Sieben **Tricks**, wie Sie Ihre Daten schützen

Sicher gesichert? Viren, Würmer und Trojaner: **Praxis-Computer** müssen sensible Patientendaten vor vielen Gefahren bewahren. Im Qualitätsmanagement gibt es dazu einige Grundregeln, die Hausärzten helfen, ihre Daten richtig zu sichern.

Katja Sperling
AQUA – Institut für angewandte Qualitätsförderung und Forschung im Gesundheitswesen, Göttingen

Computerviren machen vor Arztpraxen nicht halt. Aber auch defekte Bauteile innerhalb der IT können in einer Praxis zu Problemen führen. Um sich möglichst umfassend gegen Viren und computerrelevante Ausfälle zu schützen, sollten Ärzte einen versierten IT-Dienstleister hinzuziehen. Angebote zur IT-Beratung gibt es sehr viele und den passenden Anbieter zu finden, kann herausfordernd sein. Daher hilft es, wenn die Praxis Vorgaben zu den Inhalten der gewünschten Beratung macht und die erwarteten Leistungen klar umreißt. Nachfolgende Hinweise beschreiben, wie ein IT-Dienstleister eine Praxis gezielt bei der Datensicherheit unterstützen kann und worauf bei der Sicherheit von Praxisdaten geachtet werden sollte.

Zentrale Frage: Wie lange kann die Praxis einen Ausfall der IT verkraften?

① Umfang des Ausfallschutzes

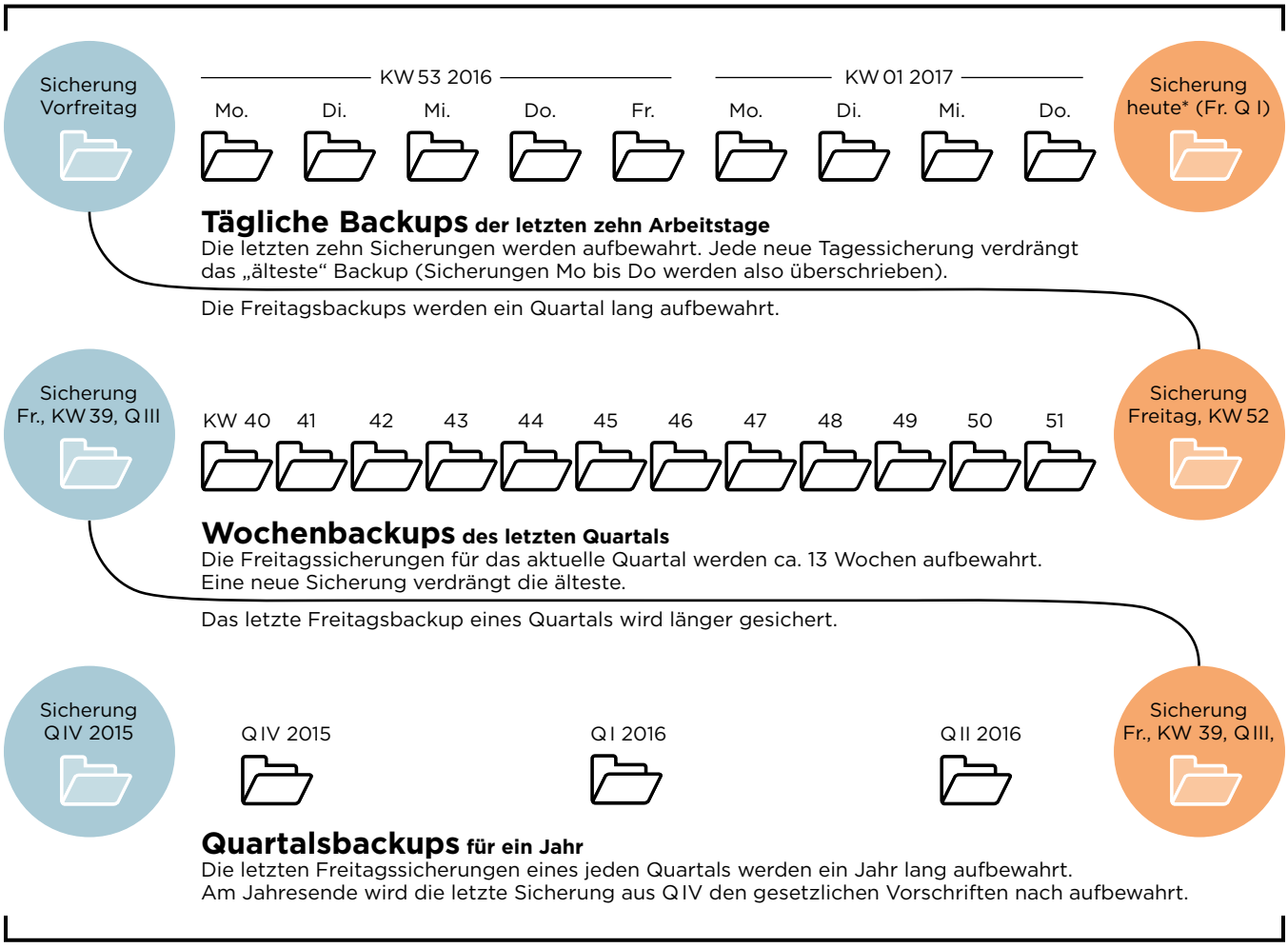
Am Anfang sollte die Frage stehen: Wie lang kann die Praxis im Notfall ohne einen PC oder das IT-Netzwerk auskommen? Die Antwort bestimmt, wie umfassend und somit teuer der gewünschte IT-Service sein wird.

Checkliste IT-Ausfall:

- Wie lange kommen wir ohne PC oder medizinische Geräte aus?
- Welche (medizinischen) Geräte sind neben dem PC beim Ausfall betroffen die am IT-Netzwerk angebunden sind?
- Welche Kosten verursacht ein Ausfall?
- Wie können Ausfälle abgesichert werden?
- Geht es evtl. kurze Zeit ohne den PC/Gerät? Was kostet das?
- Halten sich Kosten und Schutz die Waage?

Fotos: lucadp - Fotolia

Abb. 1: Beispiel für ein Backup-Konzept



** heute ist Freitagnacht in KW 1, der ersten Januarwoche 2017, Anfang Q I*

Die KV Bremen hat eine **Übersicht der Aufbewahrungsfristen** erstellt: http://hausarzt.link/UGypg

Diese Fragen sollte der in der Praxis für die IT-Verantwortliche so lange durchlaufen, bis sich die Kosten für die Lösung und der Schutzbedarf die Waage halten. Ein Beispiel: Wenn ein Röntgengerät ausfällt, kann dies eine Hausarztpraxis womöglich eine Woche lang verkraften. Funktioniert das komplette IT-System nicht mehr, können vier Stunden allerdings schon zu lang sein.

Die von der Praxis bestimmte maximale Ausfallzeit sollte mit dem IT-Dienstleister in einem **Service-Level-Agreement** (SLA) vertraglich festgelegt werden. Dort werden insbesondere die Reaktions- und Reparaturzeiten bestimmt und wie schnell, wenn nötig, Ersatzteile geliefert werden.

② Sichere Strukturen

Rechner, auf denen sensible personenbezogene Daten gespeichert sind, dies schließt Patientendaten ein, unterliegen besonderen Sicherheitsanforderungen. Verfügt eine Praxis über ein **Netzwerk**, so sollte die zentrale Datenbank und auch die weiteren Daten auf einem **IT-Server** liegen, der im Idealfall in einem abschließbaren Raum hinreichend gegen Einbruch geschützt ist. Hardware wird im laufenden Betrieb warm, so dass der Raum ausreichend gekühlt werden sollte.

Der zentrale Server sollte kein normaler PC, sondern ein eigens hierfür hergestelltes Gerät sein. Serverhardware ist für den Dauerbetrieb konzeptioniert und verfügt über dafür ausgelegte Bauteile, die in üblichen PCs nicht

zu finden ist. In einem Server sind zum Beispiel zwei oder mehr Festplatten verbaut, die parallel mit den identischen Informationen beschrieben werden. Fällt eine dieser Festplatten aus, kann mit der zweiten Festplatte normal weitergearbeitet werden. Auch andere Bauteile sind mehrfach vorhanden, so dass diese insgesamt stabilere Konstruktion das Risiko für einen Systemausfall deutlich senkt.

Die Struktur eines IT-Netzwerks kann verschieden aussehen. Die einfachste Struktur verbindet mehrere PCs miteinander, wobei auf jedem PC die Praxissoftware installiert ist und die Daten auf einer gemeinsam genutzten Datenbank abgelegt werden.
Eine höhere Sicherheit und Stabilität wird erreicht, wenn man einen **Terminalserver** benutzt. Bei dieser IT-Struktur werden die PCs mit einem zentralen Rechner verbunden, auf dem sowohl die Praxissoftware als auch alle Daten hinterlegt sind. Die PCs am jeweiligen Arbeitsplatz dienen dabei vereinfacht gesagt nur als Tastatur und Bildschirm. Fällt ein PC aus, kann er relativ schnell ersetzt werden, weil keine neue Software installiert und eingerichtet werden muss.
Ein Terminalserver muss besondere Anforderungen erfüllen, wie etwa eine automatische Benachrichtigung bei Hardwareproblemen, regelmäßige Updates und aktuell gehaltene Anti-Virus-Programme.

③ Sicherung von Daten

IT-Daten können aus verschiedenen Gründen verloren gehen. Neben Viren und Trojanern können auch versehentlich gelöschte Daten zu Problemen führen. Eine automatische Datensicherung (Backup) ist daher sehr empfehlenswert. Welchen Umfang diese Datensicherung hat, muss jede Praxis individuell für sich festlegen.

Fragen zur Datensicherung:
- Wie lange muss auf welche Daten zugegriffen werden können?
- Welche Daten müssen wie oft auf externe Medien kopiert werden?
- Wie lange müssen diese aufbewahrt werden?

Datenbanken können täglich oder auch mehrmals am Tag gesichert werden. Alle weiteren Daten, die nicht in einer Datenbank hinterlegt sind, können getrennt davon und in einem anderen Rhythmus gesichert werden.
Ein auf den ersten Blick komplizierteres, dafür aber **sichereres Konzept**: Das Backup erfolgt täglich und die Sicherungsmedien, in der Regel eine Festplatte oder ein USB-Stick, werden zwei Wochen getrennt vom eigentlichen Rechner aufbewahrt. Anschließend werden die Sicherungen von Montag bis Donnerstag überschrieben und die Freitags-Sicherung wird ein Quartal aufbewahrt. Nach einem Jahr werden die Sicherungsmedien von Quartal I bis III überschrieben und das Medium vom vierten Quartal wird entsprechend der gesetzlichen Frist aufbewahrt (s. Abb. 1).

Die Mindestaufbewahrungsfristen variieren je nach Dokumentnart.

Die Mindestaufbewahrungsfristen variieren je nach Dokumentenart und reichen meist von einem Jahr (z. B. AU-Bescheinigungen) bis zehn Jahre (z. B. Untersuchungsbefunde). Die KV Bremen hat dazu eine Übersicht erstellt (s. Linktipp). Zivilrechtliche Schadenersatzansprüche verjähren allerdings erst nach 30 Jahren, so dass es ratsam ist, Dokumente so lange aufzubewah-

ren, bis sicher ist, dass kein Schadenersatz mehr geltend gemacht werden kann.

④ Speichermedium

Es reicht nicht, sich nur darüber Gedanken zu machen, was wie oft gespeichert werden sollte, sondern auch worauf. Es gibt unterschiedliche Speichermedien wie CD, USB-Stick oder Datenband (Streamer). Bei jedem Speichermedium besteht die Gefahr, dass die Daten aufgrund der physikalischen Beschaffenheit auch ohne Einwirkung von außen verloren gehen können.
Wer eine alte Musikkassette nach vielen Jahren wieder abspielt kennt den Effekt: Die Musik klingt längst nicht mehr so klar wie am Tag der Aufnahme. Ähnlich kann es auch bei den relativ neuen Speichermedien gehen. Jedes Medium hat Vor- und Nachteile und sollte entsprechend gelagert werden. Diesen Punkt sollten Hausärzte mit dem IT-Dienstleister thematisieren und im Datensicherungskonzept festhalten.
Und: Datensicherung nützt nur, wenn die Sicherungsmedien nicht in Gefahr sind. Es empfiehlt sich, die **Sicherungsmedien räumlich getrennt** von den eigentlichen Rechnern aufzubewahren. Denn brennt es etwa im Serverraum, verbrennen die Sicherungen gleich mit.

⑤ Antivirus, Updates, Firewall

Ein **Antivirus-Programm** auf jedem Rechner ist Pflicht und hinlänglich bekannt. Neben den Gefahren aus dem Internet droht aber eine oft unterschätzte Quelle: Die Nutzer schließen zum Beispiel einen USB-Stick an, um Fotos aus dem Urlaub zu zeigen, oder eine CD wird eingelegt, auf der sich Musik befindet, die aus dem Internet geladen wurde. Auch auf diesem Weg kann Schadsoftware in ein System gelangen.
Praxisfremde Hardware sollte deshalb generell nicht angeschlossen werden. Zusätzlich sollte über die Antivirus-Software festgelegt werden, welche Dateiformate überhaupt ins System gelassen werden. Sich selbst ausführenden Exe-Dateien (Endung: .exe) kann so ein Riegel vorgeschoben werden.
Um am Internet angeschlossene Computer gegen einen Zugriff von außen zu schützen, sollte eine entsprechende **Firewall** installiert sein, die solche Zugriffe verhindert. Sie bildet einen Schutz zwischen dem Internet und dem lokalen System. Es gibt zwar Firewalls, die im Rechner integriert sind, diese allein reichen für eine Arztpraxis aber nicht. Der Schutz, den ein normaler DSL-Router gewährt, ist ebenfalls nicht stark genug, auch wenn in der Konfiguration des DSL-Routers „Firewall – aktiviert" steht.
Besser und deutlich sicherer ist es, eine Firewall mit einem Proxy einzurichten. Proxys sind eine Art Schutzschirm, der die Daten filtert und prüft, bevor sie tatsächlich ins IT-System gelangen.
Das Betriebssystem und jede andere Software sollte immer aktuell gehalten werden. Spielen Sie daher alle **Updates** der Softwarehersteller zeitnah nach deren Erscheinen ein. Es gibt Umfragen unter Sicherheitsfachleuten, die das für wichtiger halten als eine Antivirus-Software.

⑥ Mitarbeiter sensibilisieren

Letztendlich nützt die beste IT-Sicherheit aber wenig, wenn das Praxisteam nicht im Sinne der IT-Sicherheit denkt und diese im Alltag mitträgt. Häufig entstehen Schäden, weil im Praxisalltag etwas getan wird, dessen Reichweite dem Einzelnen nicht bewusst ist oder Schnelligkeit vor Sicherheit geht. Die IT-Nutzer müssen die Sicherheitsrisiken kennen und helfen, diese zu vermeiden. So kann eine Schulung für das Thema sensibilisieren.

⑦ Langfristig und wiederkehrend

Ein IT-Sicherheitskonzept gehört in regelmäßigen Abständen auf die Tagesordnung. Etwa einmal im Jahr sollte sich eine Praxis mit ihrer IT beschäftigen und notwendige Veränderungen prüfen oder hinterfragen, ob das bisherige Konzept weiter sinnvoll ist.

DAS EUROPÄISCHE PRAXISASSESSMENT

Das Europäische Praxisassessment (EPA) ist ein umfassendes Qualitätsmanagementsystem, das auf Qualitätsindikatoren basiert und die Perspektive von Patienten, Ärzten und Mitarbeitern der Praxen einbezieht. Über die Benchmarking-Software VISOTOOL® haben Arztpraxen die Möglichkeit, sich anonym miteinander zu vergleichen. Insgesamt haben rund 2.000 Hausarztpraxen an EPA teilgenommen.

- 98 Prozent der EPA-Hausarztpraxen sichern ihre Daten täglich
- 98 Prozent der EPA-Hausarztpraxen haben alle am Internet angeschlossenen Computer durch eine Antiviren-Software geschützt
- 92 Prozent der EPA-Hausarztpraxen aktualisieren ihre Antiviren-Software automatisch und täglich
- 97 Prozent der EPA-Hausarztpraxen schützen alle am Internet angeschlossenen Computer durch eine Firewall