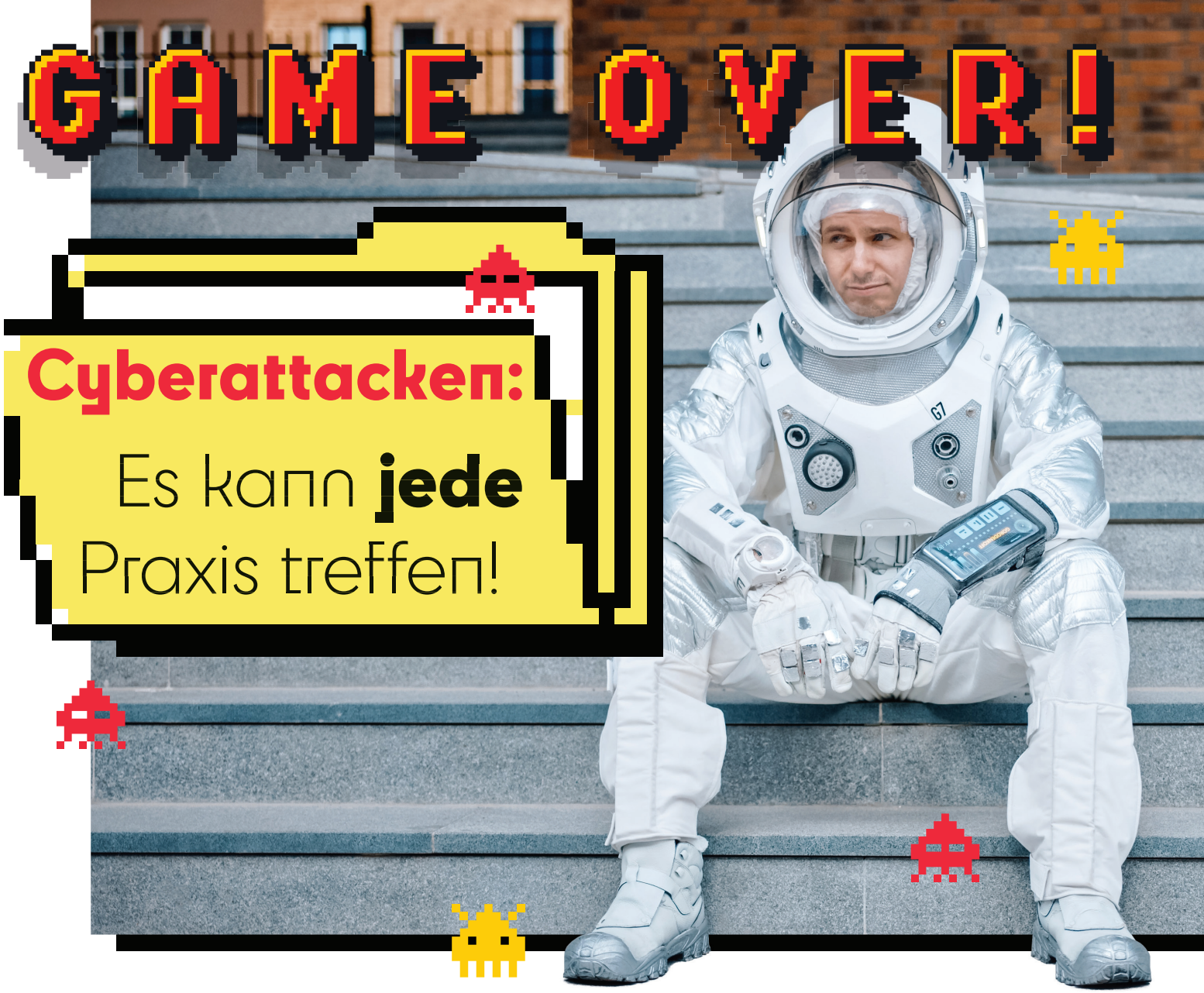


Cyberattacken: Es kann **jede** Praxis treffen!

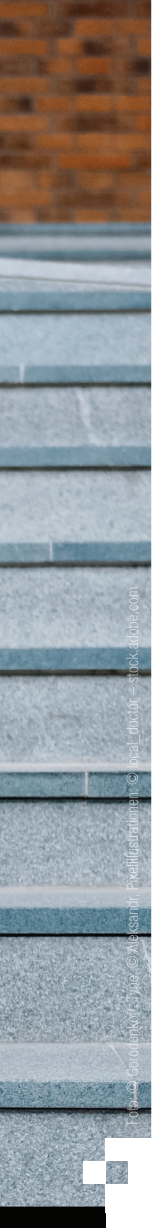
Ein Beitrag von Dr. Tobias Witte

PRAXISMANAGEMENT /// Die Rolle der IT-Sicherheit in Zahnarztpraxen hat in den vergangenen Jahren zunehmend an Relevanz und Dringlichkeit gewonnen. Spätestens nach einem Hackerangriff auf das Uni-Klinikum Düsseldorf im Jahr 2020, bei dem aufgrund eines umgeleiteten Rettungswagens die beförderte Patientin ums Leben kam, sind die verheerenden Folgen von Cyberattacken und die Notwendigkeit gut ausgestatteter Sicherheitsvorkehrungen im Gesundheitssektor unübersehbar.

Trotz dieses abschreckenden Beispiels lässt die Cybersicherheit in vielen Praxen nach wie vor zu wünschen übrig. Dies verdeutlichen die Zahlen des Cybersecurity-Branchenreports des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV).[1] Laut der Studie denkt jeder zweite Arzt, Zahnarzt oder Apotheker, dass sein Unternehmen zu klein wäre, um in den Fokus von Cyberkriminellen zu geraten. Etwa 80 Prozent der Teilnehmenden an der Studie denken zudem, dass sie ausreichend gegen Cyberkriminalität geschützt seien, was dazu führt, dass ein Drittel der Beteiligten keine weiteren Investitionen in IT-Sicherheit plant.

Cyberangriff mit Ransomware

Verdeutlicht man sich die Folgen eines Hackerangriffs, sind diese Zahlen nur schwer nachvollziehbar. Bei Erfolg eines Cyberangriffs mit einem Verschlüsselungstrojaner, sogenannter Ransomware, erhalten die Praxen eine Lösegeldforderung, um die



verschlüsselten, hochsensiblen Patientendaten freischalten zu lassen. Werden Daten dabei von den Hackern abgefangen und kopiert, muss der Praxisinhaber alle betroffenen Patienten von Gesetzes wegen darüber informieren. Das kann existenzgefährdend sein.

Die „Ransomware“ gelangt auf unterschiedlichen Wegen in das System. Die wohl bekannteste Methode ist dabei das „Social Engineering“, also die zwischenmenschliche Beeinflussung mit dem Ziel, das Opfer zur freiwilligen Preisgabe vertrauenswürdiger Informationen zu bewegen. Dies geschieht oft mittels E-Mails. Auch Zahnarztpraxen werden gut formulierte und täuschend echt aussehende Angebote, Nachfragen oder sonstige Mitteilungen zugeschickt und dazu verleitet, ein angehängtes Dokument zu öffnen und weitere Schritte aktiv vorzunehmen. Dies reicht bereits, um das System zu infizieren.

> Mit den Mindeststandards der **IT-Sicherheitsrichtlinie** bestehen erstmals klare Handlungsanweisungen für die Gewährleistung von IT-Sicherheit in Zahnarztpraxen.

Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung

Aufgrund der Zunahme von Hackerangriffen trat im Februar 2021 die „Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung“ in Kraft. Der Gesetzgeber hatte KZBV und KBV zuvor gesetzlich verpflichtet, die IT-Sicherheitsanforderungen für Zahnarzt- und Arztpraxen in einer eigenen Richtlinie verbindlich festzulegen. Übergeordnetes Ziel ist es dabei, mittels klarer Vorgaben Praxen zu unterstützen, hochsensible Gesundheitsdaten noch besser zu schützen. Die Zahnärzteschaft hatte sich bei der Erstellung der Richtlinie über viele Monate massiv und letztlich mit Erfolg dafür eingesetzt, dass die gesetzlichen Vorgaben für Zahnarztpraxen mit vernünftigem und vertretbarem Aufwand umsetzbar sind und die Anforderungen auf das tatsächlich notwendige Maß konzentriert wurden. Die Anforderungen werden daher gezielt auf die jeweilige Praxisgröße ausgerichtet und definieren besonders relevante sicherheitstechnische Voraussetzungen für Aufbau und Betrieb der Praxis-EDV.

Anforderungen an kleine Praxen

Bei einer „kleinen Praxis“ im Sinne der Richtlinie sind bis zu fünf Personen ständig mit der Datenverarbeitung betraut. Diese Praxen müssen die Anforderungen aus Anlage 1 und 5 umsetzen. Dazu gehören das Nutzen sicherer Apps

Leitfaden der KZBV und BZÄK

(Anl. 1 Nr. 1) und deren laufende Aktualisierung (Nr. 2). Diese Anforderungen sind gut in den laufenden Alltag der Praxis zu integrieren und daher bereits seit dem 1.4.2021 verpflichtend. Seit dem 1.1.2022 müssen die Praxen anspruchsvollere Punkte umsetzen, wie etwa die sichere Speicherung lokaler App-Daten (Nr. 3) sowie das Einrichten einer Firewall (Nr. 9).

Anforderungen an mittlere Praxen

Um eine „mittlere Praxis" handelt es sich, wenn zwischen sechs und 20 Personen ständig mit der Datenverarbeitung betraut sind. Diese haben, zusätzlich zu den Vorgaben aus Anlagen 1 und 5, die Anforderungen der Anlage 2 zu beachten. Dazu zählen seit dem 1.4.2021 die Kontrolle und Minimierung von App-Berechtigungen (Nr. 1) sowie seit dem 1.1.2022 die Regulierung der Mitnahme von Wechseldatenträgern (Nr. 10). Man darf Mitarbeitern also nicht ohne Weiteres USB-Sticks oder externe Festplatten mitgeben – dies muss schriftlich geregelt werden. Weitergehende Anforderungen wie die Erstellung einer Richtlinie für Mitarbeiter zur Nutzung von mobilen Geräten (Nr. 6) mussten bis zum 1.7.2022 umgesetzt werden. Hier ist also für alle „mittleren Praxen" akuter Handlungsbedarf.

Anforderungen an Großpraxen

In einer „Großpraxis" sind über 20 Personen ständig mit der Datenverarbeitung betraut. Für diese gelten die zusätzlichen Anforderungen aus Anlage 3. Dies bedeutet eine wirksame Datenträgerverschlüsselung (Nr. 10; seit 1.4.2021) und eine von der Praxis festzulegende Definition der erlaubten Informationen und Applikationen auf mobilen Endgeräten (Nr. 3; seit dem 1.1.2022). Wer also beispielsweise Tablets in der Praxis nutzt, muss hier aktiv werden.

Zusatzkriterium: Medizinische Großgeräte

Nutzt eine Praxis medizinische Großgeräte (CT, MRT, PET oder LINAC), hat sie unabhängig von ihrer Größe die Anlage 4 zu beachten. Dort sind die Anforderungen an die Nutzung der Geräte festgesetzt (z. B. Protokollierung von Systemereignissen, Nr. 3), die alle frühestens zum 1.1.2022 umzusetzen waren.

Leitfaden von BZÄK und KZBV

Zahnarztpraxen soll mit dem „Nachschlagewerk" von KZBV und BZÄK der Umgang mit der IT-Sicherheitsrichtlinie zusätzlich erleichtert werden. Diese wird bei allen relevanten Aspekten und Informationen des Leitfadens berücksichtigt. Unter anderem werden die Anforderungen an den Einsatz von PCs, Mobilgeräten, Tablets und medizinischen Geräten sowie von Praxissoftware anschaulich erläutert. Weitere Themen sind der sichere Einsatz von Netzwerken, Internet- und Online-Anwendungen sowie der Telematikinfrastruktur (TI). Ein zusätzlicher zentraler Aspekt sind grundlegende Hinweise zur zahnärztlichen Schweigepflicht in Verbindung mit datenschutzrechtlichen Regelungen.

Verstoß gegen die Vorgaben

Wird die Richtlinie nicht umgesetzt, sind Bußgelder in einer Höhe von bis zu 10 Mio. Euro bzw. bis zu zwei Prozent des weltweiten Jahresumsatzes möglich (vgl. Art. 83 Abs. 4 DSGVO) – in der Theorie. Wenngleich diese Summen nie ausgeschöpft werden würden, so kann ein Bußgeldverfahren doch nicht unerheblich Zeit, Nerven und Geld kosten.
Die Vernachlässigung der in der Richtlinie niedergelegten Standards kann bei einem Systemausfall und/oder einem Datenabfluss außerdem dazu führen, dass sich der Praxisinhaber oder der für die IT Verantwortliche zugleich datenschutzrechtlichen Ermittlungen ausgesetzt sieht. In Extremfällen – so wie beim Fall des Uniklinikums Düsseldorf – ist auch eine Ermittlung wegen fahrlässiger Körperverletzung oder fahrlässiger Tötung möglich.

Sicherheit muss sein!

Mit den Mindeststandards der IT-Sicherheitsrichtlinie bestehen erstmals klare Handlungsanweisungen für die Gewährleistung von IT-Sicherheit in Zahnarztpraxen. Diese Standards umzusetzen, wird damit ein integraler Bestand der IT Compliance. Sollte es zu einem Hackerangriff auf die Praxis kommen, werden Aufsichts- und Ermittlungsbehörden in jedem Fall prüfen, ob und inwieweit die Sicherheitsstandards umgesetzt und aufrechterhalten wurden. Zahnarztpraxen sind daher gut beraten, sich – sofern noch nicht geschehen – mit den Inhalten der Richtlinie vertraut zu machen und die Vorgaben umzusetzen.

1 Branchenreport Cyberrisiken bei Ärzten und Apotheken, Gesamtverband der Deutschen Versicherungswirtschaft e.V., 2019, www.gdv.de

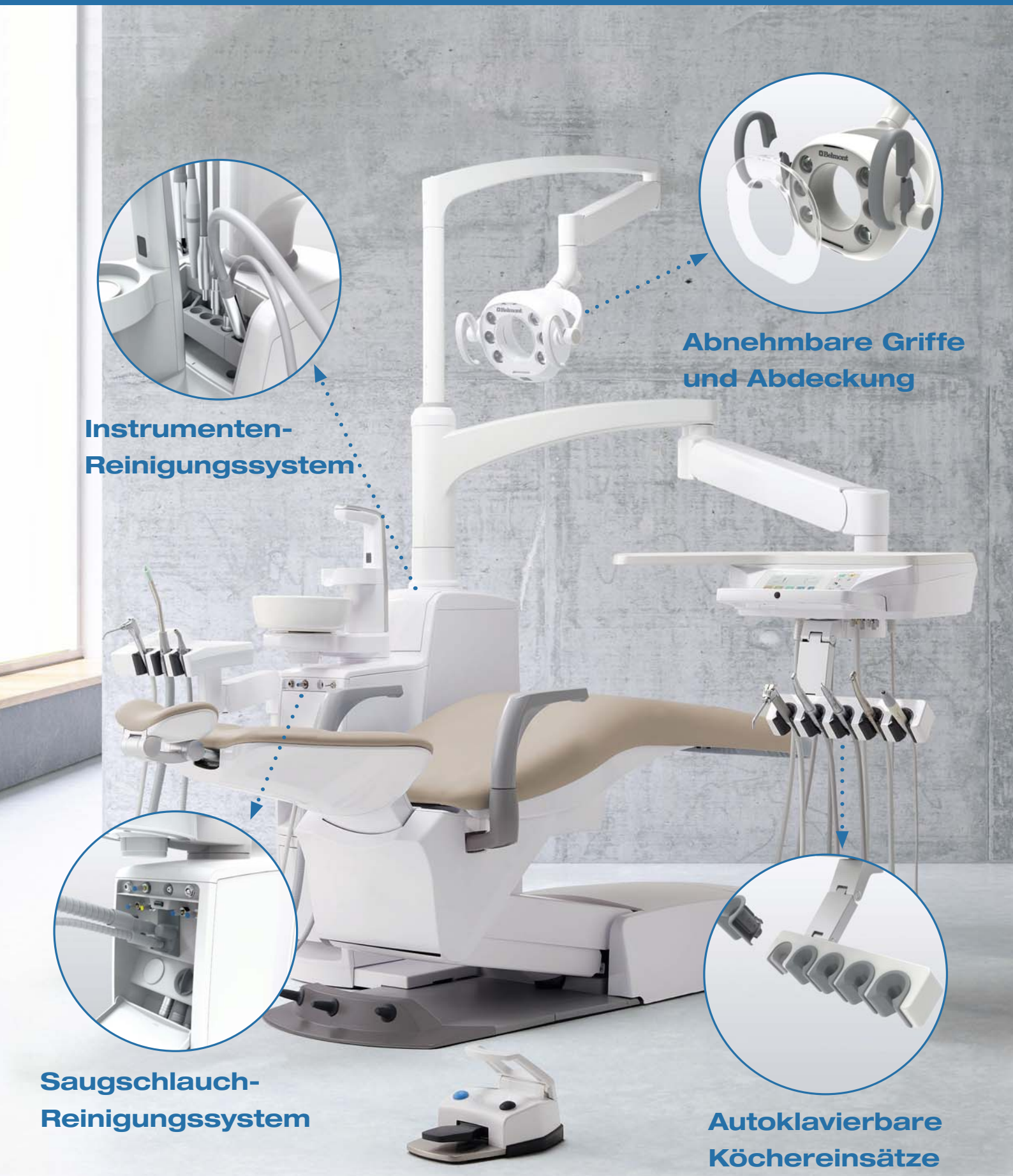
INFORMATION ///

Dr. Tobias Witte
Rechtsanwalt & Partner
Fachanwalt für Medizinrecht
Fachanwalt für IT-Recht
Justiziar | Datenschutzbeauftragter
www.kwm-law.de

Infos zum Autor

Eurus

Entwickelt für eine perfekte Hygiene



Instrumenten-
Reinigungssystem

Abnehmbare Griffe
und Abdeckung

Saugschlauch-
Reinigungssystem

Autoklavierbare
Köchereinsätze

Partner von:

BVD

VDDI

Belmont
TAKARA COMPANY EUROPE GMBH

Berner Straße 18 · 60437 Frankfurt am Main
Tel. +49 (0) 69 50 68 78-0 · Fax +49 (0) 69 50 68 78-20
E-Mail: info@takara-belmont.de
Internet: www.belmontdental.de