Foto: tostphoto – stock.adobe.com

Das Netzwerk sichern

Erklärungen zur IT-Sicherheitsrichtlinie der KZBV

Die IT-Sicherheitsrichtlinie der KZBV sorgte zum Jahresbeginn für Aufregung – doch diese ist unbegründet.

Zu Beginn des Jahres war die IT-Sicherheitsrichtlinie der KZBV der große „Aufreger" im zahnärztlichen Umfeld. Sofort schossen wieder Online-Seminare wie Pilze aus dem Boden und bei manchen Beratern und Verkäufern einschlägiger Sicherheitstechnik war eine gewisse Goldgräberstimmung nicht zu übersehen.

Dabei beinhaltet die IT-Richtlinie weder etwas Neues noch etwas Spektakuläres. Es war eine lobenswerte und keinesfalls einfache Aufgabe gewesen, für den zahnärztlichen Bereich ein entsprechendes Papier auszuarbeiten. Schließlich sind nicht alle Zahnärztinnen und Zahnärzte „IT-Aficionados". Die KZBV gibt damit – abgestuft in drei Klassen – für kleine, mittlere und große Praxen einen technisch-organisatorischen Rahmen für den sicheren IT-Betrieb vor. Damit steht den Zahnmedizinern und Zahnmedizinerinnen erstmals eine verbindliche Orientierungshilfe zur Verfügung, wie man sie sich in vielen anderen Berufsgruppen derzeit noch wünschen würde.

Foto: Hans Schenkel

Dr. Thomas H. Lenhard ist ein international anerkannter Experte für Informationstechnologie und Datenschutz. Er greift auf seinen umfangreichen Erfahrungsschatz aus drei Jahrzehnten Datenschutz und Datensicherheit zurück und ist u.a. als Datenschutzbeauftragter sowohl für die DGZMK als auch für die DGI umfassend tätig.

Der Titel dieser IT-Sicherheitsrichtlinie lautet eigentlich „Richtlinie nach §75 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit". In der Präambel ist die Intension dieser Richtlinie formuliert: Sie soll technisch-organisatorische Maßnahmen nach Art. 32 DSGVO für die Zahnarztpraxen standardisieren.

Eines darf dabei aber nicht vergessen werden: Es besteht ein grundlegender Unterschied zwischen Datenschutz und Datensicherheit. Die Datensicherheit bezieht sich ausschließlich auf technische und organisatorische Maßnahmen.

Obwohl sich die IT- oder Datensicherheit nicht nur auf den Schutz personenbezogener Daten beschränkt, sondern per Definition alle Daten schützen soll, kann diese im Zusammenhang mit der Richtlinie durchaus als ein Teil des Datenschutzes verstanden werden. Alleine die konsequente Orientierung einer Praxis an der

IT-Sicherheitsrichtlinie ist also kein Garant dafür, dass ein angemessenes Datenschutzniveau in der Zahnarztpraxis sichergestellt ist. Dazu braucht es vielmehr Verhaltensregeln, eine gute Dokumentation und die Einhaltung eines rechtlichen Rahmens in Bezug auf die Verarbeitung von personenbezogenen Daten.

Betrachtet man sich als altgedienter Datenschutzbeauftragter die Anhänge der IT-Sicherheitsrichtlinie, sind diese nachvollziehbar. Wer allerdings über keine ausgesprochene IT-Affinität verfügt, dem dürfte sich kaum der gesamte Hintergrund der zuweilen recht dürftigen Ausführungen erschließen.

Ein Beispiel dafür ist die laufende Nummer 14 aus der Anlage 1 zur IT-Sicherheitsrichtlinie. In dieser wird darauf hingewiesen, dass die Daten in „Endgeräten" regelmäßig gesichert werden sollen. Davon abgesehen, dass sehr häufig auch kleine und mittlere Praxen Server einsetzen und eine zentrale Datenhaltung betreiben, ist die Angabe des Zielobjekts „Endgeräte" etwas missverständlich. Diese eine Zeile repräsentiert demnach das Thema Datensicherung, dem der vorherige Beitrag dieser Serie (ZZI 1/21) gewidmet war und der sich bei genauer Betrachtung als höchst komplex herausstellt. Wie darin zu lesen war, handelt es sich bei der Datensicherung um eine der wichtigsten und elementarsten, wenn nicht sogar um die wichtigste technisch-organisatorische Maßnahme. Dieses Beispiel zeigt, dass es zur Umsetzung der IT-Sicherheitsrichtline der KZBV unter Umständen umfangreicher Erläuterungen der einzelnen Forderungen bedarf.

Drei Zeilen zum Thema Sicherheit. Neben allgemeinen Überlegungen zur IT-Sicherheitsrichtlinie ist es wichtig, sich mit dem Themenbereich Netzwerksicherheit auseinanderzusetzen. In Anhang A der IT-Sicherheitsrichtlinie hat man diesem hochkomplexen Themenbereich immerhin drei Zeilen gewidmet. Diese enthalten drei Forderungen:

- die Absicherung der Netzübergangspunkte,
- die Dokumentation des Netzes und
- die grundlegende Authentisierung, also den Nachweis der Identität, für den Netzmanagement-Zugriff.

Aus Sicht des Datenschutzes reicht es allerdings nicht, sich nur diese drei Punkte anzusehen. Ein wesentlicher Aspekt, der häufig übersehen wird, ist nämlich auch die Betriebssicherheit. Gerade in älteren Praxen ist dieses Problem vielleicht bekannt: Das Netzwerk wurde vor 15 bis 20 Jahren gebaut. Irgendwann wurden neue Rechner angeschafft und das Team hatte den Eindruck, dass alles deutlich schlechter läuft als zuvor.

Das Netzwerk unter der Lupe. Um dies zu verstehen, lohnt es sich, einige grundlegende Aspekte zum Netzwerk in Praxen zu beleuchten. Diese können kabelgebunden oder per WLAN1 aufgebaut werden. Häufig finden sich in Praxen auch hybride Formen, bei denen beide Technologien zum Einsatz kommen. Bei einem kabelbasierten Netzwerk gilt es, zwischen Kupferleitungen und Glasfaserleitungen zu unterscheiden, wobei in den allermeisten Fällen Kupferkabel zum Einsatz kommen.

Um standardisiert über Netzwerke kommunizieren zu können, existiert ein sieben Kommunikationsebenen umfassendes Modell, das sogenannte OSI2-Schichten-Modell. Auf Schicht vier und drei befinden sich dabei die Kommunikationsprotokolle TCP3 und IP4. Die unterste Kommunikationsschicht ist die physikalische Schicht, der man nachsagt, dass sich die Ursachen für Netzwerk- und Verbindungsprobleme dort am häufigsten finden lassen. Dazu muss man wissen, dass Netzwerke mit Hochfrequenztechnologie arbeiten. Diese wiederum ist extrem anfällig, was Störungen angeht – insbesondere dann, wenn die Verlegung von

Kabeln oder der Einbau von Netzwerkkomponenten nicht unter hohen Qualitätsanforderungen erfolgt ist.

Kann ein Netzwerk, das mit einer Frequenz von 10 oder 100 MHz betrieben wird, noch zahlreiche Fehler kompensieren, so stellt der sichere Betrieb von schnelleren Netzwerken, die mit Frequenzen von 250 oder 500 MHz arbeiten, extremste Anforderungen an die Qualität der Verkabelung. Wird an ein relativ altes Netzwerk ein neuer Rechner angeschlossen, kann es vorkommen, dass der Rechner mit dem Server oder einer Netzwerkkomponente eine schnellere Verbindung aushandelt, als das bei dem alten Rechner der Fall war. Bei einem alten Netzwerk können die höheren Übertragungsfrequenzen zu massiven Störungen bis hin zum Verbindungsabriss führen. Der Eindruck, dass neue Rechner langsamer wären, resultiert in Praxen erfahrungsgemäß fast immer aus solchen Netzwerkproblemen.

Qualifizierte Messung nötig. Aus diesem Grund ist es obligatorisch, für Netzwerkleitungen, die in einer Praxis verlegt werden, qualifizierte Messungen entsprechend der EN-50173 durchführen zu lassen. Dies ist vor allem dann wichtig, wenn im Netzwerk auch noch Medizingeräte integriert sind. Manche Hersteller geben sogar eine verlängerte Garantie für Kabel und Komponenten, wenn man die ordnungsgemäße Verlegung und Verbindung neu verbauter Komponenten mittels entsprechender Protokolle nachweist. Hier sind normale Elektriker schnell mit ihrem Latein am Ende, wenn sie lediglich den elektrischen Durchgang der Leitungen messen können und nicht etwa einen NVP5-Wert oder einen Dämpfungswert ermitteln können, um die Qualität eines neu verlegten Netzwerks nachzuweisen. Erst dann, wenn das physikalische Netzwerk fehlerfrei arbeitet, kann man sich mit den weiteren Schichten der Kommunikation befassen.

Die IT-Sicherheitsrichtlinie nennt die Absicherung der Netzwerkübergangspunkte unter der laufenden Nummer 32 der Anlage 1 zur Richtlinie. Diese wird dort in aller Kürze beschrieben: „Der Übergang zu anderen Netzen, insbesondere dem Internet, muss durch eine Firewall geschützt werden."

Leider ist das wirkliche Leben auch in diesem Zusammenhang nicht ganz so einfach, wie der Leser dieser Zeile zunächst glauben mag. In der heutigen Zeit sollte niemand mehr ohne Nutzung einer adäquaten Firewall mit seinem Rechner eine Verbindung zum Internet aufbauen. Schon gar nicht sollte dies geschehen, wenn Gesundheitsdaten verarbeitet werden.

Gehen Sie nie ohne den Schutz einer Firewall ins Internet.

Alleine mit dem Kauf einer teuren Firewall ist es aber nicht getan. Unter Umständen kann es sogar sinnvoller sein, einen Firewall-Router eines Internet-Providers einzusetzen, der regelmäßig und automatisch mit Updates „gefüttert" wird, als eine mehrere tausend Euro teure Firewall zu kaufen, deren Handbuch mehr als 300 Seiten umfasst und deren Konfiguration selbst für altgediente IT-Profis häufig ein Buch mit sieben Siegeln darstellt.

Weniger ist manchmal mehr. Ein Beispiel aus der Datenschutzpraxis zeigt, dass weniger manchmal mehr ist: In einer kritischen Infrastruktur wurde vor einiger Zeit eine neue Firewall durch ein Fachunternehmen in Betrieb genommen. Wenige Wochen später wollte der interne IT-Verantwortliche einen internetbasierten Zugriff auf einen neuen Serverdienst einrichten. Trotz fehlender ausreichender Kenntnisse bezüglich der Funktionsweise von Firewalls gelang es ihm dafür zu sorgen, dass ein Dienst im internen Netzwerk vom Internet aus erreichbar war. Dummerweise ist ihm das deshalb gelungen, weil er „alle Schleusen geöffnet hatte": Er hatte eine Regel definiert, die jeglichen Datenverkehr in alle Richtungen zuließ. Nach diesem Vorfall waren eingedrungene Computer-Viren noch das kleinste Problem des Verantwortlichen.

Firewall korrekt konfigurieren. Das Beispiel zeigt, dass der Einsatz der besten verfügbaren Firewall nutzlos ist, wenn diese nicht korrekt konfiguriert wird. Wenn eine spezielle Firewall eingesetzt werden soll, ist es sinnvoll, auf den Webseiten des Herstellers nachzusehen, welche Vertragspartner sich in der Nähe befinden. Diese sind in aller Regel geschult, die Konfiguration der Firewall dieses Herstellers einzurichten. In keinem Fall sollte man eine Firewall erwerben, wenn die Hotline für den technischen Support nur über eine Nummer im Ausland erreichbar ist oder Handbücher nicht in der Landessprache verfügbar sind.

Ein Praxisnetzwerk ist indes nicht nur gegenüber dem Internet abzusichern. Es ist darauf zu achten, dass ungenutzte Netzwerkdosen in der Praxis, insbesondere auch im Wartebereich, nicht mit dem Netzwerk verbunden sind. Einige Dienstleistungsunternehmen neigen dazu, nach Neuverkabelung einer Praxis, alle vorhandenen Netzwerkdosen an den Netzwerkverteiler anzuschließen. Zuweilen sind auch Netzwerkdosen noch mit dem Netzwerk verbunden, obwohl die Räumlichkeiten irgendwann einer anderen Nutzung zugeführt wurden und die Netzwerkdosen dort daher nicht mehr benötigt werden.

Ebenso wie Zugänge zum Netzwerk zu sichern sind, ist es auch erforderlich, eventuell vorhandene WLAN-Zugänge so zu sichern, dass keine unberechtigten Dritten darüber Zugang zu Ihrem Netzwerk in der Praxis erlangen können. Das Thema WLAN wird in einem der folgenden Artikel separat behandelt.

→ **Thomas H. Lenhard**