum Gesundheitsschutz, zu Anbau, Lieferketten und zur Besteuerung diskutiert werden.*

Aufhebung des Werbeverbots für den Schwangerschaftsabbruch

# Ärztetag fordert „notwendige Transparenz“

***Die Bundesregierung plant die Aufhebung des Verbots der Werbung für den Schwangerschaftsabbruch. In einer Öffentlichen Anhörung im Rechtsausschuss am 18. Mai 2022 ist das Vorhaben von der Mehrheit der Sachverständigen unterstützt worden. Dabei ging es vor allem um das geplante Gesetz der Bundesregierung „zur Änderung des Strafgesetzbuches – Aufhebung des Verbots der Werbung für den Schwangerschaftsabbruch (Paragraf 219a StGB), zur Änderung des Heilmittelwerbegesetzes und zur Änderung des Einführungsgesetzes zum Strafgesetzbuch“ (Bundestagsdrucksache 20/1635).***

Auch der 126. Deutsche Ärztetag in Bremen hat die von der Bundesregierung angestrebte Streichung des § 219a StGB begrüßt. „Dieser regelt bislang das Verbot, für Schwangerschaftsabbrüche zu werben. Durch diese Regelung konnte schon die sachliche Ankündigung, in einer ärztlichen Institution Schwangerschaftsabbrüche durchzuführen, zu Strafverfolgung führen“, erklärt die Bundesärztekammer (BÄK).

Neben der Streichung von Paragraf 219a im Strafgesetzbuch (StGB) sollen laut Gesetzentwurf Urteile, die aufgrund dieser Norm erlassen worden sind, aufgehoben werden. Zudem sollen Regelungen im Heilmittelwerbegesetz so angepasst werden, dass sowohl medizinisch indizierte als auch medizinisch nicht indizierte Schwangerschaftsabbrüche erfasst werden. Zur Begründung führt die Bundesregierung an, dass Ärztinnen und Ärzte nach der aktuellen Rechtslage mit strafrechtlicher Verfolgung rechnen müssten, „wenn sie sachliche Informationen über Ablauf und Methoden des Schwangerschaftsabbruchs öffentlich (etwa auf ihrer Homepage) bereitstellen oder in einer Versammlung oder durch Verbreiten eines Inhalts Paragraf 11 Absatz 3 StGB) darüber berichten“. Auch eine Reform der Norm im Jahr 2019 habe daran nichts geändert, wie die Bundesregierung mit Verweis auf die Verurteilung der Frauenärztin Kristina Hänel schreibt. Durch die Einschränkungen für Ärztinnen und Ärzte werde betroffenen Frauen „zum einen der ungehinderte Zugang zu sachgerechten fachlichen Informationen über den sie betreffenden medizinischen Eingriff und zum anderen das Auffinden einer geeigneten Ärztin oder eines geeigneten Arztes erschwert“.

Vor dem Hintergrund der verfassungsgerichtlichen Rechtsprechung zum Schwangerschaftsabbruch betont die Bundesregierung in der Begründung, dass die geplante Streichung des Paragrafen 219a StGB mit „der grundgesetzlichen Schutzpflicht für das ungeborene Leben vereinbar“ sei. Der Paragraf sei „kein tragender Bestandteil des danach gebotenen Schutzkonzepts, dem der Gesetzgeber bei der Ausgestaltung des Rechts des Schwangerschaftsabbruchs Rechnung zu tragen hat“. Die Aufhebung stehe zudem im Einklang mit dem sogenannten Beratungskonzept.

### *Versorgung muss sichergestellt werden*

„219a gehört abgeschafft. Das funktioniert nicht“, bekräftigte Bundesgesundheitsminister Professor Dr. Karl Lauterbach MdB (SPD) am 25. Mai in der Talkshow „Markus Lanz“. Ärztinnen und Ärzte, die Schwangerschaftsabbrüche durchführten, würden dadurch zu Unrecht stigmatisiert. Als Arzt oder Ärztin dürfe man zwar sagen, dass man den Eingriff macht, aber darf nicht beschreiben, wie er vorgenommen wird. Auch die Liste, die von der Bundesärztekammer (BÄK) zur Verfügung gestellt wird und Ärztinnen und Ärzten aufzeigt, die diese Eingriffe durchführen, wirke wie ein „Pranger“, konstatierte der Bundesgesundheitsminister. „Die Ärzte, die da gelistet sind, sind dann sehr häufig auch Gegenstand von Angriffen, somit will man da nicht stehen.“ Das führe in die falsche Richtung. Ärztinnen und Ärzte, die Schwangerschaftsabbrüche anbieten, würden immer weniger werden. „Das können wir nicht zulassen“, weil hier Versorgungssicherheit dargestellt werden müsse.

Die Union lehnt die von der Bundesregierung geplante Streichung des Werbeverbots für Schwangerschaftsabbrüche ab. Stattdessen solle der Paragraf 219a so modifiziert werden, dass Ärztinnen und Ärzte, Krankenhäuser und Einrichtungen „auf ihrer Internetseite wertungsfreie Angaben zu den von ihnen angewendeten Methoden zur Durchführung eines Schwangerschaftsabbruches machen können“, heißt es in einem Antrag der Fraktion mit dem Titel „Interessen der Frauen stärken, Schutz des ungeborenen Kindes beibehalten“ (Bundestagsdrucksache 20/1017). Weitere Forderungen beziehen sich unter anderem auf die Kostenübernahme für ärztlich verordnete Verhütungsmittel, die auch im Ampel-Koalitionsvertrag angesprochen wird. Aus Sicht der Union ist die grundsätzliche Beibehaltung des Paragrafen „zum Schutz des ungeborenen Lebens geboten“.

### *Anstatt „Beratungspflicht“ ein „Recht auf Beratung“*

Die Fraktion Die Linke unterstützt die von der Bundesregierung geplante Aufhebung des Werbeverbotes für Schwangerschaftsabbrüche. Darüber hinaus fordert die Fraktion in einem Antrag „§ 219a StGB aufheben – Selbstbestimmung, Entscheidungsfreiheit und ausreichende Versorgung sicherstellen“ (Bundestagsdrucksache 20/1736), „die vollständige Entkriminalisierung von Schwangerschaftsabbrüchen auf Wunsch der schwangeren Person durch Streichung des Paragrafen 218 StGB“. Im Paragrafen 218 StGB heißt es: „Wer eine Schwangerschaft abbricht, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“ Die bisherige Beratungspflicht solle ferner durch ein Recht auf Beratung ersetzt werden, der „Beratungszwang“ nach Paragraf 218a Absatz 4 und Paragraf 219 StGB soll abgeschafft werden. „Reproduktive Gerechtigkeit“ will die Fraktion zum Regierungsziel erklärt wissen.

Zu einer möglichen Abschaffung von Paragraf 218 erklärte Lauterbach: „Das ist eine breite Debatte.“ Es werde irgendwann „auch zu diesen Fragen wieder neue Lösungen geben“. Er müsse sich in seiner Position jedoch auf die Dinge konzentrieren, die jetzt anstünden. Im Ampel-Koalitionsvertrag wird auch von einem Vorhaben zur Regulierung „außerhalb des Strafgesetzbuches“ gesprochen: „Wir setzen eine Kommission zur reproduktiven Selbstbestimmung und Fortpflanzungsmedizin ein, die Regulierungen für den Schwangerschaftsabbruch außerhalb des Strafgesetzbuches sowie Möglichkeiten zur Legalisierung der Eizellspende und der altruistischen Leihmutterschaft prüfen wird.“

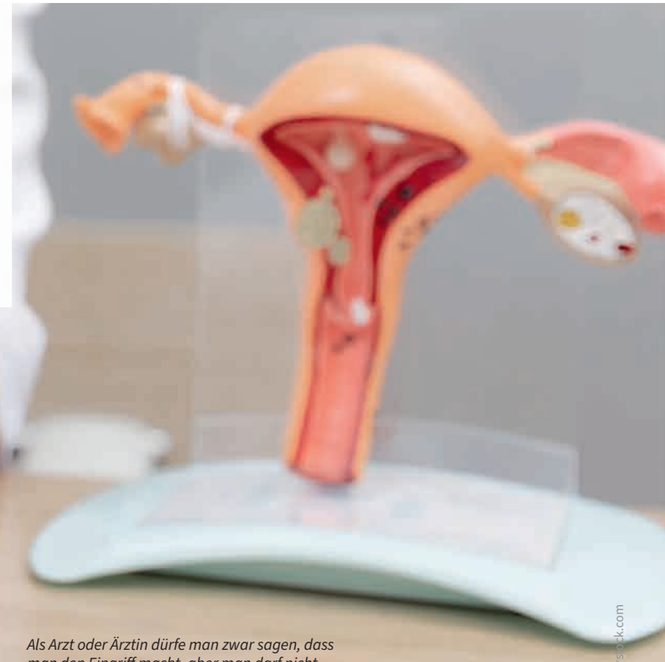
Der Ärztetag teilt die Auffassung von Bundesjustizminister Marco Buschmann (FDP), nach der dieser Rechtszustand für Ärztinnen und Ärzte unhaltbar sei. Zudem habe der Paragraf 219a StGB in der Vergangenheit dazu beigetragen, dass betroffenen Frauen der Zugang zum Schwangerschaftsabbruch trotz bescheinigter Indikation nach Paragraf 218 StGB erschwert wurde. „Die Möglichkeit, über angewandte Methoden des Schwangerschaftsabbruchs sachlich zu informieren, wird nach Streichung dieses Paragrafen auch in diesem sensiblen Kontext die nötige Transparenz herstellen, die bei anderen medizinischen Interventionen selbstverständlich und für die informierte Zustimmung der Patientinnen zu einem solchen Eingriff Voraussetzung ist“, betonte der Ärztetag.

### *Verfassungsbeschwerde eingereicht*

Die Gießener Ärztin Kristina Hänel, die selber im Jahr 2017 wegen Werbung für den Schwangerschaftsabbruch verurteilt wurde, argumentierte in einer öffentlichen Anhörung des Rechtsausschusses zu dieser Thematik, es gebe keinen guten Grund, Frauen, die von ungewollter Schwangerschaft betroffen sind, Informationen vorzuenthalten. Sie berichtete in ihrer Stellungnahme, dass sie Kontakt zu ca. 100 Medizinern und Krankenhäusern habe, die auch von einer Anzeige nach §219a StGB betroffen gewesen seien. Vielen sei nicht bewusst gewesen, dass sie sich strafbar machten. „Die Anzeigen wurden in der Regel eingestellt, die Informationen wurden aus dem Netz genommen.“ Der abzuschaffende Paragraf 219a des Strafgesetzbuches sei eine der Ursachen für die immer schlechter werdende Versorgungslage beim Schwangerschaftsabbruch, erklärte die Ärztin. „Zusätzlich zur Rechtsunsicherheit wirken noch die ungehemmten Angriffe der Anti-Choice Bewegung negativ auf die Bereitschaft der Ärzteschaft, Schwangerschaftsabbrüche durchzuführen.“ Gegen ihre Verurteilung und gegen den Paragrafen 219a hat Hänel Verfassungsbeschwerde eingereicht.

Auch die Bundesvorsitzende des Bundesverbands pro familia, Monika Börding, erläuterte, durch die Streichung des Paragrafen 219a, könnten sich ungewollt Schwangere künftig niedrigschwellig im Netz darüber informieren, wo es in ihrer Nähe eine Praxis oder eine Klinik gibt, die Schwangerschaftsabbrüche durchführt. Ärztinnen und Ärzte sowie Kliniken könnte nach der Streichung nicht mehr von Gegnerinnen und Gegnern der sexuellen und reproduktiven Selbstbestimmung wegen der Bereitstellung solcher Informationen angezeigt werden. Die Streichung sei ein guter erster Schritt, reiche jedoch nicht aus.

Die Frauenärztin Prof. Dr. Angela Köninger, Klinikdirektorin und Inhaberin des Lehrstuhls für Frauenheilkunde und Geburtshilfe der Universität Regensburg, sprach sich in ihrer schriftlichen Stellungnahme zur Öffentlichen Anhörung des Rechtsausschusses hingegen für eine sachliche und auf dem Boden der realen Tatsachen geführte Diskussion, fern von „theoretischen Angstkulissen“, aus. Aus ihrer Sicht seien die in der aktuellen Debatte um den Gesetzentwurf postulierten Missstände in der Information und Versorgung von Frauen im Schwangerschaftskonflikt in der Realität nicht präsent. Zudem stelle 219a nicht den Grund dar, warum Ärztinnen und Ärzte keine Abbrüche anbieten. Grund hierfür sei in fast allen Fällen deren Berufung auf ihr eigenes Selbstbestimmungsrecht.



*Als Arzt oder Ärztin dürfe man zwar sagen, dass man den Eingriff macht, aber man darf nicht beschreiben, wie er vorgenommen wird.*

Foto: Parilov/shutterstock.com

Ausschusssitzung der Assistenzärztinnen und -ärzte

## Ein Blick über den Tellerrand

Bei der Ausschusssitzung der Assistenzärzte in diesem Frühjahr war Patrick Klein, der stellvertretende Vorsitzende der Deutschen Gesellschaft für Physician Assistants, zu Gast. Er berichtete eindrucksvoll vom Werdegang, den Tätigkeitsfeldern und dem Arbeitsalltag seiner Berufsgruppe und ging auch auf Haftungsfragen und interprofessionelle Zusammenarbeit ein. In der anschließenden Diskussion wurde festgestellt, dass von ärztlicher Seite – dort, wo ein Physician Assistant (PA) bereits etabliert ist – die PAs als große Entlastung empfunden werden. Eine dementsprechende Resolution für den Deutschen Ärztetag (DÄT) wurde deshalb ausgearbeitet und mit dem Verband der PAs im Nachgang besprochen.

Im Sitzungsverlauf wurde außerdem das ärztliche Arbeiten in Dänemark, Großbritannien und den Niederlanden beleuchtet. Referentinnen bzw. Referenten aus allen drei Ländern präsentierten die Besonderheiten ihres Gesundheitssystems im Vergleich zu Deutschland. Die Ausschussmitglieder waren sich hinterher einig, dass vor allem Dänemark mit seiner unbürokratischen Struktur und dem geringen ökonomischen Druck überzeugend ist und die Qualität des Arztberufes steigert. Aus diesem Fazit leiteten sie ihre weiteren Forderungen für den DÄT ab. Um die Forderungen in Bremen zu unterstützen, arbeiteten sie das Projekt „Ärztinnen und Ärzte in Fes-


seln“ aus. Ein Projekt, dass die stark verringerte Arzt-Patientenzeit durch Bürokratie und wirtschaftliche Zwänge thematisiert.

Im Zuge der turnusmäßigen Wahl des Leitungsgremiums wurden Caroline Rinkel, Christian Kunze, Jan Baumann, Jon Wahnschaffe und Lisa Rosch gewählt.

Ausschusssitzung der Medizinstudierenden

## Qualität des PJ darf nicht unter die Räder kommen

Die Ausschusssitzung der Studierenden im April stand im Fokus der Zukunft – sowohl der studentischen als auch der ärztlichen. Zunächst ging es um das zukünftige ärztliche Arbeiten und die e-Health-Entwicklung. Als Referentin war Frau Dr. Geier vom Spitzenverband Digitale Gesundheitsversorgung eingeladen. Sie berichtete über mögliche Szenarien der Arzt-Patientenbeziehung, benötigte rechtliche Vorgaben durch die Bundesregierung und stieß eine Diskussion über Einsparungspotentiale und die Rolle ausländische Akteure in der Gesundheitsversorgung an. Ergänzend dazu stellte Frederic Kube die Vor- und Nachteile digitaler Gesundheitsanwendungen (DiGa), gesetzliche Regelungen sowie u.a. Zahlen und Fakten zum DiGa-Verzeichnis vor. Die Studierenden haben daraufhin nochmal ihre Forderung nach der Berücksichtigung von digitalen Inhalten im Curriculum hervorgehoben – eine Forderung, die eng mit der Einführung der neuen Approbationsordnung verknüpft ist.

Außerdem hat der Ausschuss weitere langwierige Themen wieder aufgegriffen, die nach wie vor der Bearbeitung bedürfen. Eine Herzensangelegenheit der Studierenden ist immer noch die Verbesserung der PJ-Bedingungen. Zurzeit sind PJler die „Wolpertinger“ der Kliniken: Sie sind halb Studierende, halb Ärztinnen und Ärzte und oft leider auch halb Pflegekraft. Damit sich das Praktische Jahr nicht zu einem zweiten Pflegepraktikum entwickelt, haben die Ausschussmitglieder nicht nur eine Resolution zur Umsetzung der neuen Approbationsordnung, sondern auch eine Resolution zur Sicherung der PJ-Qualität ausgearbeitet. Zusätzlich haben sie beschlossen, die Relevanz der Resolution auf dem Deutschen Ärztetag gemeinsamen mit dem Ausschuss der Assistenzärzte durch eine Inszenierung der Missstände in den Kliniken zu unterstreichen.



Da Johannes Stalter durch die Beendigung seines Studiums nun aus dem Vorstand ausscheidet, wurde im Sitzungsverlauf auch noch Moritz Roloff als Schriftführer nachgewählt.





Vierter Hartmannbund-Ärztinnentag „Karriere im Krankenhaus“

## So gelingt der persönliche Karriereweg im Krankenhaus

*Karriere- und Lebensziele gleichermaßen verwirklichen – darauf arbeiten junge Ärztinnen genauso hin wie junge Ärzte. Wenn es darum geht, Führungsverantwortung im Krankenhaus zu übernehmen, scheiden sich allerdings noch immer die Wege: “Es ist nötig, das Thema Karriere im Krankenhaus aus weiblicher Sicht zu betrachten, da wir besonders hier noch nicht von echter Chancengleichheit sprechen können”, so Dr. Dr. Galina Fischer, Sprecherin des Ausschusses Ärztinnen, Mitglied im Geschäftsführenden Vorstand und Mit-Initiatorin des Hartmannbund-Ärztinnentags. “Wir möchten allen Kolleginnen Mut machen, die eigenen Ziele trotz Hindernissen und Widerständen zu verfolgen. Deshalb haben wir zum vierten HB-Ärztinnentag erfolgreiche und inspirierende Kolleginnen eingeladen, von ihren Erfahrungen zu berichten.”*

*PD Dr. med. Doreen Richardt, PD Dr. med. Malgorzata Lanowska, PD Dr. med. Mandy Mangler und HB-Vorstandsmitglied Dr. Dr. Galina Fischer (v. l. n. r.) auf dem HB-Ärztinnentag.*

Wie gelingen Karriereschritte zur Oberärztin und Chefärztin? Wie verhandele ich die Arbeitsbedingungen, die zu meinem Leben passen?

Flexible Arbeitszeitmodelle sind die Zukunft – auch auf Führungsebene im Krankenhaus. Das beweisen Chefärztinnen PD. Dr. Mandy Mangler und PD Dr. Malgorzata Lanowska. Beide leiten eine Klinik für Gynäkologie beim Berliner Krankenhauskonzern Vivantes und gemeinsam teilen sie sich die Leitung der Klinik für Gynäkologie am Vivantes Klinikum Neukölln. In ihrem Beitrag „Chefärztinnen im Jobsharing so läuft´s“ berichteten sie eindrucksvoll, wie aus einem gemeinsamen Werdegang durch Studium, Weiterbildung, Habilitation und Zusatzqualifikation eine enge und vertrauensvolle Kooperation entstand.

Neue Führungsmodelle im Krankenhaus und Nachwuchsförderung von Ärztinnen liegen Beiden am Herzen. Und flexible Arbeitszeitmodelle anzubieten, ist für sie eine Selbstverständlichkeit – ebenso wie wirklich individuelle Gefährdungsbeurteilungen von Arbeitsplätzen schwangerer Ärztinnen und eine bedürfnisorientiere Weiterbeschäftigung.

Auch PD Dr. Doreen Richardt macht in Ihrem Vortrag „(M)ein Weg zur Oberärztin und der Umgang mit Konflikten im Krankenhaus“ Kolleginnen Mut, in der Schwangerschaft ihr Recht auf einen sicheren patientennahen Arbeitsplatz – auch im OP – einzufordern. Als Herzchirurgin und Mutter von sechs Kindern riet die Trägerin der Auszeichnung „Mutige Löwin“ Ärztinnen, zu Beginn der Karriere frühzeitig eigene Ziele zu definieren, sich in der Weiterbildung aktiv die Aufgaben zu holen, die man benötigt und zu bedenken, dass akademische Titel gerade bei männlichen Kollegen Türen öffnen können.

Vor dem Hintergrund, dass es im Medizinstudium keine Vorbereitung auf Führungsaufgaben und Konfliktbewältigung im Team gibt, dies aber ab dem ersten Arbeitstag im Krankenhaus benötigt wird, sei es sinnvoll, sich mit diesen Themen gezielt auseinanderzusetzen – gerade in einem so hierarchischen Setting wie im Krankenhaus.

In einer Coaching-Einheit vermittelte zum Abschluss des Ärztinnentages Carmen Schön, Coach und Autorin für Führungs- und Verhandlungsthemen, den Teilnehmerinnen nützliche Verhandlungstools: Verbale und nonverbale Kommunikationsstrategien, die dabei helfen, konkrete Verhandlungsziele zu erreichen – um zu lernen, sich selbst die Arbeitsbedingungen zu erkämpfen, die zum eigenen Leben passen.

Dies berufspolitisch und individuell zu unterstützen, ist Ziel des Ausschusses Ärztinnen, der die jährliche Veranstaltungsreihe „HB-Ärztinnentag“ begleitet.

Gesundheitsforum des Brandenburger Landesverbandes

# Umwertung der Werte durch die Ökonomisierung

*Prof. Dr. Giovanni Maio und Dr. Hanjo Pohle (rechts)*

***Die Frage der Werte in der Medizin spielt aus Sicht des Brandenburger Hartmannbundes eine ganz entscheidende Rolle. Der Landesverband hat sich hierzu bereits mehrfach öffentlich zu Wort gemeldet und nun eigens zu dieser Thematik im April in Potsdam ein Gesundheitsforum ausgerichtet. Eingeladen waren alle Ärztinnen, Ärzte und Medizinstudierende aus der Region. Als Hauptredner konnte Prof. Dr. Giovanni Maio, Universitätsprofessor für Bioethik der Universität in Freiburg im Breisgau und Facharzt für Innere Medizin, gewonnen werden.***

Maio wollte ursprünglich Arzt werden, weil er anderen Menschen helfen wollte – berichtete er zu Beginn seines Vortrages. Doch je länger er als Arzt arbeitete, desto deutlicher sei der Bruch zwischen dem Anspruch, mit dem er angetreten sei, und der Wirklichkeit zum Vorschein gekommen. Tatsächlich finde bereits im Studium eine „Umerziehung“ statt, die darauf ziele, dass der Mensch als das „zu Reparierende“ gesehen werde und Medizin als zweckrationale „Produktion von Handreichungen“.

Als Reaktion darauf sei es wichtig, zu den grundlegenden Fragen zurückzukehren: Wie funktioniert Medizin, wie funktioniert ärztliches Handeln? Medizin sei das Treffen von Entscheidungen unter Restunsicherheit und Handlungsdruck. Ärztinnen und Ärzte brauchen die Fähigkeit, diese Unsicherheit auszuhalten, klug zwischen den beiden Polen Aktionismus und Gelähmtheit zu entscheiden und neben der Apparatemedizin auch auf ihre Sinne zu vertrauen. Das eigentliche ärztliche Tun bestehe jedoch in der Reflektion, der Indikationsstellung, die zwischen Diagnose und Therapie liege. Darin liege auch das Spannende. Dieser Skizzierung ärztlichen Handelns stellte Maio das „industrielle Paradigma“ gegenüber, ein Denken, das eigentlich aus der Massenproduktion stamme und der Medizin übergestülpt werde.

Ärztinnen und Ärzte müssten sich besinnen, dass Medizin ein sozialer Beruf sei, der nur funktioniere, wenn eine Beziehung möglich ist. Medizin sei ihrem Wesen nach nicht nur reflexives Vorgehen, sondern eine wissenschaftlich gestützte zwischenmenschliche Praxis, um Menschen zu helfen. Wir alle müssten uns wehren, dass die Medizin weiter von der Politik in eine Richtung hineingezwängt werde, die nicht die ihre ist. Ärztinnen und Ärzte müssten gestärkt werden, sich über die bestehenden Strukturen der Medizin bewusst zu werden und darin ihrem Auftrag treu zu bleiben. Hierfür sei das Gesundheitsforum des Hartmannbundes ein guter Ort.

Der Vorsitzende des Brandenburger Hartmannbundes, Dr. Hanjo Pohle, betonte im Anschluss, wie wichtig es sei, zu hören, was eigentlich gehen sollte, wo wir stünden und welche Widersprüche wir erführen. In der regen Diskussion mit den Teilnehmenden wurde deutlich, dass die dem äußerlichen Anschein nach zu erwartende und die tatsächliche Realität in der Profession Medizin mindestens in dem Maße voneinander abweiche, wie es bei einer „Mockturtlesuppe“ der Fall sei.

Den vollständigen Bericht finden Sie unter:
***hartmannbund.de/kompetenzgipfel2022***

## Der studentische Blick

*Von: Sharie Kossatz, Studentin im 2. Semester*

Vor einem halben Jahr habe ich angefangen Medizin zu studieren. Ich fühle mich jetzt schon, als würde ich tief in der manchmal verqueren Welt von Medizin und Gesundheitswesen stecken. Es bleibt noch ein starker Idealismus, der für mich und sehr viele meiner Kommiliton*innen ein großer Motivationsgrund war, sich um unseren Studienplatz zu bemühen. Es geht uns darum einen Beruf mit Sinn zu erlernen, mit dem wir die Leben anderer Menschen verbessern können. Ich bin am Anfang, aber die idealistische Fassade bröckelt, wenn wir lernen unsere Patientengespräche möglichst zeiteffizient zu führen oder wir in unseren Studentenjobs in der Praxis die Patient*innen „schon eher“ zur teureren Behandlung anhalten sollen. Der Vortrag von Professor Maio war also ein passender Input zu meiner sich anbahnenden Frustration. Er beschrieb den gleichen Prozess steigender Unzufriedenheit, den ich jetzt über 30 Jahre später noch genauso erleben muss. Die ideale Patient*innenversorgung ist geprägt von Sorgfalt und Wandelbarkeit. Man solle sich auf jeden Menschen als Individuum einstellen können – stattdessen behandeln wir mit ständigem Einspar- und Zeitdruck. Dies führt zu einer fließbandartigen Abfertigung, die absolut ernüchternd für alle Beteiligten ist. Jeder Behandelte als auch Behandelnder, selbst der Lernende, ist sich der Probleme dieser ständigen Effizienzsteigerung bewusst. Diese ist sicher wirtschaftlich, aber lässt schwerlich das „Gute-Ärzt*in-sein“ zu. Zusammengefasst von Maio: Gutes Handeln ist ungleich zweckrationalem Handeln. Ich glaube das Thema des Gesundheitsforums hat uns Studierende nicht desillusioniert, sondern einen relevanten Einblick geschaffen, wie eine ideale Patientenversorgung aussehen könnte und warum wir diese Ideale noch nicht ausleben. Ich hoffe, dass endlich ein stärkerer gemeinsamer Antrieb gefunden werden kann, Lösungen für die Probleme der Ökonomisierung der Medizin zu finden.





Gesundheitsabsicherung in der privaten Krankenversicherung

# Welche Vorteile sich speziell für Frauen bieten …

***Mit dem Eintritt in das Berufsleben kommen auch in Bezug auf die eigene Gesundheitsabsicherung neue Fragen auf. Gerade Ärzt:innen haben schon vor dem Einstieg in das Berufsleben viele Kontaktpunkte mit dem Thema Gesundheitsabsicherung und können sich meist ein gutes Bild darüber machen, wie wichtig diese sein kann. Auch junge Assistenzärtzinnen fragen sich in diesem Zusammenhang, ob eine private Krankenversicherung (PKV) für sie als Frau interessant ist. Und was genau sind die Vorteile gegenüber der gesetzlichen Krankenversicherung?***

Keine Unterscheidung zwischen Männern und Frauen – Unisextarife machen es möglich: Ein wesentlicher Vorteil ist grundsätzlich, dass jeder – egal ob Frau oder Mann – sich entsprechend der eigenen Bedürfnisse den privaten Krankenversicherungsschutz individuell zusammenstellen kann. Zusätzlich sind alle tariflichen Leistungen der privaten Krankenversicherung – für die man sich einmal entschieden hat – ein Leben lang garantiert.

Dabei stehen Frauen und Männern alle Leistungen gleichermaßen zu, weshalb Beiträge auch geschlechtsneutral kalkuliert werden. Die Beiträge bemessen sich ausschließlich nach dem Eintrittsalter der Versicherten sowie dem aktuellen Gesundheitszustand. Es gibt allerdings keine Unterscheidung aufgrund des Geschlechts.

Doch was genau sind die speziellen Vorteile für Frauen bei einer privaten Krankenversicherung? Gerade wenn es um die speziellen Vorsorgeuntersuchungen für Frauen geht, zahlt sich eine private Krankenversicherung aus. Vor allem die gynäkologischen Untersuchungen zur Früherkennung von Erkrankungen wie Krebs sind dabei im Fokus. Diese werden zwar grundsätzlich auch in der gesetzlichen Krankenversicherung gezahlt, jedoch besteht bei einer privaten Absicherung auch hier eine größere Auswahl an Untersuchungen zur Verfügung.

Und auch wenn die Familienplanung eine Rolle spielt, lohnt sich ein weiterer Blick auf die angebotenen Leistungen. Denn gerade in der Schwangerschaft profitieren Frauen besonders von den Top-Leistungen ihrer privaten Krankenversicherung. Zu den attraktiven Leistungsvorteilen der privaten Krankenversicherung gehören beispielsweise Schwangerschaftsvorsorgeuntersuchungen, häufigere Ultraschalluntersuchungen, 3D-Ultraschall und die Pränataldiagnostik inklusive der Nackenfaltenuntersuchung oder einer Farbdopplersonografie.

Neben der Diagnostik spielt für Schwangere auch die Geburtsvorbereitung eine wichtige Rolle. Kosten für Geburtsvorbereitungskurs und Schwangerschaftsgymnastik werden im Normalfall in der privaten Krankenversicherung unbegrenzt bezahlt. Und für zusätzliche Angebote wie Aquafitness für Schwangere, Schwangerschaftsyoga und Hypnobirthing leisten sie ebenfalls.

Und wie sieht es mit der Versorgung nach der Geburt aus? Rückbildungsgymnastik wird schon kurz nach der Geburt für Frauen relevant. Die private Krankenversicherung erstattet die Kosten für Kurse, ganz unabhängig von der Anzahl der Sitzungen. Sehr praktisch: Auch Onlineangebote dürfen in Anspruch genommen werden. Somit haben Frauen auch hier die Möglichkeit sich ganz auf die Rückbildung einzulassen, ohne mögliche Selbstkosten im Blick behalten zu müssen.

Entlastung in der Elternzeit: Und auch nach der Geburt gibt es weitere Vorteile für Privatversicherte. Zwar müssen in der Elternzeit Beiträge für die private Krankenversicherung weitergezahlt werden, dies gilt aber auch für freiwillig Versicherte Mitglieder der gesetzlichen Krankenversicherung. Eine tolle Zusatzleistung ist allerdings, dass – je nach Versicherer – während des Elterngeldbezugs eine Beitragsfreiheit – für Frauen sowie Männer – bis zu sechs Monate möglich ist.

Kinder von Beginn an bestens absichern: Durch die sogenannte Kindernachversicherung kann auch das Kind direkt und ohne Gesundheitsprüfung von den Vorteilen und Top-Leistungen der privaten Krankenversicherung profitieren, sofern sie innerhalb von zwei bis drei Monaten nach der Geburt in die Versicherung mit aufgenommen werden.

Foto: Halfpoint/shutterstock.com

***Der gesicherte Einstieg in die private Gesundheitsabsicherung – der Optionstarif VIAlife:***

Auch wenn der Lebensweg noch nicht genau vorhersehbar ist – es ist immer von Vorteil sich alle Optionen offen zu halten. Mit VIAlife machen Sie den entscheidenden ersten Schritt in Ihre private Gesundheitsabsicherung. Schon heute können Sie Ihren Gesundheitszustand für Jahrzehnte einfrieren. Erhalten Sie sich mit VIAlife die Entscheidungsfreiheit, zu vielen verschiedenen Zeitpunkten in die private Gesundheitsabsicherung einzusteigen, oder passen Sie diese an Ihre veränderten Bedürfnisse an – ohne eine erneute Gesundheitsprüfung.

Und der spezielle Vorteil für Hartmannbund-Mitglieder: Der Hartmannbund übernimmt ab dem Beginn des praktischen Jahres die VIAlife-Beiträge für bis zu drei Jahre. Nach Ablauf dieser drei Jahre kann der Vertrag zum Beitrag von 5 Euro* monatlich weitergeführt werden.

*bis zum 35. Lebensjahr

apoBank-Studie „Inside Heilberufe“

# Finanzielle Sicherheit wird wichtiger!

*Wie sich die Pandemie in den letzten zwei Jahren auf die Stimmung, Werte, Ziele und Wünsche der Ärzteschaft ausgewirkt hat, zeigt die aktuelle Studie „Inside Heilberufe III“. Nach 2016 und 2019 hat die Deutsche Apotheker- und Ärztebank (apoBank) gemeinsam mit dem Institut DocCheck Insights in diesem Jahr bereits zum dritten Mal Angehörige der Heilberufe befragt – darunter 100 Allgemeinmediziner*innen und 100 Fachmediziner*innen. Die Ergebnisse spiegeln nun auch wider, wie sich ihr privater und beruflicher Alltag im Zeitverlauf verändert hat.*

**Materielle Werte gewinnen an Relevanz.** Den höchsten Stellenwert hat nach wie vor das Familienleben, das geben etwa neun von zehn aller befragten Ärztinnen und Ärzte an. Doch inzwischen genauso wichtig ist die finanzielle Sicherheit, entsprechend haben auch materielle Aspekte wie hohes Einkommen und Lebensstandard, Eigentum oder Vermögensbildung ebenfalls deutlich an Relevanz gewonnen.

### *Was ist wichtig im Leben?*

**Pandemie beeinträchtigt vor allem das Privatleben.** Vermutlich ist für die steigende Bedeutung der finanziellen Sicherheit nicht nur die Coronakrise verantwortlich, denn diesen Zusammenhang sehen nur 9 Prozent der Allgemeinärzte bzw. 13 Prozent der Fachärzte. Bei der Frage nach Auswirkungen der Pandemie zeigt sich, dass vor allem das Privatleben gelitten hat: Die Befragten sehen sich neben Reisen vor allem in ihrer Freizeit, gesunder Lebensweise und Fitness sowie beim Familienleben und ihrem gesellschaftlichen Engagement beeinträchtigt. Negative Auswirkungen auf ihre berufliche Karriere nennen lediglich 4 Prozent der Allgemeinärzte und 6 Prozent der Fachärzte.

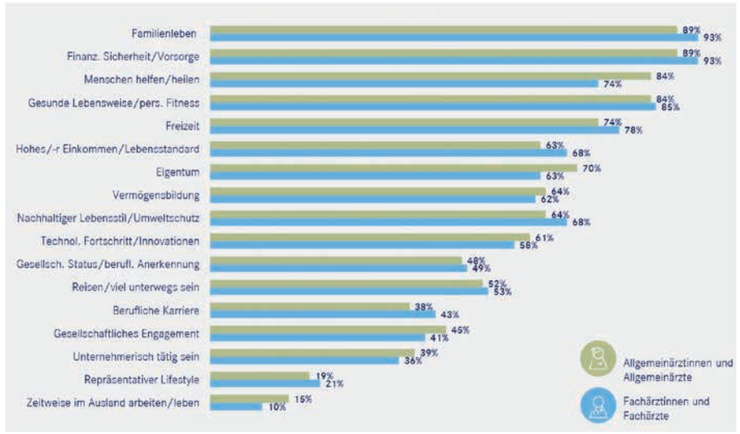
**Niederlassungsbereitschaft ähnlich wie vor Corona.** Offenbar hat die Pandemie keinen Einfluss auf die Bereitschaft der Ärztinnen und Ärzte zur Niederlassung ausgeübt: 13 Prozent der befragten Allgemeinärzte und 19 Prozent der Fachärzte planen in den nächsten drei Jahren eine Niederlassung – das ist jeweils ein Prozentpunkt mehr als vor Corona. Knapp ein Viertel wiederum bereitet sich auf den Ruhestand vor. Für 14 Prozent der Allgemeinärzte und 15 Prozent der Fachärzte bedeutet das die Aufgabe einer Praxis. Im Vergleich zu 2019 stehen damit um vier Prozentpunkte weniger allgemeinärztliche Praxen zu Übergabe. Bei fachärztlichen Praxen sind es lediglich ein Prozent mehr.

**Mehr fachlichen Austausch und Fortbildung gewünscht.** Bei der Frage nach den Wünschen für den beruflichen Alltag fällt auf, dass 2022 – sicherlich pandemiebedingt – deutlich mehr Austausch mit Kolleginnen und Kollegen gewünscht wird. Ebenso ist das Bedürfnis nach Fort- und Weiterbildung stark angestiegen. Der seit Jahren lautstarke Ruf nach weniger Dokumentations- und Verwaltungsarbeit bleibt weiterhin ganz oben auf der Wunschliste, offenbar ist hier immer noch keine Entlastung spürbar. Zu den größten Baustellen im Gesundheitswesen gehören laut der Befragten vor allem Fachkräftemangel und Bürokratie.

**Zufriedenheit nimmt weiter ab – dennoch Empfehlung des Arztberufs.** Insgesamt nahm seit 2016 die Zufriedenheit mit der beruflichen Situation ab, doch in der Corona-Zeit nur unwesentlich: bei Allgemeinärzten um einen Prozentpunkt bzw. um 3 Prozentpunkte bei Fachärzten. 55 Prozent der Allgemeinärzte geben an, zufrieden zu sein, unzufrieden sind 13 Prozent. Bei Fachärzten sind fast genauso viele (54 Prozent) zufrieden, dem gegenüber stehen 15 Prozent Unzufriedene. Alle anderen Befragten haben dazu eine neutrale Bewertung gewählt.

Etwas positiver verläuft die Entwicklung bei der Frage nach Weiterempfehlung des eigenen Berufs an junge Menschen, denn die Empfehlungsbereitschaft ist im Vergleich zu 2019 gestiegen: bei den Allgemeinärzten von 59 auf 64 Prozent und bei den Fachärzten von 49 auf 58 Prozent. Allerdings sind die Empfehlungsraten bei der ersten Befragung 2016 noch etwas höher gewesen: 70 Prozent bei Allgemein- und 62 Prozent bei Fachärzten.

Die Ergebnisse für alle Heilberufsgruppen, also auch für Zahnmediziner*innen und Apotheker*innen, gibt es im Newsroom der apoBank:








Neues Angebot von MEDI-LEARN

# Kurs für Telenotärztinnen/-ärzte

Immer mehr Regionen richten im Zuge der Ausweitung telemedizinischer Anwendungen auch Telenotarzt-Systeme ein. Für interessierte Mediziner:innen aus der Notfallmedizin bietet MEDI-LEARN passend dazu einen 56-stündigen Kurs für Telenotärztinnen/-ärzte an.

**Kurs in drei Modulen:** MEDI-LEARN greift für seinen Kurs auf das von den beiden Ärztekammern Nordrhein und Westfalen-Lippe entwickelte „Curriculum Qualifikation Telenotarzt“ zurück. Der nächste Kurs von MEDI-LEARN findet aufgeteilt in drei Module im Juli und August jeweils am Wochenende statt: An zwei Wochenenden erfolgt der Unterricht digital in Form eines Online-Seminars, das dritte Wochenende wird als Präsenzseminar absolviert.

**Experten für Theorie & Praxis:** Der Kurs umfasst zusätzlich zu der im Curriculum geforderten 28-stündigen Fortbildung „Telenotarzt“ weitere 28 Stunden praktische Übungen in der Funktion als Telenotärztin/-arzt. Ein interdisziplinäres Expertenteam mit langjähriger Erfahrung in Notfallmedizin und Rettungswesen vermittelt im Kurs neben dem erforderlichen theoretischen Wissen also insbesondere die praktische Anwendung anhand von konkreten Fallbeispielen und interaktiven Weiterer Inhalt des Kurses ist die Ausbildung in Team Resource Management (TRM) basierend auf dem Konzept von FaktorMensch®, um im Team im Notfall sicher zu handeln und menschliche Fehler – jenseits von Fachwissen – in Notfallsituationen zu vermeiden.

**Zertifizierung & CME:** Jeder der von MEDI-LEARN angebotenen Kurse für Telenotärztinnen/-ärzte wird bei der jeweils zuständigen Ärztekammer zertifiziert, sodass CME-Punkte erworben werden können.

**Info & Kurstermine:**
**www.medi-learn-praeklinik.de**

Wir sind für Sie da

# Exklusive Konditionen bei Europcar für Hartmannbund-Mitglieder

*Sie planen Ihren nächsten Familienurlaub, benötigen einen Transporter für den Umzug oder möchten sich privat oder für Ihre Praxis schlichtweg kein eigenes Fahrzeug kaufen? Dann sind Sie bei uns genau richtig. Als Europas führende Autovermietung bieten wir Ihnen von Tages- über Wochenmieten bis hin zum Auto-Abo die Mobilität, die Sie benötigen. Seit über 90 Jahren können Sie sich bei uns auf professionellen Service mit persönlichem Ansprechpartner verlassen.*

Durch unser dichtes Stationsnetz mit weltweit 3.500 Standorten in über 140 Ländern sind wir überall dort für Sie präsent, wo Sie uns privat oder beruflich brauchen. So finden Sie uns direkt in Ihrer Heimatstadt sowie am Flughafen Ihres Urlaubsortes. Unsere vielfältige Flotte reicht von modernen Kleinwagen, über sportliche Coupés und elegante Limousinen bis zu geräumigen Transportern sowie einer wachsenden Elektro-Flotte.

Wohin Sie Ihr Weg auch führt: Bei Europcar sind wir für Sie da. Wir haben die richtige Mobilität zur richtigen Zeit am richtigen Ort für Sie – und wir entwickeln uns kontinuierlich für Sie und Ihre Anforderungen weiter.

Zum Beispiel haben wir in 2021 unsere Abo-Angebote für Unternehmen sowie Privatkunden in Deutschland gestartet. Damit können Sie die für Sie individuell notwendige Mobilität besonders flexibel und komfortabel gestalten ohne sich langfristig zu binden. Diese All-inclusive-Abos passen optimal zum aktuellen Trend “Nutzen statt Besitzen” und gleichzeitig zu unserem Ziel, Ihnen attraktive und nachhaltige Alternativen zum Fahrzeugbesitz anzubieten.

**Als Hartmannbund-Partner erhalten Sie bei Europcar besondere Konditionen und Services wie:**

- Die kostenlose Europcar Privilege Executive Card
- Ihren persönlichen Ansprechpartner: Gabor Laszlo (gabor.laszlo@europcar.com)
- Individuelle und feste Konditionen für Pkw in Deutschland als auch international geltend
- Individuelle Lkw-Konditionen
- Um bei der Buchung von Ihren exklusiven Hartmannbund-Konditionen zu profitieren, nutzen Sie bitte immer die Contract ID 40295733.
- Jetzt losfahren und die exklusiven Vorteile als Hartmannbund-Mitglied nutzen.

Deglobalisierung – Die Weltwirtschaft nach der Pandemie

# Vernetztes System zeigt seine Verletzlichkeit

***Die globale Pandemie und der militärische Konflikt in der Ukraine werden über die nächsten Jahre zu einer verstärkten Neuausrichtung von globalen Wertschöpfungs- und Lieferketten führen. Die Zinswende und Rezessionsängste führten jüngst zu unerwartet starken Kursabschlägen an Wertpapiermärkten. Die Risiken werden derzeit deutlich stärker gewichtet als die Chancen. Ein Fehler?***

Die Weltwirtschaft profitierte über die letzten drei Jahrzehnte von einer steigenden globalen Arbeitsteilung und der Perfektionierung von fein abgestimmten Lieferketten. Sinkende Armut, stabiles Wirtschaftswachstum und eine sinkende Inflation waren positive Auswirkungen dieser Globalisierung. Die Zentralbanken konterten auftauchende Krisen mit immer stärkeren Geldschwemmen, auch während der jüngsten Pandemie. Die tiefen Zinsen stärkten den Konsum und führten zu einem steigenden Wohlstand dank steigender Preise bei nahezu allen Vermögenswerten. Auf der Gewinnerseiten standen Unternehmen und private Haushalte. Auf der anderen Seite erreichte die Verschuldung der öffentlichen Hand immer neue Höchstwerte.

Die globale Pandemie hat die Verletzlichkeit unseres vernetzten Systems schonungslos aufgedeckt. Noch nie wurde die Weltwirtschaft synchron gestoppt und wieder hochgefahren. Noch ist nicht klar, wie viele Jahre es dauert, bis die feingliedrigen Vernetzungen wieder eingespielt sind. Die Preise steigen seit Monaten unter anderem wegen gestörter Lieferketten, Chipmangel, der anhaltenden Null-Covid Toleranz in China und auch als Folge von stark steigenden Energiepreisen wegen des Krieges in der Ukraine.

Ein neuer Trend zeichnete sich ab. Unternehmen und Staaten möchten die Abgängigkeiten von Dritten in Zukunft reduzieren oder zumindest diversifizieren. Wir kommen in eine neue Phase der «Deglobalisierung». Die Sicherung von Lieferketten und die Produktion im Inland sollen eine grössere Rolle spielen. Die Abgängigkeit vom Energielieferanten «Russland» ist plötzlich keine Option mehr, auch wenn bezahlbare Alternativen nicht in Sichtweite sind. Deglobalisierung und ein Umbau der Wirtschaft werden zu grossen Verwerfungen und einem nachhaltigen höheren Preisniveau führen. Gewinner und Verlierer zeichnen sich ab. Der Binnenmarkt wird sicher profitieren.

Die oben erläuterten Themen belasten die Märkte genauso wie fehlende Arbeitskräfte in den USA und Europa. Die Zentralbanken sind gefordert; höheren Zinsen sollen die Wirtschaft und die Nachfrage nach Gütern rasch abkühlen, denn das Angebot reagiert nur mit Verzögerung. Das Risiko einer Rezession nimmt zu und wird bewusst in Kauf genommen. An den Börsen reagieren die Anleger sehr nervös. Besonders betroffen sind Titel aus dem Wachstumssegment mit hohen Kurs-Gewinn Bewertungen, während Substanzwerte eher profitieren. Viele Qualitätsunternehmen wurden jedoch über Mass abgestraft.

*Jacqueline Krämer, Leiterin Privatkunden, Bank Alpinum AG*

Für Anleger an den Märkten wird es wichtig sein, diese globale Trendwende richtig zu erfassen. Diversifikation in Themen wie Energie, Rohstoffe aber auch erneuerbare Energien und Nachhaltigkeit bietet genauso gute Chancen wie auf qualitativ starke Unternehmen zu setzten, die höhere Preise durchsetzen können.





Zertifizierung aus ärztlicher Hand

# Qualitätsmanagement gewinnt an Bedeutung

***Jede Vertragsarztpraxis muss heute eine Vielzahl von externen Vorgaben einhalten, den Praxisbetrieb organisieren und Vieles mehr. Diese Aufgaben sind in den immer häufiger gebildeten Gemeinschaftspraxen noch komplexer und umfangreicher. Qualitätsmanagement, das dabei helfen kann, die anstehenden Tätigkeiten systematisch vorzubereiten und umzusetzen, kann in dieser Situation sehr nützlich sein. Viele Praxen betreiben aus diesen Gründen schon Qualitätsmanagement.***

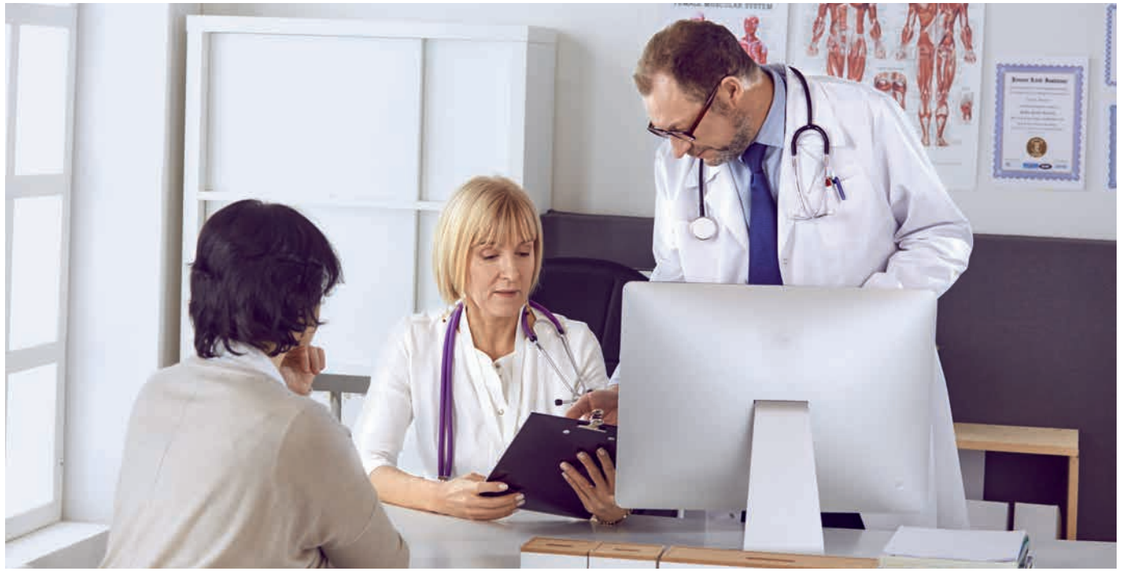


Foto: Micolas/shutterstock.com

Wenn Ihr Qualitätsmanagement einen gewissen Reifegrad erreicht hat, bietet sich unter Umständen eine Zertifizierung an. So kann die Praxis ein funktionierendes Managementsystem nach außen darstellen Eine regelmäßige Auditierung führt erfahrungsgemäß auch zu einer zunehmenden Compliance des gesamten Teams für die getroffenen Regelungen. Teilweise wird eine Zertifizierung bei der Zusammenarbeit mit den Kostenträgern z.B. im Rahmen der integrierten Versorgung sogar gefordert.

Natürlich stellt die Vorbereitung auf eine Zertifizierung für die Vertragsarztpraxis zusätzliche Arbeit dar. Auch fallen für die eventuell erforderliche Ausbildung von Mitarbeitern Kosten an. Dieser Aufwand ist jedoch meist geringer, als angenommen wird. Außerdem wird Ihr Qualitätsmanagementsystem davon profitieren.

Bleibt dann zum Ende noch die Auswahl einer Zertifizierungsstelle. Dabei sollten Sie unbedingt darauf achten, dass die Stelle für Ihre Aufgaben auch zugelassen ist, also akkreditiert wurde.

ÄKzert®, die Zertifizierungsstelle der Ärztekammer Westfalen Lippe, erfüllt diese Bedingung für die DIN 9001(akkreditiert von der Deutschen Akkreditierungsstelle) und KPQM (akkreditiert durch die Kassenärztlichen Vereinigung Westfalen-Lippe). Sie ist eine der wenigen Zertifizierungsstellen in Deutschland, die von einer Ärztin geleitet wird. Die Zertifizierungsstelle hat sich in ihren eignen Vorgaben verpflichtet, für Audits in ärztlich geleiteten Einrichtungen grundsätzlich einen Arzt oder eine Ärztin als leitenden Auditor einzusetzen.

ÄKzert® betreut ausschließlich medizinische und Medizin-nahe Einrichtungen. Dabei wird das Verfahren und strikter Einhaltung aller Akkreditierungsvorgaben möglichst kundenfreundlich durchgeführt. Auch auf die Bedürfnisse des Praxisbetriebes wird stets so weit möglich eingegangen.

Aufgrund eines Rahmenvertrages zwischen dem Hartmannbund und ÄKzert® gelten für Mitglieder des Verbandes reduzierte Zertifizierungskosten

***Ihre Ansprechpartnerin***

ÄKzert® — Die Zertifizierungsstelle
der Ärztekammer Westfalen-Lippe
Gartenstr. 210 — 214
48147 Münster
Wiebke Wagener
0251 929-2601
info@aekzert.de

In fünf Schritten …

# … zur Steuererklärung für Selbermacher

***Sie nehmen ihr Leben gerne selbst in die Hand und das gilt auch für die steuerliche Angelegenheiten? Mit der richtigen Unterstützung gelingt Ihnen das garantiert.***

Erstellen Sie schnell, leicht verständlich und mit maximaler Steuererstattung Ihre Steuererklärung 2021. Die Software führt Sie im Frage-Antwort-Stil durch die Steuererklärung und das ganze fehlerfrei ohne Steuerwissen. Mit der SteuerSparErklärung werden jährlich mehr als eine Million Steuererklärungen erstellt. Profitieren Sie von über zwei Jahrzehnten Softwareentwicklung. Holen Sie jetzt schnell und einfach mehr aus Ihrer Steuererklärung 2021 heraus! Profitieren Sie von zahlreichen Steuertipps und automatischen Optimierungsmöglichkeiten. Kostenlose Updates halten Sie steuerrechtlich immer auf dem aktuellen Stand.

Sicherheit für Ihre Daten. Ihre sensiblen Daten sind bei Ihnen am besten aufgehoben. Die Daten werden nur auf Ihrem PC oder Mac gespeichert und verschlüsselt übertragen.


***Ärmel hoch uns los geht's:***
***In 5 Schritten zur Steuererklärung***

Schluss mit unübersichtlichen Steuerformularen. Lassen Sie sich bequem von der Software-Funktion „Roter Faden" durch Ihre Steuererklärung führen.

1. **So machen Sie alles richtig:** Dank des „Roten Fadens" ist Ihre Steuererklärung der reinste Spaziergang: Die SteuerSparErklärung führt Sie Schritt für Schritt durch Ihre Steuererklärung.
2. **Genau das, was Sie brauchen … und nichts anderes.** Über einen Filter werden nur die Themen behandelt, die Ihre persönliche Steuerveranlagung angehen. Nicht mehr und nicht weniger.
3. **Von der Lohnsteuerbescheinigung direkt ins Formular.** Ihre Lohnsteuerbescheinigung vom Arbeitgeber dient als Vorlage für Ihre Dateneingabe. Belege müssen Sie nur noch abfotografieren und ins Programm übernehmen!
4. **Kaum ausgefüllt – schon auf Sparchancen gecheckt.** Optimierung inklusive! Was bisher nur ein Steuerberater schaffte, kann Ihr Programm jetzt auch: Die anschließende Steuerprüfung verrät, wie Sie noch mehr rausholen
5. **Ab ans Finanzamt.** Elektronisch mit ELSTER oder ausgedruckt per Post – jetzt kann Ihre Steuererklärung raus. Wir bleiben dran: Die SteuerSparErklärung prüft Ihren späteren Steuerbescheid sogar auf Richtigkeit.







# Interview mit UMFST-Rektor Prof. Leonard Azamfirei

Der Hartmannbund-Partner MediStart (www.medistart.de) vermittelt Studienplätze ohne Hochschulstart-NC im EU-Ausland – und seit 2019 auch ein „Auslandsstudium im Inland", nämlich in Hamburg. Möglich ist dies dadurch, dass nach europäischem Recht haben Universitäten die Möglichkeit, eine Niederlassung in einem anderen EU-Staat zu eröffnen. Die George Emil Palade Universität für Medizin, Pharmazie, Naturwissenschaften und Technik Neumarkt a. M. (UMFST) aus Siebenbürgen/Rumänien hat hiervon Gebrauch gemacht und den Universitätsmedizin Neumarkt a. M. Campus Hamburg (UMCH) in Deutschland gegründet. Wir sprachen mit dem Universitätsrektor Prof. Leonard Azamfirei, MD, PhD, um mehr über dieses außergewöhnliche Unterfangen zu erfahren.

**Hartmannbund: Prof. Azamfirei, die UMFST hat unter Ihrer Federführung 2019 eine Niederlassung in Hamburg eröffnet: den UMCH. Wie kam es dazu?**
Prof. Azamfirei: Die UMFST bietet an ihrem Hauptstandort im rumänischen Neumarkt a. M. [rum.: Târgu Mureș, Anm. d. Red.] bereits seit weit über 10 Jahren einen englischsprachigen Studiengang in Humanmedizin und Zahnmedizin an. Über die Jahre hinweg konnte hier bereits eine Vielzahl von deutschen Absolventinnen und Absolventen, die mittlerweile auf dem deutschen und internationalen Arbeitsmarkt tätig, das englischsprachige Studium abschließen. Neumarkt a. M. liegt in der dreisprachigen Region Siebenbürgen, in der es neben rumänischsprachigen auch eine beträchtliche Anzahl ungarisch- und deutschsprachiger Einwohner gibt. Aufgrund der daraus resultierenden Verbundenheit mit Deutschland sowie unserer Erfahrung in der englischsprachigen Ausbildung angehender Ärztinnen und Ärzte war die Gründung einer Niederlassung in Deutschland naheliegend.

**Hartmannbund: Was können Sie uns über den Abschluss sagen, den man am UMCH erhält?**
Prof. Azamfirei: Der Abschluss, der am UMCH nach 6 Jahren Studium erworben wird, entspricht der in Anhang V der EU-Berufsanerkennungsrichtlinie und in § 3 der Bundesärzteordnung (BÄO) aufgeführten Berufsqualifikation und bildet die Grundlage für die Erlangung der Approbation als Ärztin beziehungsweise Arzt in der EU und in Deutschland. Er ist damit äquivalent zum Staatsexamen, das an den staatlichen Universitäten in Deutschland abgelegt wird. Der Studiengang basiert zudem auf dem European Credit Transfer System (ECTS) und ist somit Bologna-konform.

**Hartmannbund: Welche Vorteile haben die Studierende am UMCH gegenüber denen, die an einer staatlichen deutschen Universität eingeschrieben sind?**
Prof. Azamfirei: Ein großer Vorteil ist die Kombination des englischsprachigen Medizinstudiums am Campus in Hamburg mit den klinisch-praktischen Studienabschnitten, die in einem Netzwerk von deutschen Lehrkrankenhäusern stattfinden. Daraus ergibt sich einerseits eine ausgeprägte Internationalität, die den Studierenden später zum Vorteil gereichen kann, andererseits lernen sie das deutsche Gesundheitssystem und die Arbeit mit deutschen Patientinnen und Patienten kennen. Der Campus in Hamburg selbst verfügt über eine ultra-moderne physische und digitale Infrastruktur, die es unseren Studierenden unter anderem ermöglicht, unabhängig von Zeit und Ort auf Kursinhalte wie Streamings von Vorlesungen zuzugreifen.

**Hartmannbund: Welche Angebote werden den Studierenden darüber hinaus am UMCH geboten?**
Prof. Azamfirei: Neben einem ausgeprägten Studierendenleben, das unter anderem aus extracurricularen Workshops und Vorträgen sowie verschiedenen Student Clubs in Bereichen wie Sport, Musik und gemeinnützigen Aktivitäten besteht, bieten wir unseren Studierenden auch die Möglichkeit, sich in der Forschung zu engagieren. So haben wir beispielsweise die so genannte Junior Researcher Academy ins Leben gerufen, die Forschungsbegeisterten Studierenden die Möglichkeit bietet, frühzeitig in diesem Bereich tätig zu werden. Darüber hinaus können sie auch am ERASMUS-Programm teilnehmen und somit einen Teil ihres Studiums im Ausland absolvieren.

**Hartmannbund: Wie gestaltet sich das Zulassungsverfahren für das Medizinstudium am Campus in Hamburg? Ist dieses vergleichbar mit dem, das an anderen Universitäten üblich ist?**
Prof. Azamfirei: Schulnoten – etwa in den naturwissenschaftlichen Fächern – spielen bei der Zulassung zum Studium am UMCH keine entscheidende Rolle. Diese erfolgt unabhängig von den ansonsten in Deutschland üblichen NC-Regelungen. Stattdessen besteht unser Zulassungsverfahren aus einer Kurzevaluation, die sich aus grundlegenden Fragen in den Bereichen Biologie, Chemie und Allgemeinwissen zusammensetzt, sowie einem Interview, bei dem die Motivation der Studieninteressierten im Vordergrund steht. Für diejenigen, die vor dem Studium noch etwaige Wissenslücken schließen und sich optimal darauf vorbereiten möchten, bieten wir zudem einen 3-wöchigen Crashkurs sowie einen 12-wöchigen Intensivkurs an.

**Hartmannbund: Welche Kosten kommen auf die Studierenden zu, wenn sie sich für ein Studium am UMCH entscheiden?**

Prof. Azamfirei: Für das akademische Jahr 2023/24, für das die Bewerbung bereits jetzt möglich ist, betragen die Studiengebühren 14.000€ pro Semester. Darüber hinaus besteht auch die Möglichkeit, einen Teil des Studiums in Neumarkt a. M. zu absolvieren. Wer die Kosten für das Studium am UMCH nicht aus eigener Kraft aufbringen kann, hat darüber hinaus die Möglichkeit, bei der Hamburger Sparkasse eine Teilfinanzierung anzufragen. Der maximale Kreditbetrag liegt hier bei 100.000 €. Zusätzlich bieten immer mehr Landkreise und Kliniken Stipendien für unsere Studierenden auf dem Hamburger Campus an.

**Hartmannbund: Planen Sie, mit dem UMCH in Zukunft noch weiter zu expandieren?**
Prof. Azamfirei: Absolut. Da wir kürzlich unsere Kapazität von 150 auf 200 neue Studierende pro Studienjahr in Hamburg erhöht haben, werden wir weiter wachsen – allerdings auf organische Art und Weise. Die Qualität der Lehre steht auch bei einem Wachstum für uns im Vordergrund. Wir meinen, dass Lehre und Forschung immer im Gleichgewicht sein müssen. Dies gewährleisten wir nicht zuletzt durch strikte Qualitätssicherungsprozesse.

**Hartmannbund: Vielen Dank, Prof. Azamfirei.**

Hinweis: MediStart ist die einzige Agentur, die von der UMFST und dem UMCH zur Studienplatzvermittlung an deutsche Abiturientinnen und Abiturienten autorisiert ist. Das Aufnahmeverfahren wird von MediStart umfassend vorbereitet. Eine Bewerbung und Zulassung ist auch bereits während des letzten Schuljahres möglich. Bislang hat MediStart eine Erfolgsquote von 100% am UMCH erzielt; eine Garantie stellt dies jedoch nicht dar. Kinder und Enkel von Hartmannbund-Mitgliedern erhalten einen Rabatt von einmalig 1.000,00 Euro auf das Erfolgshonorar, das von MediStart bei erfolgreicher Zulassung berechnet wird.

**MediStart GmbH & Co. KG Medizin-Studienplatzberatung & Auslands-Agentur für Medizin, Zahnmedizin und Tiermedizin**
Telefon: (040) 413 436 60
Telefax: (040) 413 436 61
E-Mail: info@medistart.de
Web: www.medistart.de

# Ansprechpartner für Mitglieder

*Der Hartmannbund steht Ihnen mit qualifizierten Mitarbeiterinnen und Mitarbeitern für die politische Verbandsarbeit, die Mitgliederberatung und den Mitgliederservice zur Verfügung. Haben Sie Fragen? Dann können Sie sich direkt an Ihren Gesprächspartner wenden. Unten stehend finden Sie die Kontaktdaten. Weitere Informationen finden Sie im Internet auf www.hartmannbund.de. Schauen Sie doch mal vorbei.*

© burak çakmak – fotolia.com

**Ärztliche Niederlassung und Kooperationen**
Frances Camin
Tel.: 030 206208-31

**Ärztliche Tätigkeit im Ruhestand**
Sabine Eckhardt
Tel.: 030 206208-15

**Ärztliche Weiterbildung**
Ina Reiber
Tel.: 030 206208-24

**Ausbildung/Medizinstudium**
Ina Reiber
Tel.: 030 206208-24

**Auslandstätigkeit/Internationale Angelegenheiten**
Dr. med. Michael Vogt
Tel.: 030 206208-20

**Berufsbezogene Rechtsberatung**
Axel Barenhoff /Sabine Haak/Sandy Stephan
Tel.: 030 206208-43

**Berufsbezogene Steuerberatung**
Christian Rahe
Tel.: 030 206208-46

**Betriebswirtschaftliche Praxisführung**
Christian Rahe
Tel.: 030 206208-46

**Digital Health**
Frances Camin
Tel.: 030 206208-31

**Fortbildungen/Seminare**
Johanna Heinrichs
Tel.: 030 206208-53

**GKV-Vertragsrecht**
Frances Camin
Tel.: 030 206208-31

**Honorar- und Abrechnungsfragen (GKV/GOÄ)**
Frances Camin
Tel.: 030 206208-31

**Praxisbewertung und Praxisanalyse**
Christian Rahe
Tel.: 030 206208-46

**Rechtsberatung Krankenhaus**
Axel Barenhoff
Tel.: 030 206208-58

**Rechtsberatung Niederlassung**
Sabine Haak/Sandy Stephan
Tel.: 030 206208-43

**Sektorübergreifende Versorgung und Krankenhausstrukturen**
Petra Meiners
Tel.: 030 206208-27

## Regional

**Regionalreferat Nord**
(Landesverbände Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Schleswig-Holstein)
Heike Ortlieb
Tel.: 030 206208-65

**Regionalreferat Ost**
(Landesverbände Berlin, Brandenburg, Sachsen, Sachsen-Anhalt, Thüringen)
Philipp Hoffmann
Tel.: 030 206208-41

**Regionalreferat West**
(Landesverbände Nordrhein, Westfalen-Lippe, Hessen)
Jeannette Hristov
Tel.: 030 206208-62

**Regionalreferat Süd**
(Landesverbände Baden-Württemberg, Bayern, Rheinland-Pfalz, Saarland)
Sara Daub
Tel.: 030 206208-18





# Kleinanzeigen – für Mitglieder kostenlos*

## ABZUGEBEN/ZU VERKAUFEN

### GYN KV-Sitz zu verkaufen im Kreis Mettmann (Südkreis)

Ich möchte gern meinen KV-Sitz (1.050 Scheine) mit oder ohne Eile verkaufen!
Bin offen für viele Möglichkeiten.
Kontakt: gynkvsitzmettmann@gmx.de

### 2 Sehtestgeräte in Thüringen sehr kostengünstig abzugeben

Ein Sehtestgerät OCULUS Binoptometer II und ein Audiometer MAICO ST 20 jeweils mit Zubehör an Selbstabholer in Arnstadt (Thüringen) sehr kostengünstig abzugeben.
Bei Interesse bitte Kontaktaufnahme: Dr. Nennstiel, Tel: 03628 – 41357.

### Pensionierter Gynäkloge bietet Urlaubs- und Krankheitsvertretung an (bundesweit)

Nach 33 Jahren eigener GYN-Praxis möchte ich gern in Teilzeit (15-20Std./Woche) als Urlaubs- und/oder Kranheitsvertretung meine Hilfe und langjährige Erfahrung Ihrer Praxis anbieten.
Ich suche bundesweit und bin flexibel. Bei Interesse bitte unter: 0172-20 88 227 oder c.schoengart@t-online.de melden.

## GESUCHT

### Facharzt für Orthopädie und Unfallchirurgie/D-Arzt im Kreis Minden-Lübbecke gesucht

Für einen frei werdenden vollen KV Sitz in chirurgischer 2-er Praxisgemeinschaft wird ein Facharzt für Orthopädie und Unfallchirurgie/D-Arzt gesucht. Die Anstellung mit der Möglichkeit der späteren Übernahme oder der Erwerb der Praxis sind ebenso möglich, wie die Umwandlung in eine Gemeinschaftspraxis zusammen mit dem verbleibenden Kollegen. Der Erwerb wird von der Stadt mit 75.000 € unterstützt!
Unsere Praxisgemeinschaft ist seit Jahrzehnten in unserer sympathischen Kleinstadt mit großem ländlichen Einzugsbereich gut etabliert. Unser tolles Praxisteam arbeitet in einer über 350 qm-großen und funktionell ausgerichteten Praxis mit digitalem Röntgen, Sonografie und eigenem ambulanten OP einschließlich Durchleuchtungseinheit etc. sehr motiviert zusammen.
Haben wir Ihr Interesse geweckt? Bitte melden Sie sich gern zu einem unverbindlichen Gespräch oder Besuch.
Kontakt: Dr. med. Ali Mahdi, Tel. 0171 3857670

### Nachfolgerin/Nachfolger für HNO- Gemeinschaftspraxis in Braunschweig gesucht

HNO-Gemeinschaftspraxis mit 3 Arztsitzen sucht Nachfolgerin/Nachfolger zum 01.01.2023 oder später. Die seit mehr als 25 Jahren etablierte Praxis mit breitem Diagnostik- und Therapiespektrum liegt in einem Ärztehaus (7 weitere Arztpraxen, eine Apotheke, ein Hörgeräteakustikgeschäft) im Zentrum von Braunschweig. Die Verdienstmöglichkeiten sind überdurchschnittlich, der Patientenstamm ist groß, der Privatpatientenanteil hoch. Eine belegärztliche Tätigkeit ist möglich. Das Praxisteam ist eingespielt, das Arbeitsklima angenehm.
Ggf. ist auch die Übernahme eines halben KV-sitzes möglich.
Kontaktaufnahme unter: HNO-BS@vodafonemail.de

Sie möchten auf eine Chiffreanzeige antworten oder selbst ein Inserat aufgeben? Dann wenden Sie sich bitte an: Hartmannbund, Andrea Reich, Kurfürstenstr. 132, 10785 Berlin, Tel.: 030 206208-11, Fax: 030 206208-14, E-Mail: andrea.reich@hartmannbund.de.
*Im Mitgliedsbeitrag enthalten ist die Schaltung von zwei Anzeigen (außer rein gewerbliche) im Jahr.

*IMPRESSUM*

**Herausgeber:**
Hartmannbund – Verband der Ärztinnen und Ärzte Deutschlands e.V.
Kurfürstenstraße 132 · 10785 Berlin
Tel. 030 206208-0, Fax 030 206208-29
www.hartmannbund.de
E-Mail: hb-info@hartmannbund.de

**Redaktion:**
Michael Rauscher (v.i.S.d.P.)
Gitta Dietrich
Pressereferat Hartmannbund
Kurfürstenstraße 132, 10785 Berlin
Tel. 030 206208-11, Fax 030 206208-14
E-Mail: presse@hartmannbund.de
Titelthema Ausgabe 02/2022 von:
Aileen Hohnstein

**Verlag:**
Köllen Druck+Verlag GmbH
Postfach 41 03 54 · 53025 Bonn
Ernst-Robert-Curtius-Str. 14 · 53117 Bonn
Tel. 0228 98982-90, Fax 0228 98982-99
E-Mail: r.akarcay@koellen.de

**Anzeigenverwaltung:**
Rohat Akarcay, Köllen Druck+Verlag GmbH

**Satz & Gestaltung:**
Köllen Druck+Verlag GmbH
Ernst-Robert-Curtius-Straße 14
53117 Bonn
www.koellen.de

**Druck & Vertrieb:**
Köllen Druck+Verlag GmbH
Ernst-Robert-Curtius-Straße 14
53117 Bonn
Mitteilungsblatt des Hartmannbundes – Verband der Ärztinnen und Ärzte Deutschlands e.V.

**Erscheinungsort:**
Bonn – 4 Ausgaben jährlich
Einzelheft 3,50 Euro
Jahresabonnement 12 Euro,
incl. 7 Prozent MwSt., zzgl. Versandkosten
ISSN: 0944-7369
Für Mitglieder des Hartmannbundes ist der Bezugspreis durch die Mitgliedschaft abgegolten. 

## Stufenweise Einführung

# Aktuelles zum E-Rezept


Foto: Agenturfotografin/shutterstock.com

*1. Stufe - 1. September 2022*
*Start in Pilot-Praxen und -Krankenhäusern in den Bereichen der KV Westfalen-Lippe und KV Schleswig-Holstein.*
Ziel: Durch sukzessive Integration des E-Rezeptes in den regulären Versorgungsprozess soll eine schnellstmögliche Flächenabdeckung erreicht werden. Bis zum Start der verbindlichen Nutzung des E-Rezeptes sind alle Praxen und Krankenhäuser angehalten, von der Möglichkeit der E-Rezept-Ausstellung Gebrauch zu machen. Dies ist auch außerhalb der benannten und im Fokus stehenden Regionen möglich und angeraten. Zudem werden in Stufe 1 die Apotheken deutschlandweit E-Rezepte annehmen. Die E-Rezept-App und die Website www.das-e-rezept-fuer-deutschland.de informieren die Versicherten darüber, welche Apotheken E-Rezepte schon heute annehmen können.

*2. Stufe - 1. Januar 2023*
Nach Prüfung des Erfolges der ersten Stufe wird per Beschluss in den Startregionen das E-Rezept verpflichtend eingeführt und in sechs weiteren KV-Bereichen sukzessive die Einführung umgesetzt.

*3. Stufe - Frühjahr*
übrige 9 KV-Bereiche

**Achtung:** Der Prozess der Verordnungen von Zytostatika und damit verbundener Begleitmedikation wird von der geplanten verpflichtenden Nutzung des E-Rezepts ausgenommen und in einem unabhängigen Verfahren getestet. Die Anpassungen am Fachdienst und in den Softwaresystemen der Ärzte, Apotheken und insbesondere der Krankenhäuser werden derzeit vorgenommen und zunächst in einer Testumgebung geprüft. Ab Ende 2022 wird voraussichtlich die separate Testphase starten.

(Stand Juni 2022) https://www.gematik.de/anwendungen/e-rezept/faq/einfuehrung

**Mehr aktuelle Informationen auf www.hartmannbund.de**