



Wirtschaftliche Auswirkungen von Cyberangriffen auf Gesundheitsbetriebe

Digitalisierung: Aufgaben in der Praxisführung (1)

Ist mit der Bestimmung eines Datenschutzbeauftragten in der Zahnarztpraxis alles getan? Muss ich mir als niedergelassener Zahnarzt Gedanken über Hardware- und Softwarearchitekturen in der Praxis machen? Bin ich haftbar zu machen, wenn sich eine Beschädigung oder Entwendung von digitalen Patientendaten ereignet? Sind meine Röntgenbilder, Anamnesebögen, Karteikarten und Bonitätsauskünfte der Abrechnungsgesellschaft über Patienten inzwischen digital und entsprechend so gesichert, dass sie rechtlichen Anforderungen genügen?

Das kann Ihnen bestmöglich ein Rechtsanwalt beantworten. Vielleicht ist weniger ein „Fachanwalt für Medizinrecht“ als mehr ein „Fachanwalt für Informationstechnologierecht“ der richtige Ansprechpartner. Es

kursieren im Internet auch Anwälte für „Internet“ oder „Datenschutzrecht“, jedoch soweit die Bundesrechtsanwaltskammer auf ihrer Website informiert (bit.ly/2XHk1O8), müssen Fachanwälte eins der 23 dort angegebenen offiziellen Fachanwaltsgebiete nachweisen und nachfolgende Anforderungen erfüllen: „Ein Rechtsanwalt kann maximal drei Fachanwaltstitel erwerben. Wer eine Fachanwaltsbezeichnung führt, muss jeweils jährlich belegen, dass er sich im vorgeschriebenen Umfang fachlich fortgebildet hat.“

Sollte Ihre Zahnarztpraxis Opfer einer cyberkriminellen Attacke werden, bei der die gesamten Praxispatientendaten entwendet werden, sind möglicherweise alle betroffenen Patienten in Kenntnis zu setzen, da jeder Patient ein Recht darauf hat. Es stellt sich auch die Frage, ob die Praxis für solche Fälle versichert ist. Das wiederum beantwortet Ihnen am besten ein Versicherungsmakler, der sich mit diesen neuen Bedrohungsszenarien in der digitalen Medizin gut auskennt.

Neue Welt der digitalen Medizin

Der Weiterbildungsfokus der vergangenen zehn Jahre betraf oft Themen wie Aufklärung, Dokumentation, Röntgenindikation, Leitlinien der Fachgesellschaften und Behandlungskomplikationen. Parallel musste man den Themenblock der Qualitäts- und Hygienemaßnahmen und die Anbindung an die Telematikinfrastruktur implementieren. Nun kommt auf den niedergelassenen Zahnarzt die nächste Welle in Form der rechtlichen, wirtschaftlichen und organisatorischen Auswirkungen der digitalen Medizin zu.

Ob Arztpraxis oder Krankenhaus – das „Internet of Things (IoT)“ verbindet Computer und Geräte netzwerkartig. Durch „Phishing“ versuchen Hacker, mittels gefälschter E-Mails, Kurznachrichten oder Websites an Daten von Internetnutzern zu gelangen. Ist erst einmal an einem Punkt des Netzwerks ein Angriff erfolgreich etabliert, kann

sukzessive das gesamte System infiziert werden. Neben dem Abgreifen der Datensätze gehört bei den Hackern das Erpressen zum Geschäftsmodell. Es kann natürlich auch ein Cyberangriff sein mit dem Ziel, die Daten einfach zu zerstören. Und dann? Die Folgen sind vielfältig. Die Patienten, die das Recht haben, darüber informiert zu werden, können gegen die Zahnarztpraxis klagen. Die Wiederherstellung der Datensätze ist zeitaufwendig und sehr kostenintensiv, in manchen Fällen bei einer veralteten IT-Architektur fast gar nicht wiederherstellbar, da kann man nur hoffen, noch Papierkarteikarten geführt zu haben. Auch das Praxisimage kann leiden, denn die betroffenen Patienten interpretieren den Datendiebstahl ganz unterschiedlich. Der Schaden durch einen Cyberangriff auf die Datenstruktur der Praxis hat somit wirtschaftliche, rechtliche und marketingbezogene Auswirkungen.

Lösungsansatz durch präventive IT-Strategie

Ein Lösungsansatz ist, die IT-Sicherheit zu einem Punkt mit hohem Prioritätsfaktor in der Praxis zu benennen und entsprechende Maßnahmen zu koordinieren. Die Vorbeugung gegen Cyberangriffe in der Zahnarztpraxis ist ein strategischer Faktor.

Datenschutzverletzungen und Klagen sollen vermieden werden. Dazu gehören neben den stets aktuellsten Versionen der IT-Sicherheitssoftware, die Überprüfung der praxiseigenen IT-Architektur durch einen erfahrenen IT-Spezialisten und die Investition in neue Hardware. Ob das Dentaldepot dafür der richtige Ansprechpartner ist, bleibt vom Einzelfall und dem Angebot abhängig. Auf jeden Fall muss langfristig auch eine Gewährleistung oder Haftung des IT-Dienstleisters besprochen werden, wenn man sich kostenintensiv eine neue IT-Architektur kauft. Meine persönliche Erfahrung ist, dass das mich betreuende Dentaldepot bereits

vor Jahren die Mitarbeiterbasis im Bereich IT und IT-Sicherheit verbreitert hat und fit für die Herausforderungen der Zukunft ist. Um die Investition in moderne Soft- und Hardware wird man als Praxisinhaber nicht herumkommen.

Die digitale Kommunikation mit Patienten, Praxen, Dentallaboratorien oder anderen Organisationen muss immer unter dem Gesichtspunkt der IT-Sicherheit betrachtet werden. Die Kommunikation per Mail mit Patienten könnte gegebenenfalls auf einen separaten Server oder gar ein zweites Netzwerk getrennt verlagert werden.

Ein weiterer Punkt im Maßnahmenkatalog sollte die Schulung des eigenen Personals sein, um „Phishing-Fallen“ zu erkennen und nicht anzuklicken. Zur Mitarbeiterschulung sollte auch das Regeln des Surfens im Internet von Praxiscomputern gehören, denn oft möchte man den Mitarbeitern diesen Service zur Erzielung einer höheren Mitarbeiterzufriedenheit gestatten. Da ist vielleicht die Nutzung des eigenen Smartphones die bessere Alternative, um der Cyberkriminalität auszuweichen. Auch eine begrenzte Zahl der Mitarbeiter mit der Legitimation zum Nutzen aller Computerprogramme muss überdacht werden.

Und schließlich wird man sich auf Seminaren in diesem neuen Wissensfeld fortbilden müssen.

In den nächsten beiden Artikeln zu „Technologie in der Praxis“ wird es etwa um die Strategien von „Online-Terminvergabe-Services“ gehen und wie diese Unternehmen kontinuierlich sukzessive massenweise Daten über Patienten sammeln, den Einfluss telemedizinischer Applikationen im Zuge des demografischen Wandels und der zukünftige Einsatz von Spracherkennung zur Unterstützung der digitalen Dokumentation.

Dr. Dr. Philipp Plugmann, Leverkusen

(wird fortgesetzt)

Über den Autor

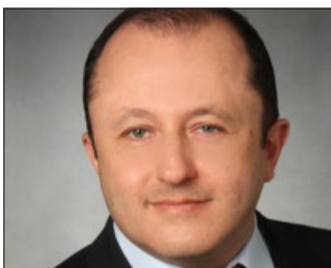


Foto: privat

Dr. med. dent. Dr. scient. med. Philipp Plugmann, MSc, MSc, MBA, Master of Science in Parodontologie und Implantattherapie (DG Paro), ist als Zahnarzt in Leverkusen niedergelassen und befasst sich intensiv mit der Weiterentwicklung der Zahnmedizin aus technologischer Sicht, der Medizintechnik und betriebswirtschaftlichen Aspekten der Berufsausübung. Er ist externer wissenschaftlicher Mitarbeiter der Abteilung für Parodontologie am Universitätsklinikum Marburg und Lehrbeauftragter an der Hochschule Fresenius Köln.

„Such neue Mitarbeiter, such!“

TOPMEDIS STELLENBÖRSE

WWW.TOPMEDIS.DE

dzw