Foto: tostphoto – stock.adobe.com

Daten richtig sichern

Technische und organisatorische Maßnahmen zum Datenschutz

Die Datenschutzgrundverordnung, welche nunmehr schon fast drei Jahre in Kraft ist, ist an den Zahnarztpraxen nicht spurlos vorübergegangen. Dokumentationspflichten, Vertraulichkeitsvereinbarungen, Informationspflichten und schließlich die Forderung nach angemessenen technischen und organisatorischen Maßnahmen. Der Datenschutzbeauftragte oder der Datenschutzkoordinator müssen längst neben der Kenntnis von Artikeln und Paragrafen von DSGVO, BDSG und weiteren einschlägigen Gesetzestexten auch umfassende Kenntnisse der Betriebsorganisation, Betriebswirtschaftslehre und der Informationstechnologie mitbringen.

Gerade im letztgenannten Bereich ist die Verwirrung zuweilen besonders groß. Insbesondere wird die Angemessenheit technischer Maßnahmen sehr unterschiedlich dargestellt und interpretiert, je nachdem welche Interessen derjenige vertritt, der eine jeweilige Stellungnahme abgibt. Für den Zahnarzt stellt sich hier dann mitunter die Frage, ob er wirklich grob fahrlässig handelt, wenn er keine viertausend Euro teure Firewall für seine Praxis anschafft. Derjenige, der die entsprechende Hardware vertreibt, wird hier in aller Regel eine andere Auffassung vertreten, als derjenige, der die Rechnung zu zahlen hat, oder derjenige, der als Datenschutzbeauftragter die Angemessenheit technischer und auch organisatorischer Maßnahmen zu bewerten hat.

Mit dem vorliegenden Artikel startet daher eine Reihe, die dem Zahnarzt Informationen zum technischen Datenschutz näherbringt und diesen auch in die Lage versetzen kann, Angebote oder Darstellungen von Anbietern einschlägiger Technik kritisch zu hinterfragen. Während sich die Artikel mit Fragen der Vernichtung von Dokumenten ebenso befassen werden wie mit Cloud-Computing oder dem gerade in jüngster Vergangenheit viel diskutierten Thema „Firewall“, startet die Reihe mit einem Thema, das häufig nur am Ran-

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.

de behandelt wird: die Datensicherung (englisch: Backup).

Solange die IT-Systeme in der Praxis ihren Dienst verrichten und keine außergewöhnlichen Vorfälle eintreten, wird häufig nicht die Vorgehensweise hinsichtlich der Datensicherung hinterfragt. Diese rückt thematisch oftmals erst dann in den Fokus der Betrachtung, wenn darauf zurückgegriffen werden muss. Ein geflügeltes Wort in der Informatik sagt: „Die beste Datensicherung ist die, die niemals gebraucht wird." Das impliziert, dass der Rückgriff auf eine Datensicherung stets die Ultima Ratio aller Maßnahmen sein sollte. Das bedeutet allerdings auch, dass in dem Fall, in dem eine Rücksicherung (engl. restore) unumgänglich ist, alle weiteren Maßnahmen zur Wiederherstellung von Systemen oder Datenbeständen ausgeschöpft sind.

Die Frage, was es für eine Zahnarztpraxis bedeutet, wenn digitale Patientenakten, Befunde und Daten plötzlich nicht mehr zur Verfügung stehen, kann sich jeder Zahnarzt und jede Zahnärztin selbst beantworten. Selbst wenn die Patientenakten noch alle in Papierform vorhanden sind, wird ein Ausfall des Praxisinformationssystems in der Regel nicht zu unterschätzende Probleme bereiten, insbesondere dann, wenn keine funktionsfähige Sicherung bereitsteht, mit der das System wiederhergestellt werden kann.

Die Bedrohung wächst. Zwar wurden Komponenten von IT-Anlagen dahingehend entwickelt, dass normale Defekte merklich seltener auftreten, als das noch vor 25 Jahren der Fall war, jedoch haben auch die Bedrohungen für die Sicherheit von Systemen seit dem massiv zugenommen. So kann man im Jahr 2021 immer noch von einer Ransomware[1]-Plage sprechen, wobei die Angriffe auf Systeme zunehmend professioneller werden.

Zwar werden immer noch Schadprogramme wie gewöhnliche Spam-Mails verschickt, jedoch werden auch E-Mails mit schädlicher Nutzlast zunehmend fallbezogen versendet, indem z.B. im Betreff auf eine konkrete Stellenausschreibung in einer Fachzeitschrift Bezug genommen wird. Klickt dann der Empfänger das vermeintliche Bewerbungsschreiben an, wird das Verschlüsselungsprogramm aktiviert und Datenzerstörung und Erpressung nehmen ihren Lauf.

Wir benötigen demnach nicht nur eine Datensicherung, wenn der Server oder die Praxis ausgebrannt sind, sondern auch bei Wasserschäden, Blitzschlag, Auftreten von Defekten auf Festplatten oder eben auch bei Sabotage oder Schädigung durch Mail- oder Ransomware. Entgegen der Aussage mancher IT-Betreuer und Berater von Praxen wird eine funktionierende Datensicherung nämlich nicht dadurch entbehrlich, dass der Server in der Praxis mit einem RAID-Laufwerk[2] ausgestattet ist und daher die Daten auf dem Server eventuell redundant vorgehalten werden. Aus der Praxis sind Fälle bekannt, in denen ein RAID-Kontroller nicht erkannt hat, dass Speichersegmente auf einer Festplatte defekt waren. Die Spiegelung defekter Segmente hat schließlich dazu geführt, dass die Daten auf der intakten Festplatte ebenfalls zerstört wurden. Ein Spiegellaufwerk erhöht zwar die Ausfallsicherheit eines Servers, ist aber niemals ein Ersatz für eine ordentliche Datensicherung.

> **Die beste Datensicherung ist die, die niemals gebraucht wird.**

Die Daten richtig sichern. Datensicherung ist eine der elementarsten und vermutlich die wichtigste aller technischen Maßnahmen zum Datenschutz. Eine funktionierende Datensicherung kann verhindern, dass ein Vorfall meldepflichtig wird, d.h., der zuständigen Aufsichtsbehörde anzuzeigen ist, oder dass eine Praxis im schlimmsten Fall in eine existenzbedrohende Situation gerät.

Häufig findet im Zusammenhang mit der Inbetriebnahme neuer Praxissoftware überhaupt keine Beratung hinsichtlich der Datensicherung statt, oder es wird nur eine sehr rudimentäre Sicherung im Rahmen der Neuinstallation einer Software eingerichtet. Mitunter laufen dann Datensicherungen scheinbar problemlos über Jahre, und es werden sogar externe Datenträger regelmäßig gewechselt und sicher aufbewahrt, bis sich im Zuge einer Havarie herausstellt, dass die Rücksicherung nicht funktioniert oder zumindest die Datensicherung nicht ohne einen enormen Aufwand verwendet werden kann.

Die folgenden Statements und Fragen sollen daher eine Hilfestellung geben, womit der Zahnarzt/die Zahnärztin selbst prüfen kann, ob hinsichtlich der Datensicherung in der eigenen Praxis ausreichende Maßnahmen getroffen wurden.

1. Es genügt für eine schnelle Wiederherstellung eines Systems nicht, dass der Datenbankinhalt des Praxisinformationssystems gesichert wird.
Soweit ein Praxisinformationssystem ausfällt, sollte es in kurzer Zeit wiederhergestellt werden können. Dazu wird aber einiges mehr benötigt als nur eine Sicherung des Datenbankinhalts:

- kompatible Hardware (soweit ein Ersatzgerät erforderlich ist)
- Grundinstallation, bestehend aus Betriebssystem, Anwendungssoftware und Datenbankmanagementsystem
- Sicherung des Datenbankinhalts
- ggf. Sicherung auf Dateiebene (Doc, PDF, Scans etc.)
- Dokumentation der Konfiguration (z.B. Einbindung ins Netzwerk).

2. Soweit die Hardware im Havariefall ersetzt werden soll, muss darauf geachtet werden, dass bei Bedarf auch ein kompatibles Ersatzgerät zur Verfügung steht.
In der jüngsten Vergangenheit waren zeitgleich drei Betriebssysteme des Herstellers Microsoft parallel verfügbar. Allerdings wurden zu diesem Zeitpunkt bereits Rechner verkauft, die nur noch mit dem neuesten dieser Betriebssysteme (Windows 10) kompatibel waren. In dem Fall ist die Rücksicherung von Rechnern mit Windows 7 oder Windows 8 regelmäßig auf einer entsprechenden Hardware gescheitert.

3. Die Datensicherung muss ebenso wie die Rücksicherung und die Aufbewahrung von Sicherungen geplant werden.
Es braucht dazu ein Datensicherungskonzept, welches obligatorisch für jede Infrastruktur ist, die eine Sicherung erfordert. Das Datensicherungskonzept enthält nicht nur eine detaillierte Beschreibung, was zu welchem Zeitpunkt gesichert wird, sondern gibt auch Aufschluss darüber, wie lange eine Sicherung aufbewahrt wird, wo die Sicherung verfügbar ist und wie die Sicherung im Bedarfsfall korrekt eingesetzt wird, um ein System wiederherzustellen.

4. Vorsicht vor Virtualisierungslösungen!
Zwar ist es in der Theorie einfach, virtuelle Rechner auf eine andere Hardware umzuziehen, zu sichern oder diese wiederherzustellen. Es sollte dabei aber beachtet werden, dass unterschiedliche Hersteller zwar gleiche Dateiendungen für die virtuellen Rechner oder deren virtuelle Datenträger nutzen, dadurch aber nur der Anschein einer oftmals nicht gegebenen Kompatibilität erweckt wird.

5. Datensicherungen sollen regelmäßig überprüft und getestet werden.
Insbesondere sollte in vertretbaren Zeitabständen ein Totalausfall simuliert werden, bei dem aus den Datensicherungen das Praxissystem wiederhergestellt wird. Das geschieht natürlich auf separaten Rechnern und niemals testweise auf den Echtsystemen einer Praxis.

6. Datensicherungen sollen an einem sicheren Ort verwahrt werden.
Bricht in der Praxis ein Feuer aus, werden i.d.R. neben den Rechnern auch die dort gelagerten Datensicherungen vernichtet. Demnach ist es sinnvoll, sowohl Datensicherungen für den schnellen Zugriff in der Praxis vorzuhalten, als auch Sicherungsmedien an einem sicheren externen Platz zu lagern.

7. Das Sicherungsmedium (z.B. NAS[3]) sollte keinesfalls permanent mit einem Rechner oder Server verbunden sein.
Soweit der Datenbestand eines Rechners durch Schadsoftware verschlüsselt wird, werden in aller Regel auch verbundene Laufwerke mit verschlüsselt. Soweit sich die Datensicherungen dann auf diesem Laufwerk befinden, sind diese für eine Rücksicherung des Systems unbrauchbar.

Sollten Sie eine oder mehrere Fragen aus dem Infokasten mit Nein beantworten, sollten Sie Rücksprache mit dem IT-Betreuer Ihrer Praxis halten oder – soweit vorhanden – Ihren Datenschutzbeauftragten zu diesem Thema konsultieren.

Häufig zeigen sich Ansätze für Verbesserungen erst dann, wenn ein Rücksicherungstest durchgeführt wird. Dabei kommt es dann schon mal vor, dass Boot-Disketten einer Sicherungssoftware veraltet und nicht mehr zur aktuellen Datensicherung kompatibel sind oder ein rückgesicherter Rechner nicht mehr startet. Daher wird dringend empfohlen, in der Praxis einen Rücksicherungstest durchzuführen oder durchführen zu lassen, damit technische Probleme im Zusammenhang mit der Datensicherung behoben werden können, bevor sie zum Problem für Ihre Praxis werden. Beachten Sie aber dabei, dass Rücksicherungstests niemals auf dem Echtsystem durchgeführt werden, sondern üblicherweise separate Testrechner dabei zum Einsatz kommen.

Die Möglichkeiten, Daten auch in Online-Archiven, Rechenzentren oder sogenannten Clouds zu speichern, wird in einem der nächsten Artikel behandelt.

⟶ Thomas H. Lenhard

CHECKLISTE FÜR IHREN DATENSCHUTZ

- Verfügt meine Praxis über ein dokumentiertes Datensicherungs- und Rücksicherungskonzept?
- Ist im Fall einer Beschädigung des Servers/Systems eine kompatible Hardware oder eine sonst vertretbare Lösung zur Einspielung der Datensicherung verfügbar?
- Sind alle aktuellen Datenträger und Installationsprogramme an einem sicheren Ort verfügbar, falls eine Wiederherstellung des Praxisinformationssystems erforderlich werden sollte?
- Werden die Daten so oft gesichert, dass die Zeitspanne zwischen letzter erfolgter Sicherung und Systemausfall mit überschaubarem Aufwand datentechnisch nachgepflegt werden kann?
- Sind sowohl Image- wie auch Dateisicherungen vorhanden?
- Werden die Sicherungsdaten offline an einem sicheren Ort verwahrt?
- Hat in der Vergangenheit bereits ein Rücksicherungstest des Praxisinformationssystems stattgefunden, oder sind derartige Tests für die Zukunft geplant?
- Werden die Datensicherungen regelmäßig getestet?

[1] Ransomware – Erpressersoftware, die häufig Datenbestände verschlüsselt
[2] RAID – Redundant Array of Independent Disks; eine Zusammenschluss mehrerer Festplatten, bei denen u.a. eine erhöhte Ausfallsicherheit durch redundante Datenhaltung oder Spiegelung erreicht werden kann.
[3] NAS – Network Attached Storage