Ein IT-Notfallkonzept für den Fall der Fälle

Was tun bei einer technischen Havarie der IT-Systeme?

Die IT-Sicherheitsrichtlinie der KZBV beschreibt Maßnahmen, deren Notwendigkeit sich aus Art. 32 Datenschutzgrundverordnung (DSGVO) ergeben. Während diese Richtlinie der KZBV konkret einzelne Maßnahmen nennt, wie Forderungen der DSGVO praktisch umgesetzt werden können, definiert die Verordnung selbst einen Rahmen, der beschreibt, was durch diese Maßnahmen sicherzustellen ist.

Neben dem Schutz vor illegalem Zugriff, Datenmanipulation oder Sabotage soll die oben genannte Rechtsvorschrift auch gewährleisten, dass im Falle eines physischen oder technischen Zwischenfalls personenbezogene Daten und der Zugang zu diesen rasch wiederhergestellt werden können (Art. 32 Abs. 1 lit. c DSGVO). Darauf zielen einige Punkte der IT-Sicherheitsrichtlinie ab. Zum Beispiel sollen Administrationsdaten sicher aufbewahrt werden. Es steht außer Frage, dass die Umsetzung dieser Vorgabe von besonderer Bedeutung ist. Verfügt ein Administrator als einziger über die Administrationsdaten wie Wiederherstellungspasswörter oder das Passwort des Domänenadministrators und ist etwa durch einen Unfall überraschend selbst nicht mehr verfügbar, hat die von ihm betreute Praxis ein Problem, wenn die Daten benötigt werden. Ist der Administrator mehrere Wochen in Urlaub und fällt in dieser Zeit ein zentraler Rechner in der Praxis aus, kann die Praxis auch nicht darauf warten, dass der Administrator wieder aus dem Urlaub zurückkommt.


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.

Für den Fall einer technischen Havarie der IT-Systeme ist es daher geboten, dass Administratordaten und insbesondere alle Passwörter, die zur Wiederherstellung oder Instandsetzung von Systemen erforderlich sind, so hinterlegt werden, dass im Notfall kurzfristig darauf zugegriffen werden kann. Allerdings ist dabei auch darauf zu achten, dass nicht jeder Zugriff auf die entsprechenden Daten hat und die hinterlegten Daten nicht leichtfertig hervorgeholt und verwendet werden können.

Bei der Hinterlegung von Passwörtern können nämlich auch Fehler gemacht werden. Das macht ein Beispiel deutlich: In ei-

nem mittelständischen Betrieb mussten sämtliche Passwörter aufgrund eines Vorfalls geändert werden. Alle Passwörter sollten danach hinterlegt werden. Die Idee: Für jeden persönlichen Account sollte ein verschlossenes Couvert mit Zugangsdaten und Passwörten im Tresor der Geschäftsleitung verfügbar sein. Die schlechte Umsetzung: Dummerweise erfasste ein Mitarbeiter alle Accounts einschließlich der Passwörter in einer Liste und verteilte diese als Kopie auf allen Schreibtischen im Unternehmen. Dumm gelaufen. Die Passwörter mussten alle noch einmal erstellt werden. Das Fazit: Wichtige Passwörter und Administratordaten sind so zu hinterlegen, dass sie nur von besonders berechtigten Personen kurzfristig genutzt werden können – und dies auch nur dann, wenn es erforderlich ist.

Für die Hinterlegung von Daten und Passwörtern hat es sich übrigens bewährt, glasfaserverstärkte Kuverts zu verwenden, die nur durch sichtbares Zerstören, z.B. mittels einer Schere, geöffnet werden können.

Die Fähigkeit, Daten und Systeme rasch wiederherzustellen, erfordert eine vorherige Planung und ein Konzept.

Ein früherer Artikel hatte sich mit der Datensicherung befasst. Auf diesen Artikel („Daten richtig sichern“; ZZI 01/2021) wird hier noch einmal explizit verwiesen, da die Datensicherung elementarer Bestandteil von IT-Notfallkonzepten ist.

Die Fähigkeit, Daten und Systeme rasch wiederherzustellen, erfordert eine vorherige Planung und ein Konzept. Es ist denkbar ungünstig, sich erst dann Gedanken darüber zu machen, wie man die Systeme der Praxis wiederherstellen kann, wenn ein zentraler Server gerade durch Blitz, Feuer, Wasser oder andere schädliche Einflüsse zerstört wurde.

Es gibt viele denkbare Szenarien, in denen auf ein IT-Notfallkonzept zurückgegriffen werden muss. Jedoch hat es sich nach den Erfahrungen des Autors bewährt, nicht jeden erdenklichen Schadensfall einzeln zu betrachten. Vielmehr erscheint es ebenso effektiv wie effizient zu sein, das IT-Notfallkonzept für den schlimmsten aller denkbaren Fälle zu planen.

Dabei gibt es jedoch auch einige Besonderheiten, die eine Zahnarztpraxis zum Beispiel wesentlich von einem Beratungsunternehmen unterscheiden. Ist ein Beratungsunternehmen, das sämtliche Daten in einem Rechenzentrum ausgelagert hat, von einer Havarie der eigenen IT-Systeme betroffen oder brennt bis auf die Grundmauern nieder, so sehen dort IT-Notfallkonzepte häufig vor, dass von beliebigen anderen Standorten auf Daten im Rechenzentrum zugegriffen wird.

Diese Möglichkeit besteht in einer zahnärztlichen Praxis, in der Patienten behandelt werden, üblicherweise nicht, insbesondere wenn neben der IT auch Medizingeräte und Räumlichkeiten zerstört sind. Der in diesem Bereich betrachtete „schlimmste Fall“, der als Grundlage für die Erarbeitung eines IT-Notfallplans in einer Praxis dienen kann, beschränkt sich daher auf die vollständige Zerstörung der IT-Infrastruktur.

Durch Betrachtung des maximal vorstellbaren Schadens im Bereich der IT-Infrastruktur, werden alle Teilbereiche abgedeckt, und eine Mehrfachnennung einzelner Maßnahmen wird im Konzept vermieden.

Sind im Rahmen eines Vorfalls nun nur Teilbereiche betroffen, so ist dennoch beschrieben, wie die entsprechenden Schäden schnell behoben oder zumindest kompensiert werden können.

Soweit die gesamte IT-Infrastruktur einer Praxis zerstört wäre, würde das folgende Teilbereiche betreffen:

- Server
- Personalcomputer oder Terminals
- Netzwerkverteiler und Patchfelder (Verkabelung)
- Monitore, Tastaturen, Drucker und sonstige Peripheriegeräte
- u.U. Schnittstellen zu Medizingeräten
- Router und Firewalls
- Internetzugänge

Die Erfahrung zeigt, dass Komponenten beim Testen von Notstromanlagen durch Blitzschlag oder Überspannung oder durch Leckage an Rohren oder Klimageräten durchaus zerstört werden können. Die Ursachen für einen entsprechenden Schaden können dabei aber weitaus vielfältiger sein, als das hier vom Umfang her beschrieben werden kann. Es hat sich allerdings auch gezeigt, dass bei entsprechender Planung die Arbeit nach Eintritt eines Schadensfalls innerhalb einer vertretbaren Zeitspanne wieder fortgesetzt werden kann.

Zunächst sollte damit begonnen werden eine Übersicht über Hard- und Software zu erstellen und zu dokumentieren, für welche Tätigkeiten, welche Geräte beziehungsweise Systeme eingesetzt werden. Im nächsten Schritt sollte realistisch bewertet werden, nach wie vielen Stunden oder Tagen jedes einzelne System spätestens wieder zur Verfügung stehen muss. Je nach System kann diese Anforderung stark variieren. Diese Einschätzung ist jedoch von grundlegender Bedeutung, damit beim Ausfall mehrerer Systeme eine Priorisierung der Wiederherstellung erfolgen kann. Üblicherweise sind Aufwand und Kosten höher, je kürzer die Zeitspanne für eine Wiederinbetriebnahme gewählt wird.

Soweit für Geräte Wartungsverträge geschlossen wurden, sollten diese Verträge als Kopie ebenfalls im IT-Notfallkonzept verfügbar sein.

Als Nächstes wäre zu beschreiben, wer zu informieren oder zu kontaktieren ist, wenn ein bestimmtes System wiederherzustellen beziehungsweise wenn ein bestimmter Schaden eingetreten ist. Dazu müssen alle Ansprechpartner, Verantwortliche, Firmen und deren Erreichbarkeit aufgelistet werden.

DAS NOTFALLKONZEPT

Im IT-Notfallkonzept sollten sich mindestens folgende Informationen finden:

1. Konzept zur Datensicherung, Rücksicherung und Wiederherstellung von Installationen und Daten oder ein Verweis darauf
2. Die Information, wo Administratordaten hinterlegt/verfügbar sind.
3. Die Übersicht über Hardware, Software und Systeme
4. Eine Priorisierung der Systeme und gegebenenfalls eine Übersicht, wer welche Systeme nutzt
5. Zuständigkeiten
6. Meldeketten, Kontaktdaten, Support- und Notrufnummern
7. Kopien der Supportverträge (Hard- und Software)
8. Individuelle Informationen, was an Material und Geräten verfügbar ist oder wie und wo diese im Notfall zu beschaffen sind
9. Eine Beschreibung, wie das Netzwerk nach Zerstörung wieder aufzubauen ist

Soweit für Geräte Wartungsverträge geschlossen wurden, sollten diese Verträge als Kopie ebenfalls im IT-Notfallkonzept verfügbar sein. Hinsichtlich solcher Verträge sollte allerdings unbedingt auch separat zur IT-Notfallplanung eine terminliche Überwachung erfolgen. Dem Autor sind Fälle bekannt, bei denen z.B. ein Serverhersteller beim Ausfall eines Netzteils darauf verwiesen hat, dass der Support für das entsprechende Gerät drei Tage zuvor ausgelaufen war. Erst nach schriftlicher Zusicherung, dass man eine Reparaturpauschale i.H.v. 2.400 Euro zzgl. MwSt. zahlen würde, der noch die Kosten für Ersatzteile und Reisekosten hinzuzurechnen wären, wollte das Unternehmen dann einen Außendienstmitarbeiter vorbeischicken, um den Schaden zu beheben. Wenn man auf einen derartigen Fall nicht vorbereitet ist, kostet eine Reparatur, die durchaus mit 300 Euro gut bezahlt wäre, schon einmal mehr, als für den Neukauf eines Servers erforderlich wäre. Soweit eine Notsituation besteht, neigen einige Unternehmen dazu, Kunden abzuzocken. Man sollte sich daher auch immer darüber informieren, zu welchen Konditionen Unternehmen tätig werden, wenn ein Notfall eintritt.

Der ein oder andere Leser wird nun denken, dass derjenige, der einen Supportvertrag auslaufen lässt selbst schuld ist, wenn er nachher mit überhöhten Rechnungen konfrontiert wird. Kaum eine Institution des Gesundheitswesens wird jedoch alle zwei oder drei Jahre ihre Server erneuern können. Einige Anbieter bieten gegen Aufpreis einen umfassenden Support für Server bis zu einem Alter von sieben Jahren. Allerdings sollten die vertraglichen Einzelheiten generell im Zuge der Erstellung eines IT-Notfallkonzepts geprüft werden, sodass auch wirklich eine Instandsetzung innerhalb eines vertretbaren Zeitrahmens sichergestellt ist.

Bei einem tatsächlichen Vorfall hatte die Institution einen sogenannten 7/24-Vertrag abgeschlossen mit einer vereinbarten Reaktionszeit von vier Stunden. Der Support sollte entsprechend rund um die Uhr an sieben Tagen der Woche gewährleistet sein. Nachdem am dritten Tag nach der Meldung des Serverausfalls immer noch keine Rückmeldung durch das Unternehmen erfolgt war, brachte erst ein Telefonat mit dem Geschäftsführer der Deutschen Tochtergesellschaft eines US-Konzerns den Vorgang in Bewegung. Allerdings betrug die Standzeit in diesem Fall doch insgesamt vier Tage. Die Zuverlässigkeit eines Unternehmens sollte daher bei der Auswahl von IT-Geräten unbedingt berücksichtigt werden, wobei die Größe eines Unternehmens kein Garant ist für seine Zuverlässigkeit.

Hinsichtlich eingesetzter Hardware sollte auch die Ersatzbeschaffung geregelt sein. Eine Neubeschaffung, bei der zwischen Bestellung und Lieferung vier Wochen vergehen, ist nicht zielführend. Hier kommt auch das Datensicherungskonzept zum Tragen. Soweit nämlich mit Virtualisierungstechnik oder mit hardwareunabhängigen Datensicherungen gearbeitet wird, ist man eher nicht an einen bestimmten Hersteller von Servern und Rechnern gebunden.

Es muss also die Frage beantwortet werden, wo und wie schnell Ersatzgeräte zur Verfügung stehen können, wenn IT-Geräte in der Praxis ausfallen. Dabei gilt es zu bedenken, dass die beste Datensicherung nichts hilft, wenn ein System nur auf einer „exotischen“ Hardware betrieben werden kann und diese eine Lieferzeit von mehreren Wochen oder sogar Monaten hat.

In der Übergangsphase von einem Betriebssystem zum Nachfolgesystem bei einem Schadensfall hatten sich Konstellationen ergeben, bei denen PC-Systeme auf verfügbaren Ersatzgeräten installiert werden sollten. Die Ersatzgeräte waren jedoch teilweise nicht mehr mit dem alten Betriebssystem kompatibel, sodass in solchen Fällen trotz des Vorhandenseins von Reservegeräten mitunter doch noch Hardware beschafft werden musste. Die Kompatibilität spielt also auch eine wesentliche Rolle, wenn Server oder Rechner ersetzt werden müssen.

Wenn das Netzwerk in einer Praxis zerstört wurde, kann man sich zumindest in kleinen und mittleren Praxen eventuell damit behelfen, dass man eine Notverkabelung vornimmt oder Rechner mittels WLAN integriert. Die Zerstörung von Netzwerken kann z.B. durch Blitzeinschlag oder Feuer im Netzwerkverteiler auftreten. Netzwerkverteiler, die zwar nicht für den professionellen Dauerbetrieb geeignet sind, aber durchaus im Rahmen eines Notfalls zum Einsatz kommen können, gibt es bereits für wenig Geld in jedem Geschäft, das Computerzubehör vertreibt. Im Notfall kann man dann mittels solcher Switches und mit vorkommissionierten Patchkabeln und RJ45-Kabelrollen eine Verkabelung für den Notbetrieb aufbauen. Hierbei sollte aber unbedingt auch der Brandschutz beachtet werden.

Es ist daher sinnvoll, auch die Kontaktdaten des Brandschutzbeauftragten im IT-Notfallkonzept zu erfassen. Ansonsten kann ein Netzwerk auch kurzfristig mittels WLAN aufgebaut werden. Dabei müssen dann je nach Größe der Praxis eventuell

noch sogenannte Repeater eingesetzt werden. Das Material dazu ist auch in aller Regel schnell zu beschaffen.

Schließlich sollte die Frage geklärt werden, wie lange eine Praxis ohne Internet auskommt oder wie eine Internetverbindung zur Verfügung gestellt werden kann, wenn der sonst genutzte Anschluss ausfällt. Dabei darf nicht übersehen werden, dass eine Firewall oder ein Router nicht in jedem Computerladen vorrätig sind und gegebenenfalls beschafft werden müssen. In einem solchen Fall könnte ein Notbetrieb z.B. mittels einer Datenverbindung über das Mobilfunknetz kurzfristig etabliert werden. Dabei sollte allerdings das erforderliche Sicherheitsniveau gewährleistet sein. Es kann sinnvoll sein, die Nutzung von Internet und E-Mail im Rahmen eines Notbetriebs auf das absolut Notwendige zu beschränken.

Zuweilen kommen proprietäre Systeme zum Einsatz, die z.B. als Konverter fungieren, um bestimmte Geräte in das Computernetzwerk zu integrieren. Solche Schnittstellen können mitunter recht teuer sein, fallen jedoch auch nur selten aus, sodass man vor Ort meistens kein Ersatzgerät zur Verfügung hat. In diesem Fall ist es gut zu wissen, wie und wo ein Ersatzgerät kurzfristig beschafft werden kann. Je nach Wichtigkeit einer Komponente ist es im medizinischen Umfeld nicht ungewöhnlich, Ersatzteile auch schon einmal über mehrere hundert Kilometer vom Hersteller per Taxi anliefern zu lassen. Soweit exotische Hardware zum Einsatz kommt, ist dringend angeraten im Vorfeld zu klären, wie diese kurzfristig beschafft werden kann. Die entsprechende Vorgehensweise sollte dann auch im IT-Notfallhandbuch beschrieben sein.

Erstellt man ein IT-Notfallkonzept, das sich an einem Totalausfall der IT-Infrastruktur orientiert, so sind alle Teilbereiche abgedeckt und das Konzept kann entsprechend kurzgehalten werden. Das ist insbesondere deshalb wichtig, weil im Falle einer IT-Havarie niemand Handbücher im Umfang von mehreren hundert Seiten wälzen möchte.

Wenn ein schlüssiges IT-Notfallkonzept vorliegt und eine gut durchdachte Datensicherung existiert, können technische Störungen und Systemausfälle in aller Regel in einem überschaubaren Zeitrahmen behoben werden. Selbst wenn dazu auch zuweilen Interimslösungen erforderlich sind, ist es nach einem technischen Vorfall möglich, Systeme und Daten in einer Praxis rasch wieder verfügbar zu haben, wenn eine strukturierte Planung zugrunde liegt.

Wenn ein IT-Notfallkonzept fehlt, sollte dieses mit dem IT-Administrator abgestimmt werden. Es sollte insbesondere schriftlich festgehalten werden, innerhalb welches Zeitraums die Praxis wieder vollständig arbeiten kann, wenn die IT-Infrastruktur zerstört wurde.

Im nächsten Artikel dieser Serie erfahren Sie, warum Technik allein als Schutz vor Cyberangriffen und Vorfällen im Bereich von Datenschutz und Datensicherheit nicht ausreichend ist und was Sie bei der Schulung und Sensibilisierung von Mitarbeitern unbedingt beachten sollten.

→ **Dr. Thomas H. Lenhard**