Tipps und Tricks zum Datenhandling

Tobias Bauer

Einleitung

Wenn man heutzutage über Datenverwaltung und -sicherheit spricht, denkt man unwillkürlich an Nachrichten von Datendiebstählen bei großen Online-Unternehmen wie Yahoo, Telekom, Dropbox oder dem Deutschen Bundestag. Das Wort „Datensicherheit" wird verbunden mit Begriffen wie „Internet" oder „Online". Im Zusammenhang mit der eigenen Zahnarztpraxis spielt die besondere Schutzwürdigkeit der Patientenakten und ein möglicher Missbrauch dieser Daten durch Angriffe über das Internet eine große Rolle. Tatsächlich jedoch liegt das größte Risiko für die digitalen Praxisdaten in ihrem Verlust durch unbeabsichtigtes Löschen, Verschlüsselungstrojanern, defekten Festplatten, alternden Archivierungsdatenträgern oder dem physischen Diebstahl der EDV Geräte (wobei es die Diebe meist auf die Geräte an sich – weniger auf die Daten selbst abgesehen haben).

Dieser Artikel soll Ihnen helfen, gemeinsam mit Ihrem IT Dienstleister ein langfristig tragfähiges Konzept zur IT Infrastruktur und Datensicherheit zu entwickeln und so Ihre IT Systeme zu einem effizienten und nützlichen Teil Ihres Praxisworkflows zu machen.

Die richtige Infrastruktur für Ihren Bedarf

Ohne PC geht es praktisch in keiner Praxis mehr. Spätestens wenn es um digitale Bildgebung mit intraoralen Röntgenbildern mittels Speicherfolienscanner oder Sensoren geht, digitale Panoramaschichtaufnahmen oder 3D-Röntgen, ist ein IT Netzwerk in der Praxis notwendig.

Bei der Planung dieser Infrastruktur werden meiner Erfahrung nach gerne der wirkliche Bedarf und die Auswirkungen mancher Entscheidungen auf die tägliche Praxis übersehen. Lassen Sie mich dies anhand eines Beispiels erläutern:

Eine Praxis hat bislang mit Film geröntgt und nur die Patientenakte in einem Abrechnungsprogramm digital geführt. Dazu gibt es einen „Hauptrechner" mit einer Desktop Windows Version an der Rezeption und in den drei Zimmern PCs, die nicht über eine Netzwerkverkabelung, sondern über das sichere WLAN des Internetrouters mit dem Hauptrechner verbunden sind. Die PCs sind drei Jahre alt. Die tägliche Datensicherung wird zum Arbeitsende mit der Verwaltungssoftware durchgeführt und auf einer externen Festplatte gespeichert. Nach der ca. zehn Minuten dauernden Datensicherung wird die externe Festplatte in einen feuerfesten Safe gelegt und alle PCs in der Praxis ausgeschaltet.

Die Praxis möchte nun auf digitales Röntgen inkl. 3D-DVT umsteigen. Bis auf einen neu anzuschaffenden, leistungsfähigen PC im Röntgenraum, erfüllen im Prinzip alle PCs die technischen Anforderungen der neuen Röntgensoftware.

Bei einer oberflächlichen Analyse der Gegebenheiten in der Praxis könnte man sagen, dass lediglich ein neuer Röntgen-PC (mit Befundungsmonitor) gekauft werden muss. Schaut man jedoch genauer hin, erkennt man einiges, auf das der Anbieter das Praxisteam hinweisen sollte.

- WLAN Verbindungen sind in der Regel langsamer als kabelgebundene Netzwerkverbindungen. Aktuell haben WLAN Netze meist 300 Mbit während Kabelnetze bei 1 Gbit (1000 Mbit) liegen. Dauert das Öffnen eines Röntgenbildes mit kabelgebundenem Netz zwei Sekunden, so sind es mit WLAN evtl. schon 5 - 6 Sekunden. Das klingt zunächst nicht viel, spätestens bei 3D-Daten (ca. 100 MB) macht es mehrere Sekunden bis Minuten mehr Wartezeit aus. Das ganze System fühlt sich langsamer an und stört evtl. den Praxisworkflow. Rechnet man die Anzahl der Bilder, die täglich angeschaut werden, zusammen, kann sich der Aufwand Kabel zu legen durchaus lohnen.

- Die Datensicherung digitaler Röntgendaten dauert deutlich länger, als die Sicherung der reinen Abrechnungsdaten. Eine manuelle Sicherung ist nicht mehr praktikabel, und es sollte auf eine automatische Sicherung umgestellt werden. Der „Hauptrechner" muss also über Nacht an und die externe Platte dauerhaft verbunden bleiben. Da ein Desktop PC nicht für Dauerbetrieb ausgelegt ist (Festplatten, Netzteil, Lüftung), empfiehlt es sich spätestens jetzt, einen echten Server anzuschaffen. Dieser sollte über ein Notstromsystem, eine sogenannte unterbrechungsfreie Stromversorgung (USV) verfügen.

- Die dauerhaft mit dem System verbundene externe Festplatte stellt in zweierlei Hinsicht ein Risiko dar. Zum einen kann ein Verschlüsselungstrojaner oder Virus sowohl die Hauptdaten, als auch die Datensicherung befallen und unbrauchbar machen, zum anderen wäre die Festplatte im Falle eines Brandes oder eines Einbruchs ebenfalls betroffen. Das Sicherungskonzept muss hier überdacht und z. B. durch eine zweite externe Festplatte, die mit der anderen im Wechsel in den feuerfesten Safe gelegt wird oder ein Online-Back-up ergänzt werden (siehe dazu später den Abschnitt Sicherungskonzepte).

Das Beispiel verdeutlicht, dass ein für einen bestimmten Zweck geplantes IT System – in diesem Fall die Verwendung des Abrechnungsprogramms – für andere Ansprüche nicht mehr geeignet sein kann, selbst wenn die verwendeten Komponenten an sich ausreichend wären.

Die beschriebene Lösung kann für eine Praxis mit Abrechnungsprogramm und reinem 2D-Röntgen durchaus ausreichen. Die Hardware des Hauptrechners sollte dazu aber auf Dauerbetrieb ausgelegt sein und mit einem geeigneten Serverbetriebssystem betrieben werden. Ich empfehle aber auch bei kleinen Netzwerken immer einen dedizierten Server, der nicht als Arbeitsplatz genutzt wird. Für eine reine Betrachtung der Röntgenbilder in den Behandlungsräumen wäre auch eine iPad-Lösung denkbar. Ein PC im Röntgenraum ist nicht unbedingt notwendig (zumindest nicht bei 2D-Systemen). Wie oben beschrieben erfordert die Integration von 3D-Systemen einen etwas höheren Aufwand und sollte aufgrund der Datenmengen nicht kabellos erfolgen, auch wenn man WLAN Geräte – z. B. ein Notebook oder Tablet – gerne kombinieren kann.

Neben der digitalen Bildgebung sollte auch an andere Geräte in der Praxis gedacht werden, die in Zukunft ebenfalls Daten über das Netzwerk austauschen. Dazu gehören die Behandlungseinheiten,

Sterilisatoren oder neue diagnostische Systeme wie z. B. die KaVo DIAGNOcam. Abbildung 1 zeigt eine typische IT-Umgebung einer digitalisierten Praxis. Bei der Netzwerkverkabelung muss man daher auf Flexibilität achten und sollte nicht an der Anzahl der Netzwerkdosen in den Räumen sparen. Nicht jede Dose muss direkt an das Netzwerk angeschlossen werden. Dies kann bedarfsgerecht am sogenannten „Patchfeld" erfolgen, bei dem die Dose wahlweise mit einem Netzwerkverteiler oder mit der Telefonanlage verbunden wird.

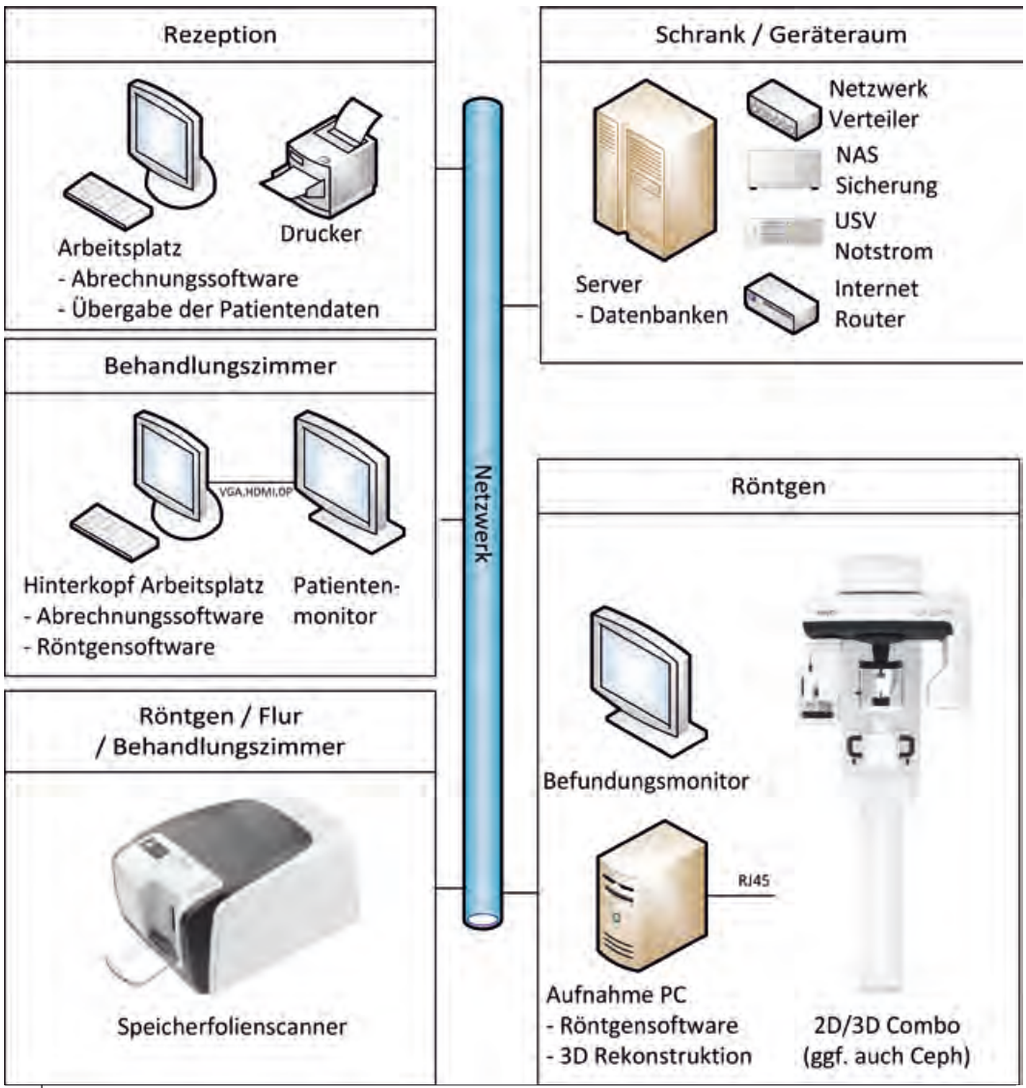

Abb. 1: Typisches IT-Netzwerk in einer digitalisierten Praxis

Kompatibilität und Schnittstellen – Systeme verschiedener Hersteller miteinander verbinden

Entscheidet man sich dafür, digitale Systeme in die Praxis zu integrieren, kommt es unweigerlich zu der Frage, ob die jeweils besten Systeme miteinander kombiniert werden können. Nicht in jedem Fall kann ein Hersteller alle gewünschten Systeme als integriertes System anbieten. Oft ist dies auch absichtlich nicht gewünscht, um sich nicht komplett von einem Anbieter abhängig zu machen („Apple Effekt").

Die Lösung beschreibt ein Schlagwort sehr gut: „Schnittstellenstandards". Standards werden sowohl auf internationaler Ebene, als auch innerhalb Deutschlands entwickelt. Die wichtigsten Standards in Bezug auf dentale Bildgebung sind:

DICOM (international, DICOM = Digital Imaging and Communication in Medicine)
Praktisch jedes Bildprogramm kann DICOM Daten inkl. Patienteninformationen manuell als Dateien im- und exportieren. Manche Systeme unterstützen auch eine automatische Netzwerkübertragung von oder zu einem entsprechenden Speichersystem (PACS - Picture Archiving and Communication System). Ab 01.01.2020 gilt auch für Zahnarztpraxen die Verpflichtung, Röntgenbilder im DICOM Format zu archivieren. Daher werden PACS Systeme vermehrt zum Einsatz kommen, da sie herstellerunabhängig von allen Systemen Daten entgegennehmen und auch übertragen können. KaVo liefert z. B. bei den 3D-Geräten ein solches PACS- System mit.

VDDS-Media (national, VDDS = Verband der deutschen Dentalsoftwarehersteller)
Die VDDS-Media Schnittstelle ermöglicht die Übergabe von Patientendaten und Bildern. Das Verwaltungsprogramm übergibt den Patienten an das Bildprogramm und kann von diesem auch die Bilder abrufen. Praktisch alle Abrechnungs- und fast alle dentalen Bildprogramme unterstützen VDDS-Media. Manche Programme unterstützen beide Richtungen gleichzeitig (z. B. KaVo Conexio, Dampsoft DSWin) und können auch zwischen anderen Systemen vermitteln.

JPG (oder JPEG), PNG, TIF (Bildformate)
Auch wenn diese Bildformate gerne zum Bildaustausch genutzt werden, sind sie eigentlich für Röntgenbilder ungeeignet, da es hier keine standardisierte Möglichkeit gibt, Metadaten wie den Patientennamen, die Aufnahmeparameter etc. zu übermitteln. Zudem ist das JPG-Format für Farbbilder optimiert und kann röntgenrelevante Graustufen nur reduziert darstellen (ein JPG kann nur 256 Graustufen darstellen, aktuelle Röntgensysteme erzeugen jedoch bis zu 65536 Graustufen). Das TIF-Format an sich ist geeignet – die Dateien sind nur recht groß und Metadaten müssen auf anderem Weg übermittelt werden.

TWAIN (das Wort ist tatsächlich keine Abkürzung, sondern eine Erfindung der Entwickler)
Dieser recht alte Standard kann für die Anbindung von 2D bildgebenden Systemen an fast jede Software genutzt werden (selbst Microsoft Word kann über TWAIN Bilder einbinden).

STL (Stereo-Lithographie oder auch Standard Tesselation Language)
Dieser Quasi-Standard ist ein Datenformat, das sich bei CAD / CAM Systemen (intraorale 3D-Scanner, virtuelle WaxUps, „Backward-Planning") etabliert hat. In Zukunft wird dieses Format wahrscheinlich in den DICOM-Standard integriert werden.

UVC (USB Video Class)
Für aktuelle Kamerasysteme, die über USB mit einem PC / Mac verbunden sind, eignet sich dieser Standard optimal, da hier keinerlei spezielle Treiber mehr installiert werden müssen. Ältere Kamerasysteme nutzen noch WDM (Windows Driver Model), WIA (Windows Image Acquisition) oder sogar den sehr alten VfW (Video for Windows) Standard, der meist bei aktuellen PCs mit Windows nicht mehr funktioniert.

TCP / IP (Transmission Control Protocol / Internet Protocol)
Diesen Standard für Netzwerkverbindungen, TCP / IP, gibt es in der Version 4 und Version 6, wobei die meisten Geräte und Internetprovider noch immer die ältere Version 4 nutzen. Die meisten Geräte (Dentaleinheiten, Sterilisatoren etc.) werden direkt über TCP / IP entweder Wireless (WLAN, meist 300 – 600 MBit) oder über Kabel (Cat5 / 6 / 7 meist 100 Mbit – 10 Gbit) angebunden. Außer bei Videokameras, die auch den Strom über USB beziehen, sollten Sie darauf achten, dass Geräte mit eigener Stromversorgung über TCP / IP angebunden werden, da dieser Standard die größte Flexibilität in der Aufstellung der Geräte und Softwareunterstützung bietet.

PDF bzw. PDF / A (Portable Document Format / Archiv)
Für die Langzeitarchivierung von Dokumenten wurde PDF / A standardisiert, so dass sichergestellt ist, dass diese Dokumente auch in 10 Jahren noch gelesen werden können.

Bei der Produktauswahl sollte darauf geachtet werden, ob es sich um sogenannte „offene" oder „geschlossene" Standards handelt. Manche Hersteller nutzen zwar die Standards, markieren aber die Daten so, dass andere diese entweder nicht nutzen können, oder dass sie selber nur Daten lesen können, die von ihren Systemen erstellt wurden. Die Empfehlung: Achten Sie auf offene Standards.

Die Datensicherung – oft unzureichend geplant und dokumentiert

Inzwischen ist jedem bewusst, dass eine Datensicherung sinnvoll ist. Da meist aber der IT Dienstleister die Sicherung eingerichtet hat, können viele Praxisinhaber folgende Fragen nicht beantworten. Testen Sie selbst:

- Bis zu welchem Datum in der Vergangenheit kann ich den Zustand meiner Praxisabrechnung / Röntgendaten wiederherstellen? Diese Frage kann relevant sein, wenn ein Fehler nicht sofort bemerkt wird und ggf. eine fehlende Datei oder Information erst später bemerkt wird.)
- Wie stelle ich Daten bei einem nicht mehr startenden Server / Arbeitsstation wieder her?
- Was mache ich, wenn jemand die Praxis EDV gestohlen hat oder diese beschädigt ist?

Wenn die Antwort auf diese Fragen „dann rufe ich mein Systemhaus an“ lautet, sollten Sie Ihr Sicherungskonzept überdenken. Denn gemäß „Murphys Law“ ist Ihr Systemhaus im Fall der Fälle vielleicht gerade nicht erreichbar oder kann nicht sofort helfen.

Die Datensicherung sollte daher abgestuft erfolgen und die eigenen Mitarbeiter sollten je nach Stufe selbstständig Maßnahmen einleiten können, um ein Problem zu beheben.

Stufe 1: Daten redundant halten

Inzwischen ist es üblich, in ein Serversystem redundante „Hot-Swap“ Festplatten einzubauen. Das bedeutet, dass die Daten mindestens auf zwei oder auch mehr Festplatten verteilt abgelegt werden und eine defekte Festplatte bei laufendem Betrieb ausgetauscht werden kann, wobei das System dann automatisch die Daten wiederherstellt. So schützt man sich am besten vor einem Hardwareausfall. Wichtig ist hier aber, dass dies keinen Schutz vor Veränderungen oder Löschen der Daten bietet – dafür sind echte Sicherungen notwendig.

Stufe 2: gelöschte / veränderte Dateien oder Daten in einfach strukturierten Programmen

Seit Windows 7 bietet Microsoft ohne Zusatzprogramme in Windows die Funktion „Dateiversionsverlauf“ an. Damit sichert das System in einstellbaren Zeitabständen (sogar halbstündlich) den Zustand definierter Verzeichnisse auf einer Festplatte. In der einfachen Konfiguration wird dazu ein Speicherbereich auf derselben Festplatte reserviert – es können aber auch andere lokale Speicher oder Netzwerklaufwerke ausgewählt werden. Die Funktion sollte am Server für die Partitionen aktiviert werden, auf denen die Praxisdokumente liegen. Zusätzlich kann es auch sinnvoll sein, sie für Partitionen mit Anwendungsprogrammen (z. B. dem Abrechnungsprogramm) zu aktivieren.

Die Zeittiefe, die wiederhergestellt werden kann, variiert dabei abhängig von der Größe des reservierten Bereichs und der Menge an Änderungen (es werden Dateiunterschiede gespeichert). Die Wiederherstellung einer gelöschten Datei oder eines ganzen Verzeichnisses ist dabei sehr einfach und kann von jedem Mitarbeiter leicht ausgeführt werden. Manche Programme sind so einfach aufgebaut, dass ihr Datenbestand über diese Funktion auch sehr einfach auf einen Zeitpunkt in der Vergangenheit zurückgestellt werden kann. Dabei kann man sogar leicht zwischen zwei Zeitzuständen hin und herspringen.

Stufe 3: Wiederherstellungssicherungen von Arbeitsstationen und Servern

Auch hier reichen im Prinzip Windows eigene Programme, die in Verbindung mit einem startbaren Datenträger (USB Stick oder DVD) die Wiederherstellung eines PCs ermöglichen. In Verbindung mit dem Dateiversionsverlauf lässt sich so auch eine defekte Festplatte in relativ kurzer Zeit wiederherstellen. Da auf einer Arbeitsstation meist keine aktuellen Daten enthalten sind (in der Annahme, dass alle Dokumente und die Datenbanken der Programme auf dem Server liegen), reichen hier Wiederherstellungssicherungen in wöchentlichen oder ggf. monatlichen Abständen (durch Windows-Updates werden auch diese Systeme ständig verändert). Bei einem Server sollte dies täglich erfolgen.

Wichtig bei der Systemplanung ist hier, dass die großen Datenmengen (meist 2D- und 3D-Bilddaten) von den Systemdaten getrennt gehalten werden – z. B. liegt das Windows System auf der Partition C:\ der Festplatte und die Bilddaten auf der Partition D: \. Die Systemsicherung bleibt so relativ klein und kann über Nacht durchgeführt werden.

Stufe 4: Archivierung und Sicherung der Praxis- und digitalen Bilddaten

Die meisten Verwaltungsprogramme nutzen nur eine relativ geringe Datenmenge von unter 5 GB. Je nach Praxis kann die Datenmenge der Röntgenbilder mit oder ohne 3D-Daten aber leicht über 50 (bei reinen 2D-Daten häufig zu sehen) oder sogar 2000 GB (bei Praxen mit 3D-Daten nach einigen

Nacera®

ceraMotion®

ceraMotion® One Touch Concept.

Foto: © Christian Ferrari®

Mit **Nacera®*** und **ceraMotion®** verbinden sich zwei starke Marken zu einem einzigartigen Produktspektrum für alle Indikationen und Verarbeitungstechniken zur Herstellung von vollkeramischen Versorgungen aus Zirkonoxid. Sie sind individuell zugeschnitten auf die Bedürfnisse und Anforderungen des Anwenders.

Genießen Sie 2017 spannende ceraMotion® Momente...
Hamburg 27. April 2017 I **Dortmund** 11. Mai 2017
Nürnberg 29. Juni 2017 I **Wien** 19. Oktober 2017
› Mehr Infos: Telefon +49 72 31 / 803 - 470 I kurse@dentaurum.com

* Nacera® ist eine eingetragene Marke der DOCERAM Medical Ceramics GmbH.

DENTAURUM

Turnstr. 31 I 75228 Ispringen I Germany I Telefon +49 72 31 / 803 - 0 I Fax +49 72 31 / 803 - 295
www.dentaurum.com I info@dentaurum.com

Abb. 2: Systeme, die Bilder liefern, die bei einer Beratung zum Einsatz kommen

Jahren) ansteigen. Der reine Festplattenplatz für die laufende Praxis ist bei diesen Datenmengen kein Problem – eine 4 TB (= 4000 GB) Festplatte liegt preislich unter 200,- € und reicht somit mehrere Jahre. Die Datensicherung und Archivierung wird bei diesen Datenmengen aber aus zwei Gründen schwieriger:

1) Um einem nicht sofort bemerkten Datenverlust zuvor zu kommen, werden oft mehrere Sicherungen angelegt, so dass man ggf. eine Woche, einen Monat oder sogar ein Jahr zurückgehen kann. Bei einer täglichen Vollsicherung bewegen sich die Datenmengen aber schnell in einer Größenordnung, die nur mit speziellen und teuren Speichersystemen zu bewältigen ist.

2) Sichert man – wie oft üblich – die Daten über ein Netzwerk auf ein spezielles Sicherungssystem („NAS" - Network Attached Storage) und hat ein normales 1 GBit (100 MB / Sek.) Netzwerk, dauert die Sicherung von 1000 GB bei optimalen Bedingungen mindestens 2,5 Stunden. Oft erreichen die Systeme aber „nur" 50 MB / Sek. und brauchen entsprechend länger. Zusammen mit Fotos, dem Abrechnungsprogramm, den Briefen und anderen Dokumenten kann es passieren, dass die Sicherung länger dauert, als Zeit zwischen Arbeitsende und –anfang zur Verfügung steht. Läuft die Sicherung noch, ist das System meist so belastet, dass man nicht normal arbeiten kann (eine Sicherung im laufenden System ist dank der Windows Funktion „ShadowCopy" inzwischen kein Problem mehr).

Um dieser Problematik Herr zu werden, setzt man differentielle oder inkrementelle Backups ein. Dabei wird in beiden Fällen zunächst eine Vollsicherung gemacht (z. B. wöchentlich). Dann werden nur noch die Änderungen zu der letzten Vollsicherung gesichert. Beim differentiellen Backup werden dabei jedes Mal alle Änderungen zur letzten Vollsicherung gespeichert, beim inkrementellen Backup werden immer nur die Änderungen zur letzten Sicherung an sich gespeichert.

Beispiel: Vollsicherung 1 TB am Sonntag; Änderungen pro Tag jeweils 1 GB: die differentielle Sicherung wächst jeden Tag um 1 GB, sodass am Samstag 5 GB gesichert werden, während die inkrementelle Sicherung jeden Tag nur 1 GB sichert. Um eine solche Sicherung wieder einzuspielen, muss

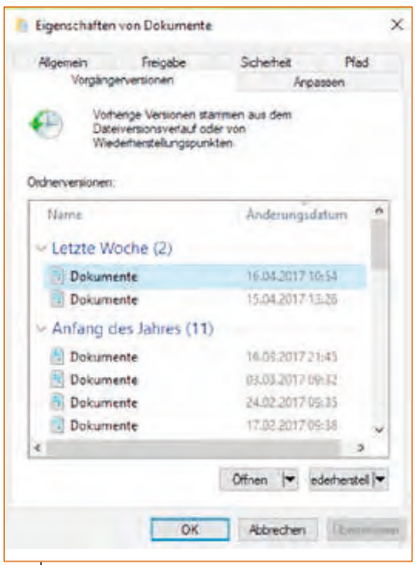

Abb. 3: Dateiversionsverlauf in Windows

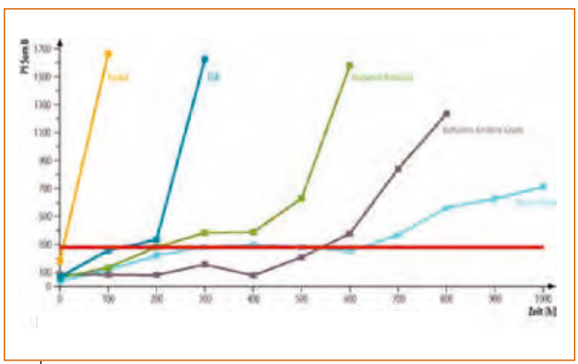

Abb. 4: Fehlerrate bei verschiedenen DVD Marken

zunächst die Vollsicherung und dann entweder das letzte differenzielle Backup oder nacheinander alle inkrementellen Backups bis zum letzten wiederhergestellt werden.

Stufe 5: Kontrolle der Sicherungs- und Archivierungsmedien und der Sicherungsprotokolle

Nicht selten habe ich persönlich erlebt, dass eine Praxis über ihren IT-Dienstleister eine automatische Sicherung eingerichtet bekam, diese aber nicht geprüft wurde. Das Programm dokumentierte jeden Tag einen Fehler im Sicherungsprotokoll, jedoch wurde dieses nie angeschaut. Stellen Sie sicher, dass alle Fehler bei Sicherungsvorgängen auch für das Praxispersonal klar erkennbar sind. Dies kann über eine automatische E-Mail, SMS oder auch ein Warnhinweis am Rezeptions-PC (bitte nicht am Server – da schaut niemand hin) erfolgen.

Sollten Sie eine Archivsicherung einsetzen, die Daten auf Langzeitmedien wie z. B. Bänder, DVDs oder Blue-Ray-Discs auslagert, so sollten auch die alten, beschriebenen Medien in regelmäßigen Abständen überprüft werden. Bei einer Archivierung, die die Originaldaten entfernt (auslagern älterer Daten) ist anzuraten, diese auf zwei Medien zu verschieben (z. B. eine Festplatte und eine DVD). In Abbildung 4 sehen Sie die Fehlerrate von DVDs, die Hitze ausgesetzt waren – über der roten Linie waren die Daten unbrauchbar. Die Kurven stehen für unterschiedliche Hersteller und Qualitäten der DVD Medien.

Stufe 7: Entkoppeln der Sicherungsmedien vom Netzwerk

Verschlüsselungstrojaner sind Programme, die alle verfügbaren Daten verschlüsseln und den Anwender dann auffordern einen Geldbetrag zu überweisen um die Daten wieder zugänglich zu machen. Solch ein Programm kann Ihr Netzwerk befallen, wenn Sie ohne aktuellen Virenschutz Software aus dem Internet ausführen oder auch Software von einer DVD oder einem USB-Stick starten, die Ihnen ein Patient übergibt (z. B. eine DVD mit 3D-DVT Daten aus einer anderen Praxis, die Sie nicht in Ihre 3D-Software importieren können, sondern das Betrachtungsprogramm der DVD nutzen müssen).
Im schlimmsten Fall starten Sie diese Schadsoftware als Super-User Ihres Netzwerks und es werden sowohl die aktuellen Daten, als auch alle angeschlossenen Sicherungsmedien befallen.

Am besten ist es, wenn Sie täglich das Medium der Stufe 3 und 4 wechseln (z. B. über zwei externe Festplatten), so dass zumindest der Vortag nicht befallen werden kann.

Tobias Bauer

Tobias Bauer ist seit über 20 Jahren in der dentalen Industrie tätig. Seit 2003 ist er bei KaVo in verschiedenen Positionen für die Entwicklung von Software und digtalen Lösungen verantwortlich. Als Produktmanager für digitale Workflow Integration verbindet er nun die einzelnen Entwicklungsbereiche, um integrierte Systemlösungen zu schaffen.

Fazit

Eine gute Dokumentation der Maßnahmen zur Sicherungsprüfung bei Datenverlust oder Hardwaredefekt ist oberstes Gebot. Im Prinzip sollte jeder Mitarbeiter der Praxis oder auch beliebige externe Dienstleister mithilfe der Dokumentation die Sicherung jeder Stufe wieder einspielen können. Dabei hilft z. B. auch ein versiegelter Umschlag mit den ggf. notwendigen Kennwörtern, um im Ernstfall nicht auf einen bestimmten Dienstleister angewiesen zu sein.

Achten Sie auch darauf, dass die Sicherungen bei eingesetzter Kompression ebenfalls in Standardformaten (z. B. ZIP, RAR, CAB) bzw. unkomprimiert im Originalformat gespeichert werden, damit Sie nicht von einer spezifischen Sicherungssoftware abhängig sind. Es ist nicht selten passiert, dass der PC mit der Sicherungssoftware aufgrund eines Defektes nicht mehr nutzbar war und man die Sicherungen nicht mehr einspielen konnte, weil kein Installationsprogramm dieser speziellen Software für den neuen PC mehr vorhanden war bzw. die Lizenz dieser Software verlegt wurde und dadurch die Sicherungen nicht mehr zugänglich waren.

Kommunikation mit Kollegen – Austausch medizinischer Daten

Manchmal möchte man Patientendaten – Röntgenbilder oder auch andere Befunde – mit Kollegen teilen und besprechen. Der Datenaustausch geschieht häufig per E-Mail und die Daten werden dabei unverschlüsselt (z. B. als JPG) angehängt. Sofern der E-Mail Transport nicht über einen besonderen, speziell gesicherten Dienstleister erfolgt, ist dieser Weg in Deutschland unzulässig (Gmail oder GMX sind keine Dienstleister dieser Art). Als Datenformat für Bilder sollten Sie, wenn möglich, DICOM nutzen. Für Dokumente eignet sich das PDF bzw. PDF / A.

Es gibt etliche Gesetze und Verordnungen, die die elektronische Kommunikation für medizinische Daten regeln (EU Richtlinien 95/46/EG, 2002/58/EG, Bundesdatenschutzgesetz, Länderverfassungen) und unter bestimmten Bedingungen erlauben.

Generell kann man sagen:

Bei elektronischem Austausch müssen die schutzwürdigen Daten verschlüsselt werden. Nur der gewählte Empfänger darf die Daten lesen können = der Schlüssel muss auf anderem Weg ausgetauscht werden und für jeden Empfänger unterschiedlich sein.

Ein einfacher Weg dies zu erreichen ist es, die Daten in einer mit einem Kennwort verschlüsselten Archivdatei zusammenzupacken (z. B. mit dem kostenlosen Programm 7-Zip), das Kennwort über Fax, Telefon oder gesonderte E-Mail an eine andere Adresse zu übertragen und das Archiv dann per E-Mail (wenn die Datei nicht größer als 10 MB ist) oder über z. B. MagentaCloud (Anbieter Telekom, Server gesichert in Deutschland) zu übertragen. Es gibt auch einige spezialisierte Anbieter für sichere, medizinische Datenübertragung (z. B. DocCopy oder Transfer.Net).

Zum Abschluss

Wie bei einem Hausbau benötigt die richtige IT-Infrastruktur auch eine genaue Planung und Dokumentation. Viele dentale Fachhändler haben eigene IT-Spezialisten oder arbeiten mit Systemhäusern zusammen, die die besonderen medizinischen und dentalen Anforderungen kennen. Normalen IT-Dienstleistern fehlt oft das Wissen über die speziellen Bedürfnisse, Bestimmungen und Schnittstellen. Zudem gewähren viele Hersteller nur trainierten und zertifizierten Technikern Zugang zu allen Dokumentationen und stehen diesen auch über Hotline und speziellen Internet-Portalen zur Verfügung. Die Digitalisierung einer Praxis bringt immense Vorteile und Möglichkeiten. Richtig geplant und umgesetzt, ausführlich geschult und dokumentiert können Sie diese Vorteile beruhigt nutzen. Es wird immer irgendetwas passieren, aber mit der richtigen Vorbereitung lassen sich diese Probleme schneller und sicherer lösen. Ihr IT-System wird einem regelmäßigen Wandel unterliegen – wird dieser schon von Beginn an eingeplant, gibt es später kein böses Erwachen.

Kontakt:

Tobias Bauer
Senior Product Manager
Digital Workflow Integration
KaVo Biberach, BU-Imaging, 1st Floor
Telefon: +49 7351 56 1792