Michael Reinke

IT-Verfügbarkeit in der zahnärztlichen Praxis

Indizes

Datensicherung, Informationstechnik (IT), IT-Systemausfall, Hochverfügbarkeit, Röntgenverordnung, kontinuierlicher Praxisbetrieb

Zusammenfassung

Eine kontinuierliche Verfügbarkeit der in der zahnärztlichen Praxis vorhandenen Informationstechnik ist nicht nur aus wirtschaftlichen, sondern auch aus datenschutzrechtlichen Gründen erforderlich. In dem Beitrag werden Ursachen von praxisrelevanten Systemausfällen, die Konsequenzen hieraus sowie Strategien zur Steigerung der Gesamtverfügbarkeit beschrieben.

Michael Reinke
Dipl.-Ing. (TU)

Erlenweg 9
64665 Alsbach
E-Mail: firstcontact@rswe.com

Einleitung

Mit der zunehmenden Digitalisierung von Patientenakten, bildgebenden Modalitäten und weiteren Daten gewinnt die Informationstechnik (IT) eine steigende Bedeutung in der zahnärztlichen Praxis. Wichtige Patienten- und Bildinformationen können in der Regel nur auf elektronischem Weg erreicht werden. Systemausfälle und somit nicht verfügbare Daten sind kaum zu tolerieren und haben auch negative Auswirkungen auf zu erfüllende Anforderungen im Bereich der Datensicherheit und -integrität[4,5].

Nachfolgend werden auf der Basis einer allgemeinen Analyse sowohl Ansätze zur Steigerung der IT-Verfügbarkeit als auch wirtschaftliche Aspekte für den Praxisalltag vorgestellt.

IT in der zahnärztlichen Praxis

Die Abbildung 1 zeigt eine typische IT-Landschaft mit multiplen digitalen Modalitäten. Von den einzelnen Arbeitsplätzen aus sind die für den Praxisalltag notwendigen Anwendungen erreichbar, u. a.

- Praxisverwaltungssoftware (PVS),
- bildverwaltende Anwendungen (BVS),
- Implantatplanung und

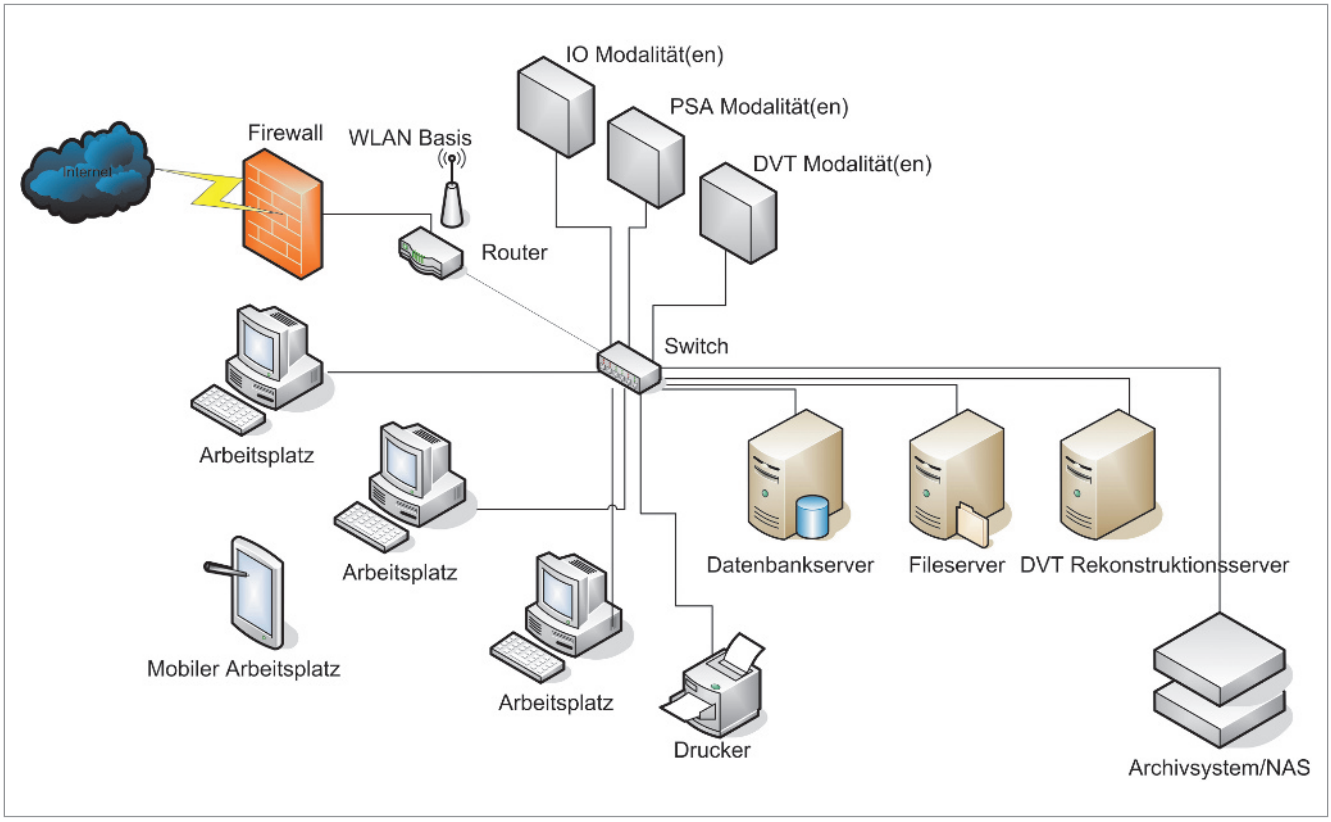

Abb. 1 Schematische Darstellung eines typischen Praxisnetzwerks mit multiplen digitalen Modalitäten und sternförmiger Vernetzung

- Rekonstruktionsanwendungen der digitalen Volumentomographie (DVT).

Sowohl die Datenhaltung als auch zentrale Abläufe und Anwendungen werden auf netzwerkverfügbaren Servern realisiert. Mit einem Router ist das Praxisnetzwerk an das Internet gekoppelt. Dieser Router stellt sehr häufig auch die Funkbasisstation für ein WLAN (Wireless Local Area Network) dar. Über diese Basis können drahtlose, mobile Arbeitsplätze (Tablets, Smartphones etc.) in das Praxisnetzwerk integriert werden. Die Vernetzung aller Komponenten findet über einen oder mehrere so genannte Switches in Sterntopologie statt.

Gründe für die Nichtverfügbarkeit der Praxis-IT

Die Definition der Nichtverfügbarkeit bzw. des Ausfalls im Zusammenhang mit IT-Systemen variiert in der Literatur und in den Produktbroschüren entsprechender Lösungsanbieter sehr stark. In unserer Betrachtung gehen wir von folgender, praxisorientierter Annahme aus: Wenn ein Anwender die gestellte Aufgabe (digitale Röntgenaufnahme, Abrechnung, Planungen etc.) nicht im gewünschten Zeitraum erledigen kann, ist das für diese Aufgaben notwendige IT-System nicht verfügbar, und es liegt ein Systemausfall vor. Für den Anwender ist hierbei nur die Ende-zu-Ende-Verfügbarkeit aller Komponenten auf der benötigten Kette von Einzelsystemen relevant.

Die Ursachen eines Ausfalls sind vielfältig und können in die im Folgenden näher beschriebenen Klassen eingeteilt werden (Abb. 2).

Hardwareausfälle

An diese Ursache denkt man in der Regel zuerst, da in einem solchen Szenario meist ein Großteil der Praxis-IT betroffen ist. Der Ausfall eines Netzwerkswitches legt sehr oft das komplette Praxisnetzwerk lahm. Prominente Kandidaten in dieser Kategorie sind ebenfalls Netzteile und PC-Lüfter. Ein defektes Servernetzteil bringt alle auf diesem PC installierten Serverdienste zum Stillstand.

Softwareausfälle

Diese Ursache tritt in der Praxis erheblich öfter auf. Hierunter fallen u. a.

- Applikationsabstürze und -blockaden („Hänger"),
- Anwendungsprobleme bei ausgeschöpften Systemressourcen, z. B. bei zu wenig verfügbarem Systemspeicher,
- Datenbankfehler,
- fehlerhafte Software, etwa nach Anwendungs- oder Betriebssystemaktualisierungen, sowie
- Ausfälle nach Virusbefall.

Bedienfehler

Einen nicht unwesentlichen Anteil von Systemausfällen haben die Anwender selbst zu verantworten. Ein versehentliches Anhalten benötigter Serverdienste oder irrtümlich wiederhergestellte Datenbanken mit nicht geprüften Backup-Datenbeständen kann dazu führen, dass die Praxis-IT nicht verfügbar ist. Dies betrifft nicht nur die Gruppe der Administratoren, sondern oft auch die Praxisanwender selbst. So kann z. B. das Fehlen eines an einem Server abgezogenen Lizenz-Kopierschutzsteckers (Dongle), der über das Wochenende am Notebook gebraucht wurde, zu Wochenbeginn in der Praxis weitreichende Probleme zur Folge haben.

Geplante Ausfälle

Eine oft übersehene, aber ebenfalls in Frage kommende Ausfallursache sind geplante Aktivitäten, die zur Unterbrechung der Systemverfügbarkeit führen. Hierzu gehören z. B.

- Softwareaktualisierungen von Serveranwendungen,
- Betriebssystemaktualisierungen,
- Austausch von Serverhardware und
- Festplattenergänzungen im Serverumfeld.

Meist sind diese Ausfälle aufgrund ihrer Planbarkeit tolerabel. In bestimmten Umgebungen (z. B. Kliniken)

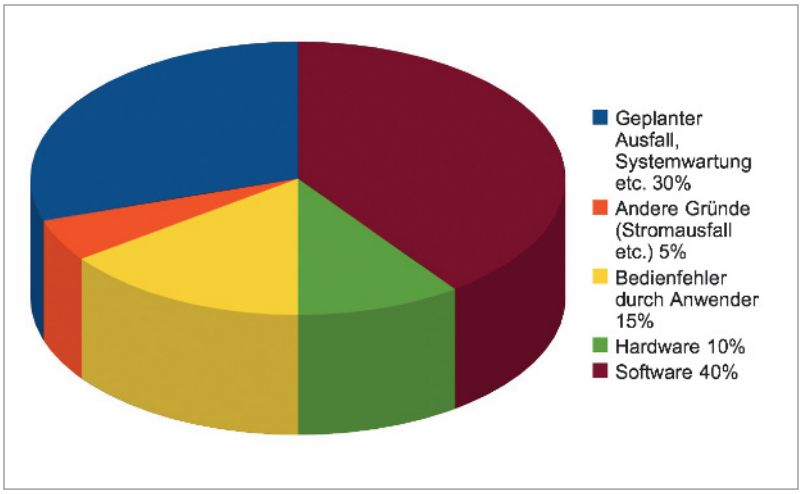

Abb. 2 Klassifikation von IT-Ausfallursachen (Gartner Group 2000). 75 % aller Fälle treten ungeplant auf und können den IT-abhängigen Praxisablauf empfindlich unterbrechen

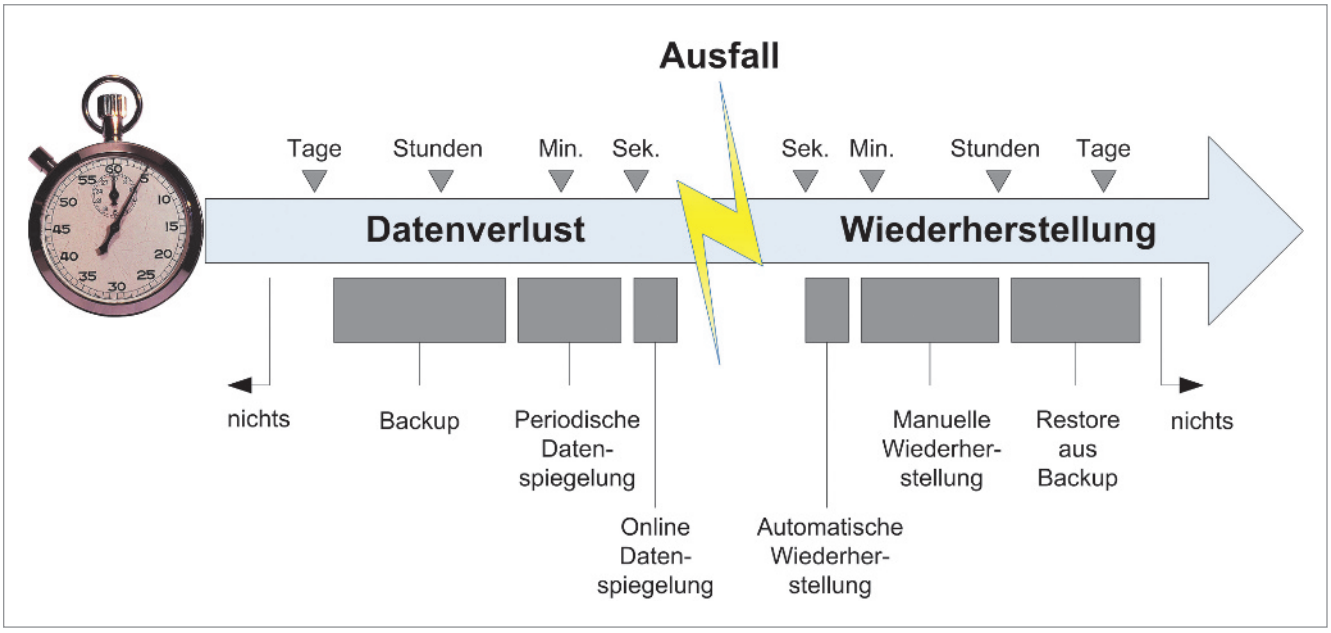

Abb. 3 Zeitlicher Ablauf eines IT-Systemausfalls[1]. Bei fehlender, zeitnaher Datensicherung kann ein unwiederbringlicher Datenverlust eintreten. Die Wiederherstellungsphase nach dem Ausfall lässt sich durch Maßnahmen zur Verfügbarkeitssteigerung erheblich verkürzen. Somit können auch die wirtschaftlichen Auswirkungen eines IT-Systemausfalls reduziert werden

ist es möglich, durch eine entsprechende Verfügbarkeitsgestaltung des IT-Systems auch in diesen Zeitperioden mit dem normalen Betrieb fortzufahren, während gleichzeitig Wartungsarbeiten durchgeführt werden.

Sonstige Gründe

Die restlichen Ausfallursachen sind in der Praxisumgebung zu suchen. Stromausfälle kommen in Deutschland glücklicherweise relativ selten vor. Feuer- und Wasserschäden zählen ebenfalls in diese Kategorie und sollten zumindest bei der Datensicherung[4] an einem praxisexternen Ort berücksichtigt werden.

Lebenszyklus eines Totalausfalls

Abbildung 3 stellt einen einfachen Zeitablauf eines Ausfalls dar. Die Ursache des Ausfalls, in der Regel das Versagen einer kritischen Komponente, spielt bei unserer Betrachtung eine untergeordnete Rolle, da eine Störung des Gesamtsystems vorliegt und z. B. kein Zugriff auf digitale Röntgenbilder möglich ist. In unserem Beispiel gehen wir vom Verlust einer Datenbank oder des entsprechenden Servers aus.

Der Ausfallzeitpunkt teilt diesen Lebenszyklus in zwei Hälften: Rechts des Ausfallzeitpunktes beginnen die Maßnahmen zur Wiederherstellung des Gesamtsystems, und auf der linken Seite werden mögliche Datenverluste im Zeitraum vor dem Ausfall betrachtet.

Die Wiederherstellungsphase ist geprägt von verschiedenen Strategien und Techniken zur Minimierung dieser Zeitspanne. Im Fall des beschriebenen Datenbankausfalls muss nach Wiederbeschaffung aller betroffenen Hardwarekomponenten das zuletzt angefertigte Backup eingespielt werden. Wenn kein Backup vorhanden ist, kann das System nicht komplett wiederhergestellt werden, und es liegen dann ggf. erhebliche Verstöße gegen geltende Datenschutzrichtlinien[4] vor.

Eine Verkürzung der Wiederherstellungszeit kann durch eine laufend gepflegte Kopie des Datenbankservers inklusive Hardware realisiert werden. In diesem Fall ist es meist nur erforderlich, Konfigurationen umzustellen und das System erneut in Betrieb zu nehmen.

Die absolut kürzeste Ausfallzeit kann durch eine automatische Wiederherstellung erreicht werden. Hierbei erfolgt die Bereitstellung eines „Standbysystems" mit gültigem Datenbestand vollautomatisch. Eine Notifikation via E-Mail informiert über den Ausnahmezustand und erlaubt eine entspannte Planung der Reparatur des ausgefallen Systems.

Je nach implementierter Datensicherungsstrategie liegt bei einem Systemausfall ein Datenverlust vor. Alle im laufenden Betrieb eingegebenen bzw. erstellten Daten sind zwar korrekt im primären Datenbanksystem abgelegt, aber noch nicht via Backup gesichert. Mit Eintritt des Ausfalls gehen daher auch alle ungesicherten Daten verloren. Bei einem täglich angefertigten, manuellen Backup erstreckt sich der Verlust auf erhebliche Datenmengen. Eine automatische Spiegelung relevanter Datenbestände minimiert diesen Verlust wirkungsvoll.

Die optimale Lösung besteht in der laufenden Online-Datenspiegelung auf das erwähnte Standbysystem. Die potenzielle Datenverlustspanne kann so auf wenige Sekunden verkürzt werden, und in der Praxis gehen meist keine Daten verloren.

Kosten der Nichtverfügbarkeit

Die Ermittlung entstehender Kosten bei einem IT-Systemausfall ist nur praxisindividuell durchführbar und umfasst neben klar ersichtlichen direkten eine große Anzahl indirekter Kosten. Man spricht in diesem Zusammenhang auch von der Feststellung der „realen" Kosten eines nicht verfügbaren IT-Systems.

Direkte Kosten

Zunächst fallen hierunter alle Kosten zur Wiederherstellung eines laufenden Systems, konkret:

- Arbeitskosten eigener oder externer Servicetechniker;
- Beschaffung von Ersatzkomponenten für defekte Teile (Server-Hardware, Netzwerkkomponenten, Festplatten etc.);
- Beschaffung ggf. nicht (mehr) vorhandener Softwareinstallationen;
- geringere Produktivität des Praxispersonals. So ist die papierbezogene Datenerfassung und Dokumentation (als Ersatz für die PC-gestützte Variante) zeitintensiver. Zusätzlich müssen die so erfassten Daten nach Systemwiederherstellung erneut eingepflegt werden. Alle Daten werden ergo zweimal in die Hand genommen. Dieser Kostenanteil steigt proportional mit der Dauer des Systemausfalls.
- Entgangene Umsätze im Bereich bildgebender Modalitäten. Dieser Kostenfaktor kann recht genau beziffert werden und steigt ebenso proportional mit der Ausfalldauer.

Indirekte Kosten

Im Bereich dieser Kostenposition sammeln sich

- alle Kosten im Zusammenhang mit der Rekonstruktion des Altdatenbestandes. Liegen keine gültigen oder vollständigen Datensicherungen vor, so müssen diese Daten sehr aufwändig aus alternativen Quellen rekonstruiert werden, sofern dies dann überhaupt noch möglich ist. Der korrespondierende Zeitbedarf ist nur sehr schwer schätzbar und die daraus resultierende Zeit bis zur Wiederherstellung entsprechend unsicher.
- Kosten im Zusammenhang mit nicht vorhandenen, digitalen Diagnosedaten. So kann z. B. aufgrund nicht verfügbarer DVT-Systeme auch keine auf diesen Daten basierende Implantatplanung etc. durchgeführt werden.
- Nicht erstellbare oder dem Zugriff entzogene digitale Daten haben auch negative Einflüsse auf die Terminplanung. Existierende Patiententermine müssen reorganisiert werden oder fallen komplett weg. Diese Außenwirkung hat im Extremfall auch

negative Auswirkungen auf die Praxisreputation und auf die Motivation des Praxisteams.
- Aufgrund eines durch den Systemausfall bedingten Datenverlustes (vgl. Abschnitt „Lebenszyklus eines Totalausfalls") und somit nicht vorhandener Bild- und Befundungsdaten kann im Fall einer juristischen Auseinandersetzung von einer fehlenden Beweislage ausgegangen werden. Dies hat Konsequenzen für etwaige Schuldklärungen und Schadenersatzpflichten.

Strategien zur Steigerung der IT-Verfügbarkeit

Keine „Single points of failure"

Ein „Single point of failure" (SPOF[1,3]) ist eine Einzelkomponente (Hardware, Software und andere), die bei Störungen oder Defekten einen Ausfall des benötigten Systems begründet. Eine in der Zahnarztpraxis oft vorgefundene Situation ist die zentrale Vernetzung über einen einzigen Switch (vgl. Abb.1). Ein Ausfall dieser Komponente legt das komplette IT-System lahm. Ein baugleicher Ersatzswitch in den eigenen Praxisräumen ist nicht nur billig, sondern auch leicht auszutauschen.

Im Bereich eingesetzter PC-Serversysteme ist der Redundanzgedanke bereits innerhalb des PC-Servers durch den Einsatz multipler Lüfter, Netzteile, Festplatten (RAID) und Netzwerkkarten realisiert. Auf der Ebene zentraler Serveranwendungen kann eine Ausfallsicherheit durch die Einführung von parallel laufenden Ersatzservern (Standbyserver PC) erreicht werden. Dieser Ansatz hat ebenso den Vorteil, dass bislang nicht redundant verfügbare Komponenten (z. B. die Hauptplatine im PC-Server) ausfallsicher gedoppelt werden. Bei baugleichen Servern mit kompletter Duplikation der Hardware- und Softwarekomponenten spricht man dann von Shared-Nothing-Clustern[3], da keine einzige Ressource innerhalb dieses Verbundes nur einmal vorhanden ist.

Manuelle Wiederherstellung

Dieser Ansatz wird am besten mit folgender Aussage beschrieben: „Warten, bis etwas passiert, und erst dann korrigierend einschreiten". Sofern wirksame Verfahren zur Datensicherung praktiziert werden, ist diese Methode effektiv und wird in der heutigen Praxis sehr oft vorgefunden. Man macht sich erst nach einem IT-Systemausfall Gedanken zur notwendigen Wiederherstellung und akzeptiert die nicht prognostizierbare Dauer der Wiederherstellungsphase. Folgerichtig sind die mit dieser Phase korrespondierenden Kosten ebenfalls nicht limitiert.

Automatische Wiederherstellung

Bei der Abwägung, ob eine manuelle oder automatische Lösung den Praxisanforderungen gerecht wird, hilft auch die Beantwortung der folgenden Fragen:
- Was ist, wenn der IT-Experte im Moment des IT-Ausfalls nicht erreichbar ist?
- Ist ein IT-Ausfall am Wochenende oder in der Urlaubszeit tolerierbar?
- Was ist, wenn der Servicetechniker, der das Praxisnetzwerk aufgebaut hat, das Serviceunternehmen verlässt?
- Wie schnell kann in diesem Fall ein gleichwertiger Ersatz aufgebaut werden?
- Wie lange können Verwaltungsaufgaben ohne IT mit handschriftlichen Notizen realisiert werden?
- Wie lange darf die letzte Datensicherung zurückliegen, ohne dass ein effektiver Datenverlust eintritt?

Die automatische Wiederherstellung löst Probleme, die aus diesen Fragestellungen resultieren. Mit automatischen „Failover"-Systemen erfolgt die laufende Überwachung des IT-Gesundheitszustands wichtiger Komponenten und bei einem Ausfall der vollautomatische Ersatz ausgefallener Ressourcen.

Am Beispiel eines digitalen DVT-Systems mit explizit benötigtem Rekonstruktionsserver skizziert Abbildung 4 eine mögliche Hochverfügbarkeitslösung. Zum DVT-Installationszeitpunkt erfolgt die Softwareinstalla-

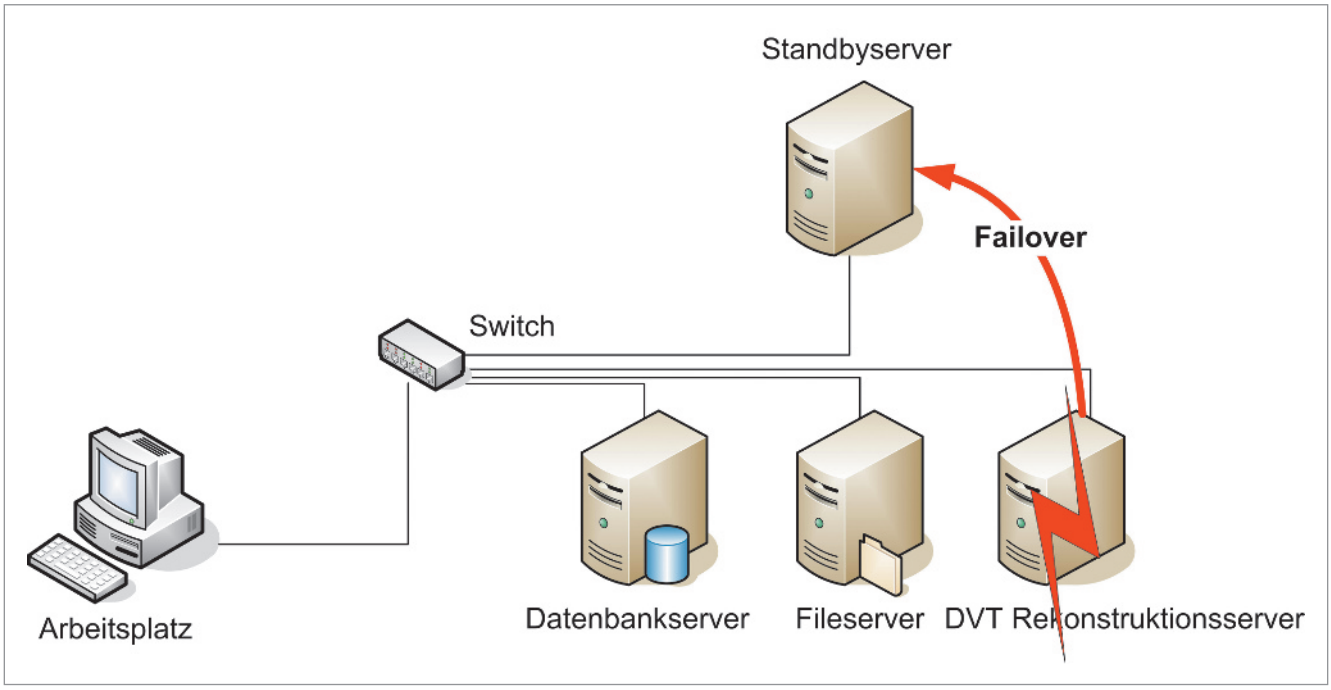

Abb. 4 Schematische Darstellung einer Failover-Clusterkonfiguration. Ein dedizierter PC stellt alle Dienste und Anwendungen eines zu sichernden Servers bereit. Im Fall eines Ausfalls tritt der „Failover" durch Übernahme der Netzwerkidentität des ausgefallenen Systems ein. Die Anwender im Netzwerk merken vom Serverausfall meist nichts und können ungestört weiterarbeiten

tion und -konfiguration zusätzlich auf einem redundanten Ausfallsystem (Standbysystem). Eine auf dem Standbyserver ebenfalls installierte Failover-Clustersoftware[2,6-8] kennt nun sowohl die neu installierten DVT-Komponenten als auch die Netzwerkidentität des zu sichernden, primären Rekonstruktionsservers. Im unerwarteten Fall eines Ausfalls des Primärsystems erkennt die Clustersoftware das Fehlen dieser Ressource und leitet die automatische Übernahme ein. Diese besteht aus zwei Schritten:

1. Sofern erforderlich werden benötigte Softwareanwendungen auf dem Standbysystem aktiviert.
2. Die ausgefallene Netzwerkidentität wird zusätzlich zur eigenen auf dem Standbyknoten hergestellt.

Als Ergebnis ist der DVT-Rekonstruktionsserver aus Sicht der Netzwerkclients (z. B. DVT-Modalitäten, PC-Workstations) auf dem Standbyserver verfügbar. In der Regel merken diese Clients gar nichts vom Ausfall des Primärsystems.

Die zusätzliche Absicherung weiterer zentraler Serverdienste kann leicht erreicht werden. So lässt sich der in Abbildung 4 dargestellte Datenbankserver zusätzlich zur DVT-Ausfallkonfiguration auf dem Standbyserver parallel ergänzen. Im Normalbetrieb werden alle Datenbankänderungen zeitnah auf das Standbysystem gespiegelt. Im Moment des Ausfalls übernimmt der Standbyserver auf dem Stand des zuletzt erfolgreich übertragenen Datenbankinhaltes, was in der Praxis meist ohne irgendwelche Datenverluste geschieht.

Die skizzierte Failover-Clusterlösung verkraftet auch einen gleichzeitigen Ausfall sowohl des Datenbankservers als auch des DVT-Rekonstruktionsservers, da das Standbysystem in diesem Fall neben der eigenen auch die Netzwerkidentitäten der ausgefallenen Server einnehmen kann.

Die Möglichkeiten zur Gestaltung eines Clusters beginnen bei zwei getrennten Systemen. Bereits bei drei eingesetzten Servern mit gegenseitiger Überwachung sowie Anwendungs- und Datenübernahme bei Ausfall eines Knotens erreicht man eine sehr hohe Gesamtsystemverfügbarkeit.

Ein wichtiges Kennzeichen bei automatischen Failover-Lösungen ist die Tatsache, dass man zu selbst gewählten Zeitpunkten entsprechende Strategien und Systeme plant und nicht bei vollbesetzter Praxis ungewollt von kritischen Ausfällen überrascht wird. Auch die Wiederherstellungsphase ist deutlich entspannter, da sie ja nicht mehr für die aktuelle IT-Verfügbarkeit notwendig ist. Das Standbysystem übernimmt diese Rolle. Entsprechende Serviceeinsätze zur Wiederherstellung ausgefallener Komponenten können somit mit dem Praxiskalender synchronisiert werden.

IT-Dokumentation und Notfallkonzept

Eine IT-Dokumentation weist folgende Bestandteile auf:

- Dokumentation aller IT-Komponenten und Knoten,
- Netzwerkschema mit Darstellung zentraler Netzwerkdienste,
- Beschreibung der installierten Anwendungen inklusive aller Aktualisierungen,
- Speicherung aller verwendeten Installationsprogramme in einem Softwarearchiv,
- Beschreibung des Datensicherungsprozesses (Backup),
- Beschreibung des Datenwiederherstellungsprozesses (Restore),
- Beschreibung des Langzeitarchivierungsprozesses und
- Dokumentation aller am Aufbau und an der Wartung des IT-Systems beteiligten Firmen und Ansprechpartner.

Das Notfallkonzept beschreibt weiterhin

- die Konfiguration eingesetzter Failover-Clusteranwendungen,
- alle Maßnahmen zur Wiederherstellung ausgefallener Serversysteme nach einem Ausfall und eingetretenem Failover durch das Standbysystem (Recover) sowie
- das Inventar aller Ersatzkomponenten (z. B. Ersatzswitch) mit Ortsangabe.

Diese Dokumentation muss mit jeder Änderung aktualisiert werden. Bewährt haben sich in diesem Zusammenhang auch chronologisch fortgesetzte Änderungslisten in kompakter Form (Log).

Eine aktuelle und klar verständliche Systemdokumentation steigert die IT-Verfügbarkeit in mehrfacher Weise:

- Bedienfehler von Seiten der Anwender, z. B. bei Datensicherungen oder Wiederherstellungen, werden durch einfach nachvollziehbare Bedienschritte vermieden.
- Die Wiederherstellungsphase nach einem Systemausfall wird verkürzt, da keine aufwändige Analyse des alten Ist-Zustandes erfolgen muss. Alle Komponenten und Konfigurationen sind in dokumentierter Form verfügbar.
- Das Wissen über das eigene IT-System bleibt nach Konfiguration oder Änderung und Verlassen des (meist externen) Servicetechnikers in der Praxis erhalten.
- Auch neues oder wechselndes Servicepersonal kann ohne Umwege oder langwierige Analysen mit der Systempflege oder -wiederherstellung beginnen.

Zusätzlich ist die konsequente Systemdokumentation ein wichtiger Baustein der Qualitätssicherung. Gepaart mit einer praxisindividuellen IT-Notfallplanung, können auch wichtige Aspekte des Risikomanagements abgedeckt werden.

Fazit

Im Praxisalltag ist nicht entscheidend, ob es zu einem fatalen IT-Systemausfall kommt, sondern wann dieser Fall eintritt, wie lange die nachfolgende Wiederherstellungsphase dauert und ob negative Auswirkungen für zu sichernde Datenbestände vorliegen. Eine Risikomi-

nimierung nur auf der Basis korrekt erstellter Datensicherungen alleine reduziert nicht die Wahrscheinlichkeit eines Systemausfalls und somit nicht verfügbarer, wichtiger IT-Komponenten für den Praxisalltag.

Statt sich zu fragen, wie bei einem IT-Ausfall (nur) der Datenverlust verhindert werden kann, sollte man sinnvoller zu folgender Fragestellung fortschreiten: „Wie lässt sich trotz eines IT-Systemausfalls ein kontinuierlicher Praxisbetrieb gewährleisten?" Die vorgestellten Lösungsansätze reduzieren hierbei nicht nur mögliche wirtschaftliche Schäden, sondern auch implizit das Risiko eines Datenverlustes.

Auf der Basis einer praxisindividuellen Analyse von potenziellen Ausfallkosten ist es möglich, einen sinnvollen Investitionsrahmen für die Einführung entsprechender Arbeitsprozesse und zusätzlicher Komponenten (Hochverfügbarkeitshardware und -software) zu ermitteln. Die konkrete Umsetzung der empfohlenen Maßnahmen lässt sich zu planbaren Zeiten ohne negative Beeinflussung des Praxisalltags „stressfrei" realisieren. Ein „Montagmorgen, 8 Uhr, nichts geht mehr ..." kann dann mit gutem Gefühl in Vergessenheit geraten.

Literatur

1. Marcus E, Stern H. Blueprints for high availability. 2. ed. Indianapolis: John Wiley & Sons, 2003.
2. PCCLUSTEX Clustersoftware. Internet: www.sidexisplugins.de.
3. Pfister GF. In search of clusters. 2. ed. New Jersey: Prentice Hall PTR, 1998.
4. Röntgenverordnung (RöV) in der Fassung der Bekanntmachung vom 30. April 2003, § 28 (Aufzeichnungspflichten).
5. Schulze D. Rechtliche Aspekte der Weitergabe und Sicherung von Röntgenaufnahmen – Teil 2: Datensicherung. Quintessenz 2010;61:201-205.
6. Wikipedia. Computercluster. Internet: www.de.wikipedia.org/wiki/Computercluster.
7. Wikipedia. High-availability cluster. Internet: www.en.wikipedia.org/wiki/High-availability_cluster
8. Wikipedia. Hochverfügbarkeit. Internet: www.de.wikipedia.org/wiki/Hochverfügbarkeit.