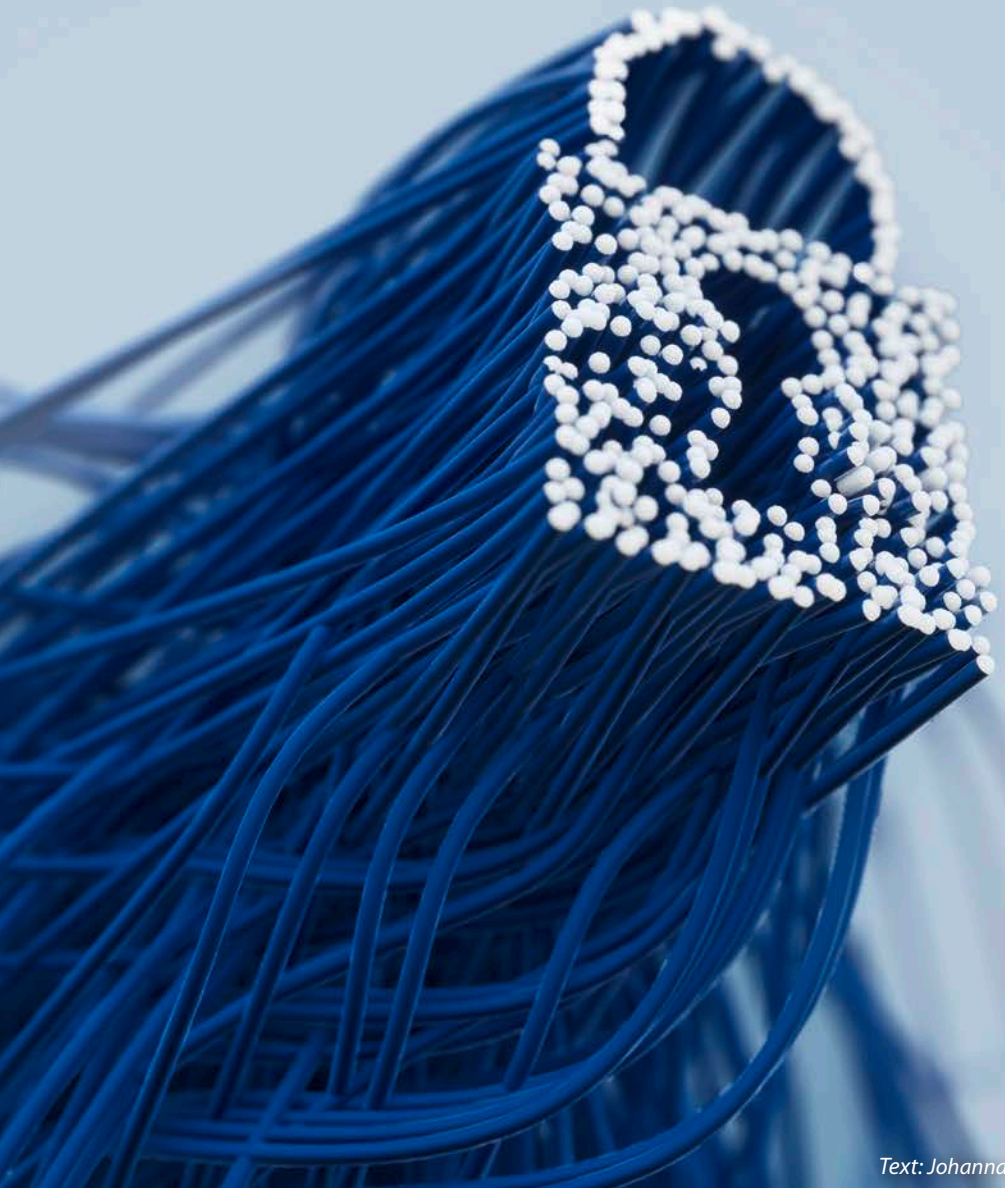
Anforderungen an die IT-Sicherheit

Sichere Technik *Was ist in Kliniken, Praxen und sonstigen medizinischen Einrichtungen zu tun, um die IT-Sicherheit zu gewährleisten. Rechtsanwältin Johanna Clausen hat sich dieses Thema für den BVKD angesehen und gibt praktische Tipps.*



Text: Johanna Clausen.

Hackerangriffe sind kein Hirngespinst aus Science-Fiction-Filmen und in der realen Welt sind auch nicht nur Regierungen oder Industriekonzerne Ziel von Cyberkriminellen. Nachdem der Virus „Emotet“ zahlreiche Unternehmen, gleich welcher Größe, lahmgelegt hat, haben Datenpannen und Hackerangriffe auch auf medizinische Einrichtungen Schlagzeilen gemacht. Solche Vorfälle stellen nicht nur einen unangenehmen Umstand für die Betroffenen dar, zählen Gesundheitsdaten doch zu den sensibelsten Informationen über eine Person; das Vertrauensverhältnis zwischen dem

Redaktion: 06131/9607035

Patienten und der behandelnden Einrichtung würde langfristig beschädigt oder zerstört. Nicht zuletzt der Hackerangriff auf die Heinrich-Heine-Universität in Düsseldorf im September vergangenen Jahres hat aber auch gezeigt, dass neben Unannehmlichkeiten wegen ausgefallener IT-Systeme auch Menschenleben bedroht sein können. Der Angriff auf die Uni Düsseldorf hatte zur Folge, dass auch das Universitätsklinikum Düsseldorf nicht auf die IT-Systeme zugreifen konnte. Aufgrund dessen musste ein Rettungswagen mit einer Patientin nach Wuppertal umgeleitet werden, die kurz nach Einlieferung verstarb. Nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik hätte bereits ein einfacher Grundschutz den Angriff auf die IT-Systeme vereiteln können, zumal das BSI bereits zu-

i Über die Autorin

Johanna Clausen ist Rechtsanwältin bei Taylor Wessing am Berliner Standort. Sie berät überwiegend im Datenschutz sowie in urheber-, wettbewerbs-, IT- und fernabsatzrechtlichen Themen sowie sonstigen technologierechtlich relevanten Fragestellungen. Sie berät im Zuge dessen zur Umsetzung und Einhaltung der DS-GVO. Ein Schwerpunkt von Johanna Clausen liegt in der Beratung gesundheitsbezogener Datenschutzfragen, wie etwa im Rahmen klinischer Studien, und e-Health.

vor auf mangelnde Sicherheitsvorkehrungen in dem Krankenhaus verwiesen hatte.

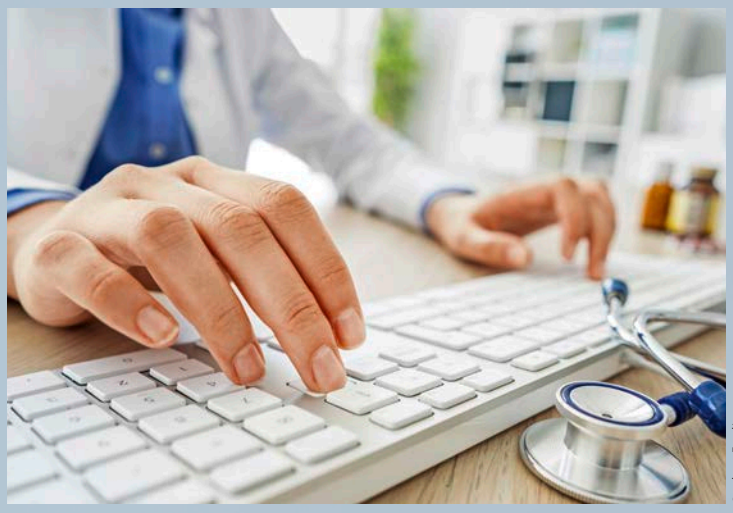
Datenschutzrechtliche Haftung bei nicht ausreichendem Schutz

Auch die Datenschutzaufsichtsbehörden sind hellhörig geworden und haben diese datenschutzrechtlich relevanten Vorgänge im Fokus. Denn eine unbefugte Offenlegung von Gesundheitsdaten bzw. das Fehlen ausreichender Schutzmaßnahmen vor einem unbefugten Zugriff auf personenbezogene Daten kann nach den Vorgaben der Datenschutz-Grundverordnung („DS-GVO“) mit einem Bußgeld belegt werden. Hierbei stehen Summen von bis zu 20 Mio. Euro oder 4 % des weltweiten Bruttojahresumsatzes, je nachdem, welcher Betrag höher ist, für Fälle der Zuwiderhandlung im Raum.

Gesetzliche Verpflichtung zur Gewährleistung angemessener Schutzmaßnahmen

Die DS-GVO legt in Art. 32 fest, dass der Verantwortliche gehalten ist, „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“ technische und organisatorische Maßnahmen zu ergreifen. Darunter sollen etwa fallen: die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme im Zusammenhang mit der Verarbeitung sicherzustellen. Ferner wird die Fähigkeit genannt, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen nach einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der ergriffenen Maßnahmen zu schaffen.

> *„Durch Angriffe auf die IT-Technologie können auch Menschenleben gefährdet sein.“*


© zebra - Fotolia

Für den Gesundheitssektor hat das Bayerische Landesamt für Datenschutz („BayLDA“) hat eine Checkliste mit Prüfkriterien herausgegeben.

Was bedeutet das konkret für Gesundheitsdaten?

Nach Art. 32 sind bei der Beurteilung des angemessenen Schutzniveaus insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind. Der Wortlaut der Vorschrift aus der DS-GVO bleibt insoweit ungenau. Das hat den Grund, dass sie eine Vielzahl von Fällen regeln muss. Es verbleibt die Frage, welche Sicherheitsmaßnahmen im konkreten Fall getroffen werden müssen. Für den Gesundheitssektor hat das Bayerische Landesamt für Datenschutz („BayLDA“) hat eine Checkliste (abrufbar unter www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf) mit Prüfkriterien herausgegeben, die es medizinischen Einrichtungen ermöglichen soll, einen Überblick zu erhalten und sensibilisiert zu werden. Die Liste beinhaltet präventive Maßnahmen, wie etwa eine dem neuesten Stand entsprechende Virus-Software, zählt aber ebenfalls Instrumente wie Passwortschutz, Backups und Anleitung bei Cyberattacken und ein Notfall-Konzept auf. Im Rahmen der Beurteilung der vorhandenen und noch zu schaffenden Maßnahmen kann keine schematische Antwort gegeben werden. Vielmehr wird sich dies stets nach den Gegebenheiten des Einzelfalls richten. Hierbei kommt es darauf an, was für IT-Systeme bereits vorhanden sind, welcher Schutz bislang existiert und auf welche Weise personenbezogene Daten, einschließlich Gesundheitsdaten, verarbeitet werden.

Überprüfung der Maßnahmen

Es bietet sich daher aus mehreren Gesichtspunkten an, die für den Schutz der Daten ergriffenen IT-Sicherheitsmaßnahmen zu prüfen und gegebenenfalls nachzubessern. IT-Sicherheit läuft in der Regel zwar im Hintergrund ab, wenn jedoch etwas „schief“ läuft, kann dies nicht nur zu monetären Konsequenzen führen, sondern auch zu einem Vertrauensverlust auf Seiten der Patienten. Die nach der DS-GVO statuierte Pflicht, Maßnahmen zur IT-Sicherheit zu ergreifen betrifft jeden, der personenbezogene Daten als Verantwortlicher (oder auch Auftragsverarbeiter) verarbeitet, wobei Gesundheitsdaten als besondere Kategorien personenbezogener Daten ausgesprochen sensibel sind. Sie bedürfen daher in der Regel einem höheren Schutzstandard als „gewöhnliche Daten“. Um festzustellen, ob die getroffenen Maßnahmen ausreichend die Sicherheit der verarbeiteten Daten gewährleisten, müssen sie regelmäßig auf den Prüfstand gestellt werden. Mit einer ausführlichen Dokumentation kann man der datenschutzrechtlichen Rechenschaftspflicht nachkommen.

„Ausführliche Dokumentation gehört zur datenschutzrechtlichen Rechenschaftspflicht.“

Gute Zusammenarbeit ist das (Ver-)Schlüsselwort

Wenn nunmehr Einrichtungen die technischen und organisatorischen Maßnahmen überprüfen wollen, muss eine Zusammenarbeit mit den entsprechenden Mitarbeitern aus der IT-Abteilung oder, wenn es sich um eine kleinere Einheit handelt, mit einem externen Berater erfolgen. Denn eine Einschätzung, welche Maßnahmen angesichts der Verarbeitung von (Gesundheits-) Daten angemessen sind und dem Stand der Technik entsprechen, erfordert Fachwissen. Die Checkliste des BayLDA kann insoweit als erster Anhaltspunkt dienen und einen Einblick in den Status quo geben, sofern kein eigenes Konzept vorliegt. Unvermeidlich ist es jedoch, die Maßnahmen auf die eigenen Verarbeitungsvorgänge und IT-Systeme anzupassen.

Wie wichtig die IT-Sicherheit im Gesundheitsbereich ist, hat auch die Politik erkannt. Die Bedingungen für eine Inanspruchnahme des mit bis zu 4,3 Mrd. Euro ausgestatteten „Krankenhauszukunftsfonds“, der die Digitalisierung von Krankenhäusern fördern soll, sehen vor, dass 15 % der Fördersumme für IT-Sicherheit ausgegeben werden müssen.

heinz@kirchheim-verlag.de

Autor

Johanna Clausen
Rechtsanwältin bei Taylor Wessing
Berlin
E-Mail: j.clausen@taylorwessing.com