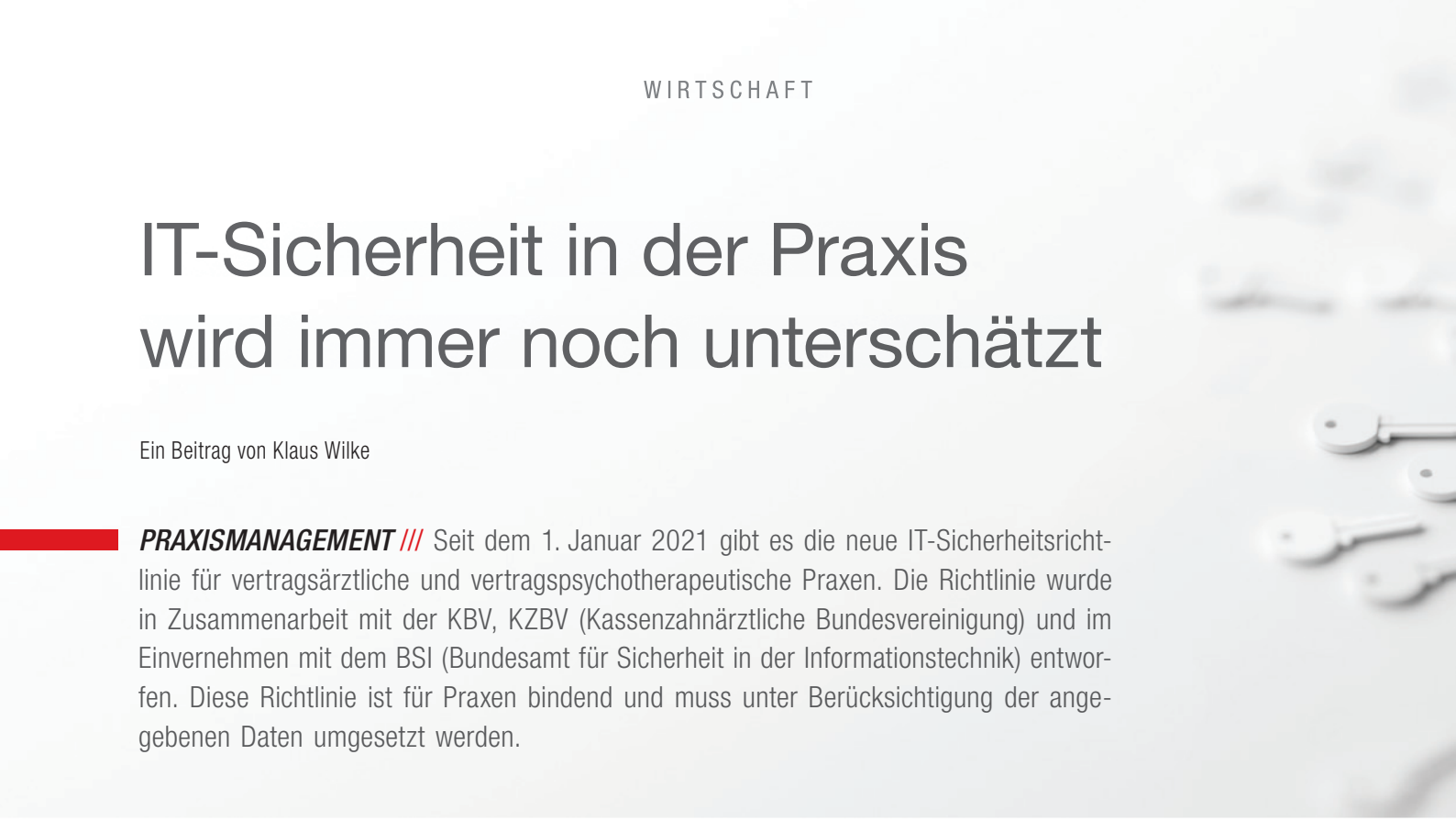
# IT-Sicherheit in der Praxis wird immer noch unterschätzt

Ein Beitrag von Klaus Wilke



***PRAXISMANAGEMENT*** /// Seit dem 1. Januar 2021 gibt es die neue IT-Sicherheitsrichtlinie für vertragsärztliche und vertragspsychotherapeutische Praxen. Die Richtlinie wurde in Zusammenarbeit mit der KBV, KZBV (Kassenzahnärztliche Bundesvereinigung) und im Einvernehmen mit dem BSI (Bundesamt für Sicherheit in der Informationstechnik) entworfen. Diese Richtlinie ist für Praxen bindend und muss unter Berücksichtigung der angegebenen Daten umgesetzt werden.

Viele Praxisinhaber*innen und IT-Dienstleister*innen wissen leider noch nicht, dass eine derartige IT-Sicherheitsrichtlinie existiert. Vor diesem Hintergrund ist es umso wichtiger, sich mit diesem Thema zu beschäftigen und wenn nötig, sich bei Spezialisten*innen zu informieren.

Grundsätzlich regelt die DSGVO (Datenschutz-Grundverordnung) den Schutz der personenbezogenen Daten. Letztlich ist diese teilweise zu ungenau oder für Praxen nur sehr schwer umzusetzen, sodass der Gesetzgeber die KBV und die KZBV damit beauftragt hat, diese Regelungen auf die Praxen anzupassen und zu vereinheitlichen. Die Richtlinie ist strukturell aufgebaut und orientiert sich an drei verschiedenen Praxisgrößen: Praxis, mittlere Praxis und Großpraxis mit krankenhausähnlicher Struktur sowie MVZs oder Labore. Des Weiteren gibt es noch die Anlage 4, die für Praxen gedacht ist, welche mit Großgeräten wie z. B. Computertomografen arbeiten. Es gibt fünf Anlagen, die je nach Praxisgröße zu berücksichtigen und umzusetzen sind. Die Sicherheit richtet sich immer an die Anzahl der Personen, die ständig mit der Datenverarbeitung betraut sind, und den Umfang der zu verarbeitenden Daten.

## Schutz von Daten

Im Zeitalter der Digitalisierung werden immer mehr Daten über das Netz ausgetauscht. Es ist bequem, einfach und schnell. Allerdings ist dieser Datenaustausch auch mit einer Vielzahl an Risiken verbunden. Vor allem Gesundheitsdaten, die sehr sensibel sind, werden von Kriminellen hoch gehandelt und müssen deswegen besonders geschützt werden. Gerade während der Coronakrise haben solche Angriffe auf IT-Systeme zugenommen. Die IT-Sicherheit wird leider viel zu häufig unterschätzt und hat bei einem erfolgreichen Angriff meist verheerende Folgen für die Praxen. Es gibt eine Vielzahl an erfolgreichen Hackerangriffen – einige Angriffe werden erkannt, andere bleiben allerdings unentdeckt. Laut TÜV Hessen-Blog wurden 2019 in Deutschland Tests von renommierten IT-Sicherheitsunternehmen gemacht, die die Sicherheit der Praxen auf den Prüfstand stellten, und das mit erschreckenden Ergebnissen: Fast 80 Prozent der Praxen wären nicht mehr in der Lage, ihre Patienten*innen zu behandeln. Gerade einmal fünf Minuten dauerte es in einer Praxis, um an sensible Daten zu kommen. Teilweise könnte mit einfachsten Mitteln eine relativ gute Sicherheit hergestellt werden, zum Beispiel durch Schulungen der Mitarbeiter*innen, die einen wesentlichen und nicht zu unterschätzenden Teil darstellen. Social Engineering hat einen immer noch sehr hohen Bestand in der Hackerszene und wird immer besser. Gerade (Spear-)Phishing-Attacken werden dabei immer professioneller und sind kaum bis gar nicht zu unterscheiden von Original-E-Mails.

## Sicherheitsrichtlinie

Aufgrund dessen beschäftigten sich auch die KBV und KZBV mit diesem Thema und haben eine einheitliche Sicherheitsrichtlinie auf den Weg gebracht, die auf den jeweiligen Seiten für Praxen, aber auch für IT-Dienstleister*innen zur Verfügung steht. Der

***INFORMATION*** ///

**Klaus Wilke**
IT-Sicherheits-Beauftragter/Manager (TÜV)
KBV-zertifiziert nach § 75b Absatz 5 SGB V
Geschäftsführer/Inhaber
Safe Cyber Identity
www.mvs-sci.de


übergeordnete Auftrag der KBV und KZBV lautet, die technisch-organisatorischen Maßnahmen in den Praxen gemäß Artikel 32 Datenschutz-Grundverordnung (DSGVO) zu standardisieren. Die Richtlinie beschreibt ein Mindestmaß an technischen Anforderungen, um die IT-Sicherheit und die Schutzziele Vertraulichkeit, Integrität sowie Verfügbarkeit in den Praxen zu gewährleisten und sicherzustellen. Da sich die Bedrohungslage kontinuierlich ändert, ist es auch sehr wichtig, sich in regelmäßigen Abständen, jedoch laut Richtlinie mindestens einmal im Jahr, mit der IT-Sicherheit zu beschäftigen, um so gewährleisten zu können, dass man auf dem aktuellen Stand der Technik ist.

## Hilfestellung

Für die Praxisinhaber*innen bedeutet diese Richtlinie erst einmal nichts Schlimmes. Es soll lediglich der Schutz der personenbezogenen und -beziehbaren Daten gewährleistet werden, insbesondere der Gesundheitsdaten, die nach Artikel 9 der DSGVO der besonderen Kategorie angehören, und somit vielmehr meiner Meinung nach als Unterstützung gesehen werden. Praxisinhabern*innen soll durch diese Richtlinie eine Hilfestellung gegeben werden, um ein Mindestmaß an IT-Sicherheit in der Praxis umsetzen zu können. Die Richtlinie zeigt auch, dass die IT-Sicherheit in der heutigen Zeit immer wichtiger wird, und die Verantwortung, die Praxisinhaber*innen gegenüber den Patientendaten tragen, soll mit dieser Richtlinie deutlich gemacht werden.
Es gibt immer Schwachstellen, die nicht mit geeigneten Mitteln oder mit viel zu teuren Methoden abgesichert werden können. Dafür gibt es Möglichkeiten, wie Versicherungen oder IT-Dienstleister*innen einen Teil der Verantwortung übernehmen können. Oder Praxisinhaber*innen akzeptieren die Restrisiken, was allerdings nicht anzuraten ist, da die Kosten bei einem Sicherheitsvorfall enorm sein können, bis hin zum Verlust der existenziellen Grundlagen. Ein weiterer Punkt ist auch der Reputationsverlust. Diese Restrisiken sind durch eine Versicherung meist sehr gut abgedeckt.

## Fazit

Abschließend würde ich den Praxisinhabern*innen empfehlen, sich mit Ihrer Praxis-IT auseinanderzusetzen, da in letzter Konsequenz immer die Praxisinhaber*innen für die IT-Sicherheit verantwortlich sind. Dann würde ich empfehlen, sich zertifizierte Berater*innen zu holen, die einen Maßnahmenplan für die Praxis erarbeiten, der dann von den jeweiligen IT-Dienstleistern*innen der Praxis umzusetzen ist.