APRIL 2022

IT-Sicherheit in Arztpraxen und die Einordnung von Bedrohungen

GRUNDLAGEN

Erstellt durch die AG Digitales im Hausärzteverband Niedersachsen in Kooperation mit Daniel Köhler

DEUTSCHER HAUSÄRZTEVERBAND
Landesverband Niedersachsen e.V.

INHALT

IMPRESSUM

Deutscher Hausärzteverband - Landesverband Niedersachsen e. V.
Berliner Allee 46 | 30175 Hannover
Telefon 0511 - 22 87 78 0 | Fax 0511 - 22 87 78 77 | info@haevn.de

Vorstand: *Vorsitzender Dr. med. Matthias Berndt*
Vereinsregister: *Amtsgericht Hannover | Nummer: 3545*
Redaktion & Layout: *Forum Digitales, Dr. med. Kristina Spöhrer, Daniel Köhler, Tim Fischer*
Bilder & Grafiken: pixabay.de | canva.com

LIEBE KOLLEGINNEN UND KOLLEGEN,

„Digitalisierung im Gesundheitswesen“ ist in aller Munde und wir erleben aktuell in den Praxen praktisch jedes Quartal eine Neuerung, die unsere etablierten Prozesse verändert. Manches ist positiv, aber vieles funktioniert bisher nur in der Theorie. Seit vielen Jahren arbeiten wir Hausärztinnen und Hausärzte mit unseren PVS bereits erfolgreich digital. Zum Beispiel bei der Dokumentation, Abrechnung oder Kodierung. Viele von uns haben in den vergangenen Jahren neue digitale Anwendungen wie Online-Terminkalender oder Videosprechstunden eingeführt.

Das Forum Digitales im Deutschen Hausärzteverband hat es sich auf Bundes- sowie auf den Landesebenen zum Ziel gesetzt, die Digitalisierung im Gesundheitswesen möglichst eng zu begleiten, um auf gute Lösungen für Hausarztpraxen hinzuwirken. Wir wollen – soweit möglich – den digitalen Wandel mitgestalten, um wichtige Aspekte der hausärztlichen Tätigkeit einzubringen und „die Digitalisierung“ mit Sinn zu füllen. Auch ist uns wichtig, Sie als Kolleginnen und Kollegen auf dieser digitalen Reise zu begleiten, anstatt sie mit ihrem IT-System und den entstehenden Fragen allein zu lassen.

In dem hier vorliegenden Leitfaden nehmen wir die IT-Sicherheit in den Hausarztpraxen in den Blick, die mit zunehmender Vernetzung immer wichtiger wird. Daraus ergibt sich für uns als Verantwortliche die dringende Notwendigkeit, sich intensiver damit zu beschäftigen. Sonst besteht die Gefahr, dass nach einem erfolgreichen Hackerangriff Patientendaten gegen Lösegeld zurückgegeben oder frei ins Internet gestellt werden.

Gemeinsam mit dem IT-Experten Daniel Köhler gibt das Forum Digitales im Landesverband Niedersachsen mit dieser Broschüre eine Orientierung, wie Sicherheit in einer zunehmend digitalen Praxis funktionieren kann.

Was muss ich beachten? Welche Wege führen zu einer sicheren Praxis-IT? Auf diese und weitere Fragen möchten wir mit diesem Leitfaden erste Antworten geben. Um ihn künftig zielführend anpassen und ergänzen zu können, freuen wir uns sehr über Anregungen zu neuen Themen oder Fragen. Wir wünschen eine informative Lektüre!

Mit freundlichen, kollegialen Grüßen

Dr. med. Matthias Berndt und Dr. med. Kristina Spöhrer

Vorsitzender des Deutschen Hausärzteverbandes - Landesverband Niederssachsen e. V.

Sprecherin im Forum Digitales in Niedersachsen

VORWORT

GRUNDLAGEN

GRUNDSÄTZLICH SIND EINIGE DINGE BEI DER IT-SICHERHEIT IN ARZTPRAXEN ZU BEDENKEN. WIE IN JEDEM BERUFLICHEN UMFELD SOLLTEN AUCH HIER GEWISSE VORGABEN GELTEN. INSBESONDERE SOLLTE DIE NUTZUNG DER LOKALEN EDV-SYSTEME AUF PRAXISRELEVANTE ARBEITSVORGÄNGE BESCHRÄNKT WERDEN. PRIVATE NUTZUNG IST MÖGLICHST KOMPLETT ZU UNTERBINDEN.

Beispiele:

- **Bilder und Videos von privaten USB-Sticks teilen/betrachten**
- **Privates Surfen im Internet über die Praxis-EDV**
- **Nutzung von privaten Smartphones im Praxisnetzwerk**

LOKALE SICHERHEIT

Sämtliche EDV sollte vor Zugriffen durch Patienten oder Besucher geschützt werden. Hierzu zählen sowohl Einsicht in Passwörter von Systemen oder WLANs (z. B. auf dem Schreibtisch notiert) als auch Zugriffe auf Systeme – beispielsweise bei Wartezeiten allein im Sprechzimmer.

Beispiele:

- **Netzwerkdose im Wartezimmer**
- **Kein Windows Passwort**
- **WLAN-Router im Flur**
- **WLAN-Passwort an Pinnwand**

GRUNDLAGEN

NETZWERKSICHERHEIT

Prinzipiell sollte eine Praxis keinen Internetzugriff von außen auf die Praxis erlauben (siehe Firewalls/Router). Früher musste eine Arztpraxis nicht mit dem Internet verbunden sein. Doch durch die stetig voranschreitende Digitalisierung wird eine Verbindung mit dem Internet aus organisatorischen sowie gesetzlichen Gründen immer häufiger benötigt. Hierbei gilt es, gewisse Abläufe und Verhaltensmuster im Umgang mit dem Internet zu üben. Sie werden im Folgenden in groben Zügen beschrieben.

Daten, die mit dem Internet ausgetauscht werden können:

- **Abrechnungsdaten**
- **Labordaten**
- **Patientendaten**
- **[...]**

Beim Austausch über das Internet gilt es zu unterscheiden, ob Daten versendet oder empfangen werden. Beide Wege haben jeweils unterschiedliche Herausforderungen, die von einer Praxis bewältigt werden müssen.

VERSENDEN VON DATEN

Beim Versenden von Daten ist die eigene Praxis in der Regel keiner unmittelbaren Gefahr ausgeliefert. Hier sind z. B. folgende Szenarien vorstellbar:

- **Schicken einer E-Mail (an PatientInnen/KollegInnen)**
- **Übermitteln von Abrechnungsdaten**
- **Übermitteln von EKGs an Auswertungsdienste**
- **Übermitteln von Versichertendaten über die TI**
- **Schicken einer KIM-Nachricht**
- **Faxnachricht**

Bei den aufgeführten Punkten kann kein Angriff von außen auf die Praxis erfolgen. Hier ist nicht die IT-Sicherheit das Problem, sondern der Datenschutz, der zu bewahren ist.

Werden z. B. Patientendaten unverschlüsselt an eine falsche E-Mail-Adresse gesendet, hat man sich schnell strafbar gemacht, da man Gesundheitsdaten veröffentlicht hat. Das ist auch der Fall, wenn der Empfänger eigentlich ein Kollege sein sollte und der Adressat versehentlich falsch ausgewählt wurde.

Beim Versenden von Abrechnungsdaten sorgt das Verschlüsselungsmodul des PVS vorab für eine sichere Übertragung der Daten und Einhaltung des Datenschutzes.

Bearbeitet man mit Kollegen gemeinsam EKGs oder andere Daten, werden diese meist anonymisiert ausgetauscht, um den Datenschutz zu gewährleisten. Bei allen Anwendungen der TI ist die Verschlüsselung und die Authentizität des Empfängers sichergestellt.

Beim Versenden von Daten sollte der Fokus also immer auf dem Datenschutz liegen. Anders sieht es beim Abrufen oder Empfangen von Daten aus.

GRUNDLAGEN

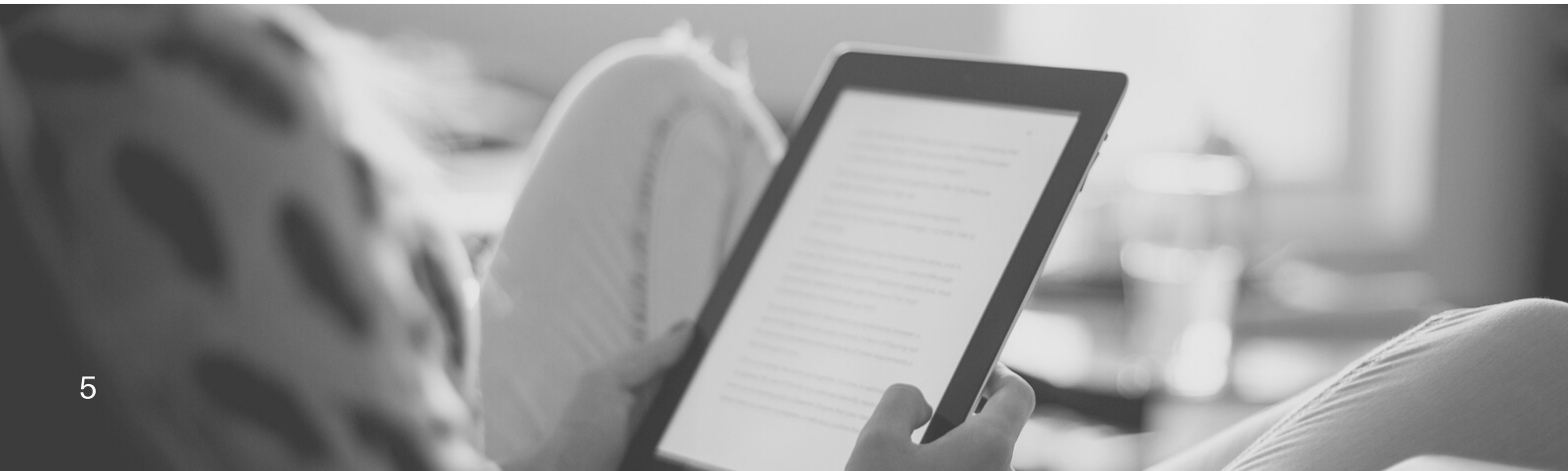
EMPFANGEN VON DATEN

Beim Empfangen von Daten ist nicht der Datenschutz die zu meisternde Hürde. Hier geht es darum, dass alle Daten, die das Praxissystem erreichen, geprüft werden müssen. Der Empfang von Daten ist in der Regel auf folgenden Wegen möglich:

- **Per E-Mail**
- **Per CD/USB-Stick von PatientInnen**
- **Per CD/USB-Stick von KollegInnen**
- **Empfang einer KIM-Nachricht**
- **Empfang/Abruf von ePA-Dokumenten**
- **Aufruf einer Website**

EMPFANG EINER E-MAIL

Beim Empfangen von E-Mails gibt es aktuell besonders viel zu beachten. Bei gängigen E-Mail-Programmen können Viren und Co nur durch Anhänge oder schädliche Links aktiviert werden, jedoch sind diese oft gut versteckt. Wenn eine Praxis z. B. ein Inserat beim Arbeitsamt aufgibt, ist es nicht ungewöhnlich, dass die Praxis zeitnah E-Mails mit Bewerbungsschreiben und Lebensläufen als Anhang erhält. PDF Anhänge an E-Mails gelten zwar grundlegend als sicher, jedoch wird diese Sicherheit gerne ausgenutzt, indem die angehängte Datei als PDF vorgetäuscht wird. Oft lauten Dateinamen dann „Bewerbung.pdf.exe“. Bei Word-Dateien können wiederum schädliche „Makros“ in den Dokumenten versteckt sein. Deshalb ist es wichtig, die Ausführung von Makros standardmäßig in Office Dokumenten zu deaktivieren (was eine Standard-einstellung geworden ist).



KIM & CO.

KIM (KOMMUNIKATION IM MEDIZINWESEN) IST VON DER TECHNIK HER GLEICHZUSTELLEN MIT DER HANDELSÜBLICHEN E-MAIL-KOMMUNIKATION. IM VERGLEICH ZU EINER HERKÖMMLICHEN E-MAIL SORGT KIM FÜR EINE BESONDERS SICHERE ÜBERTRAGUNG DER DATEN UND EINEN EINDEUTIGEN ABGLEICH VON SENDER UND EMPFÄNGER (AUTHENTISIERUNG) GEGENEINANDER.

So kann man bei einer über KIM erhaltenen Nachricht sicher sein, dass diese auf dem Weg vom Sender zum Empfänger weder verändert noch entwendet wird. Zusätzlich ist eine KIM-Nachricht durch einen nachgewiesenen Absender authentisiert. So ist sichergestellt, dass der Absender auch wirklich der ist, der er vorgibt zu sein (siehe Beispiel Spam oder Malware).

Die Vorteile von KIM sorgen nun dafür, dass die üblichen, für E-Mails geltenden Regeln schnell nicht mehr umfassend angewendet werden (Absender überprüfen, Anhänge nicht öffnen, Links hinterfragen). Da bei KIM stets ein „echter" Absender hinter einer Nachricht steht, ist hier eine stärkere Vertrauensbasis vorhanden, als bei unbekannten E-Mail-Absendern. Wichtig ist allerdings zu beachten: Bei der Infektion eines einzigen KIM-Absenders können aus dem gesamten KIM-System Spam, Viren und Malware versendet werden! Diese Viren würden dann das hohe Vertrauen in den als sicher angesehenen Absender genießen und so leichter die menschliche Sicherheitsprüfung überstehen.

Zusammenfassend gelten für den Umgang mit KIM mindestens die selben Sicherheitspunkte wie für reguläre E-Mails.

Um die Angriffsfläche zu minimieren und den Schutz zu maximieren empfiehlt es sich also auch hier darauf zu achten, dass ein aktueller Virenscanner stets aktiv, aktuell und richtig konfiguriert ist. Grundlegend sollte ein Virenscanner jede Datei und jede Website vor dem Öffnen oder Ausführen einmal überprüft haben.

Ob Sie hierbei auf den kostenlosen Windows Defender setzen, der in jedem

.....>

KIM & CO.

Microsoft Windows System integriert ist, oder ob Sie von einem IT-Dienstleister einen remote verwalteten Virenscanner kaufen, damit dieser die Überwachung für Sie übernimmt, bleibt dabei Ihnen selbst überlassen.

Eine Firewall kann hier ergänzend nützlich sein, da sie die Verbindungen zu schädlichen Websites auf Basis von Filterlisten blockieren kann. Bei versehentlichem Ausführen eines Anhangs oder Anklicken eines gefälschten Links wird so den Datenverkehr zu den schädlichen Servern blockiert.

Virenscanner und Firewall sind natürlich Rettungen in letzter Sekunde. Wichtiger ist, dass das Praxisteam darauf sensibilisiert ist, wie man falsche Anhänge und E-Mails erkennt und diese sicher löscht.

Gerade durch die Verschlüsselung von KIM können Nachrichten nicht vor dem Eingang von Firewalls und Virenscannern geprüft werden. Dies ist bei normalen E-Mails hingegen auf technischem Wege möglich.

UPDATES UND PATCHES

Damit man sich nicht allein auf die Funktionalität seines Virenscanners oder der Firewall verlassen muss (kein Produkt kann eine 100%ige Sicherheit bieten), sollten alle Programme und Betriebssysteme auf allen Arbeitsplätzen regelmäßig geupdatet werden. Dazu zählen unter anderem Windows, Java, Firefox, Thunderbird und Adobe Reader.

Auch häufig verwendete Anwendungen können Sicherheitslücken aufweisen. Dies macht es Schadsoftware möglich, auf Wegen ins System einzudringen, die Virenscanner nicht unmittelbar im Auge haben. So könnte z.B. ein Fehler im Internetbrowser Firefox dazu führen, dass beim Aufrufen einer unscheinbaren Website im Hintergrund ein Code ausgeführt wird, der den Virenscanner deaktiviert und sich Zugriff verschafft. Ein Virenscanner hat keine absolute Hoheitsgewalt im System und ist von dessen Stabilität abhängig.

VIRENSCANNER

Das Thema Virenscanner ist eins der wichtigsten Themen und gleichzeitig besonders undurchsichtig. Die Werbung für entsprechende Produkte suggeriert häufig, dass man heutzutage einen Virenscanner mit Firewall und vielen Extrafunktionen benötige. Dabei beschreibt ein Artikel aus der c't von 3/19 ziemlich gut den nötigen Nutzungsumfang. Er hat auch heute noch Gültigkeit.
https://www.heise.de/select/ct/2019/3/1549002696073866

Auch bei Arztsystemen gelten die Grundsätze dieses Artikels und sollen hier nur ergänzt werden.

Grundsätzlich bieten sehr viele Virenscanner einen gleichartigen Schutzstandard. Wie in aktuellen, unabhängigen Tests von av-test.org und av-comparatives.org dargelegt wird, sind alle namhaften

KIM & CO.

Antivirushersteller regelmäßig sehr nah an der 100-%-Erkennungsrate dran.

Was zu unterscheiden ist, sind die kostenlosen Virenscanner von den kostenpflichtigen. Hierbei sollte man sich entweder zwischen dem kostenlosen und aktuell werbefreien Windows Defender oder einer werbefreien kostenpflichtigen Version eines anderen Anbieters entscheiden. Werbe-Pop-Ups haben in einer Praxis schließlich nichts zu suchen!

Bei kleineren Praxen oder bei guten IT-Kenntnissen ist aus Sicht der Schutzleistung nichts gegen die mit Windows vorinstallierte Windows Defender Version einzuwenden. Dieser Scanner kann entsprechend konfiguriert und eingesetzt werden. Es gilt hierbei nur darauf zu achten, dass Updates regelmäßig auf allen Geräten geprüft und die Funktionalität sichergestellt wird.

Diesen Punkt kann man sich durch einen IT-Dienstleister, der oft auch mindestens einen Virenscanner vertreibt, häufig sparen. Ein sog. „Managed Antivirus Client“ wird zentral von einem Dienstleister auf Funktion, Updates und Konfiguration überwacht. Im Anbetracht des Preises sollte es auch die ausschlaggebende Rolle spielen, ob man die Verwaltung des Virenschutzes an jemanden abgibt und dafür eine Lizenz bezahlt.

DIE EINSTELLUNGEN DES VIRENSCANNERS

Da es nicht möglich ist, alle Einstellungen von allen Virenscannern abzubilden, hier einmal ein Ausschnitt der Grundfunktionen, die konfiguriert sein sollten. Diese heißen bei jedem Hersteller ein wenig anders oder sind teilweise unter Begriffen zusammengefasst:

Zugriff vor Ausführung	**Bevor eine Datei/E-Mail einem Anwender angezeigt/geöffnet wird, muss der Virenscanner diese prüfen. Ausnahmslos!**
Prüfung von SSL-Zertifikaten	**Der Virenscanner prüft beim Surfen im Internet, ob es sich bei einer aufgerufenen Website bzw. deren Verschlüsselungszertifikat um ein Original handelt. Dies prüft der Virenscanner unabhängig von vertrauten SSL-Zertifikaten des Browsers oder Betriebssystems.**
Prüfung von E-Mails	**Einige Virenscanner haben Plugins für Mailprogramme, andere prüfen grundlegend POP3- und IMAP-Verkehr. Durch Verschlüsselung ist dies nur noch begrenzt möglich (siehe KIM).**
Prüfung von Wechselmedien	**USB-Sticks, USB-Festplatten und CDs sollten immer vor dem Öffnen komplett gescannt werden. Dies sollte voreingestellt sein, damit es automatisch passiert.**
Ausschlussfilter kleinhalten	**Softwarehersteller geben gern eine Ausnahme für ganze Verzeichnisse an, die vom Virenscanner ausgeschlossen werden. Hierbei ist besonders bei KIM darauf zu achten, dass solche Filter angepasst werden. KIM legt Dateien ggf. im PVS-Verzeichnis ab, wo künftig ein Virenscanner nicht ausgeschlossen werden sollte.**
Cloud Prüfung	**Aktivieren, falls verfügbar. Hier werden die aktuellsten Informationen zu Virenmustern mit anderen Teilnehmern abgeglichen.**

DEUTSCHER HAUSÄRZTEVERBAND
Landesverband Niedersachsen e.V.

BACKUPS

IN DIESEM ABSCHNITT SOLLTE ZUNÄCHST GEKLÄRT WERDEN, WAS EIN SINNVOLLES BACKUP IST UND WAS NICHT.

Unter einem Backup ist eine vollständige Sicherung sämtlicher Daten zu verstehen. Diese Daten umfassen in der Regel die Patientendaten aus dem PVS, externen Daten wie Befunde, Praxisdaten, die zur Abrechnung und Praxiskoordination gehören, sowie – wenn möglich – sämtliche Konfigurationen von Servern und Geräten. Im Grunde also alles, was irgendwie digital gespeichert ist. Hierbei kann man sich folgende Frage stellen: „Wenn meine Praxis von einem Brand betroffen ist, bekomme ich dann mit meinem Backup alle Daten wiederhergestellt?“

Dies führt auch direkt zur Frage, wofür man ein Backup braucht und warum eine Festplattenspiegelung (z.B. durch ein RAID-System) kein Backup ist. Backups sind dafür verantwortlich, in den Fällen von:

- **Brand / Wasser / Naturkatastrophen**
- **Diebstahl**
- **Löschung von Daten (mutwillig oder unabsichtlich)**
- **Viren / Verschlüsselungstrojanern**
- **Systemfehlern**

... sämtliche Date zum Zeitpunkt des letzten Backups wiederherzustellen. Ein Backup dient hingegen nicht der Ausfallsicherung, falls Server oder Festplatte kaputt gehen. Ein Backup kann dann nach Austausch der defekten Hardware nur alle Daten wiederherstellen, verhindert einen Ausfall jedoch nicht. Ein RAID oder Virtualisierung können hierbei hingegen helfen.

BACKUP-SZENARIOS

Damit die vorab genannten Anforderungen an ein Backup erfolgreich gewährleistet werden können, ist es wichtig, dass es gewisse Kriterien erfüllt.

Ein Backup sollte:

- **Verschlüsselt sein**
- **Regelmäßig überprüft und durch Rücksicherungen getestet werden**
- **An mindestens 2 Standorten aufbewahrt werden**
- **Mindestens täglich stattfinden**

BACKUPS

Diese Kriterien sind wichtig, weil:

- Unverschlüsselte Backups können beim Transport aus der Praxis verloren gehen oder sogar in der Praxis gestohlen werden (USB-Festplatte) und würden dann alle Patientendaten problemlos lesbar machen. Außerdem schützt eine Verschlüsselung bei einer sogenannten „Offsite Sicherung" der Daten bei Cloud-Anbietern.
- Ein Backup, welches sich im Notfall nicht zurückspielen lässt, ist unbrauchbar.
- Diebstahl, Naturkatastrophen etc. und besonders Viren zerstören meist das gesamte Netzwerk inkl. der dortigen Sicherung. Deshalb ist es wichtig, eine Sicherung nach dem 3-2-1 Prinzip aufzubewahren. Es sollten 3 Datensätze vorhanden sein, auf 2 unterschiedlichen Medien und davon 1 außer Haus.
- Eine wöchentliche oder sogar monatliche Sicherung ist zwar besser als keine Sicherung, erfordert aber im Ernstfall eine sehr komplexe Aufarbeitung der verlorenen Daten, was zu sehr viel Ausfallzeiten führen kann.

WELCHES BACKUP?

Da es verschiedene Arten von Backupsystemen gibt, sollten vorab gewisse individuelle Fragen in der Praxis geklärt werden.

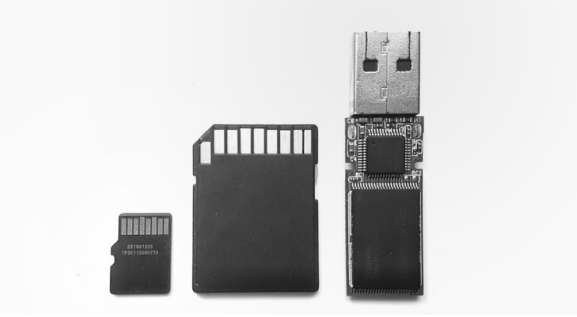
Als erstes sollte der benötigte Speicherplatz für die Backups überprüft werden. Hier lohnt es sich, den Server einmal genauer unter die Lupe zu nehmen, ob irgendwo längst veraltete Daten (ganz besonders alte Backups vor einem Systemwechsel) herumliegen. Anschließend sollte notiert werden, wie viele aktive Daten vorhanden sind (sind es einige 100 GB oder doch schon mehrere TB).

Dann sollte die grundlegende Frage für das Offsite-Backup geklärt werden. Hier gibt es in der Regel drei Möglichkeiten. .

1. MÖGLICHKEIT: KOPIE MITNEHMEN

Die wohl bekannteste Möglichkeit ist, dass ein Mitarbeiter oder Praxisinhaber eine Kopie des Backups mit nach Hause nimmt. Diese Version kostet meist nur eine einmalige Hardwareanschaffung für z. B. einige USB-Festplatten oder Bänder.

Was hierbei natürlich am wichtigsten ist, ist die Verschlüsselung des Backups. USB-Festplatten können schnell beim Transport verloren werden. Wenn die Verschlüsselung stimmt, ist die größte Gefahr hier nur, dass das Backup mit der Zeit nicht mehr fachgerecht jeden Tag gewechselt wird oder dies in Urlaubszeiten vernachlässigt wird.



BACKUPS

2. MÖGLICHKEIT: EXTERNE CLOUD

Die einfachste Möglichkeit besteht darin, das Backup nach erfolgreicher lokaler Sicherung zusätzlich auf einen Cloud-Speicher zu übertragen. Auch hier ist die richtige Verschlüsselung ein wichtiger Aspekt, da die Daten sonst eventuell durch den Cloud-Anbieter oder durch einen Hackerangriff auf diesen gelesen werden könnten.

Diese Methode benötigt das Vertrauen in einen Cloud-Anbieter und kostet meist einen geringen monatlichen Betrag pro GB an gespeicherten Daten (beispielsweise 3 € pro 100 GB). Außerdem muss hier eine DSL-Verbindung mit einer etwas höheren Upload-Geschwindigkeit vorhanden sein. Ein 50.000-KB-Anschluss mit 10.000-KB-Upload sollten es mindestens sein.

3. MÖGLICHKEIT: PRIVATE CLOUD

Ein Kompromiss aus beiden Lösungen ist es, sich eine eigene Cloud daheim zu installieren.

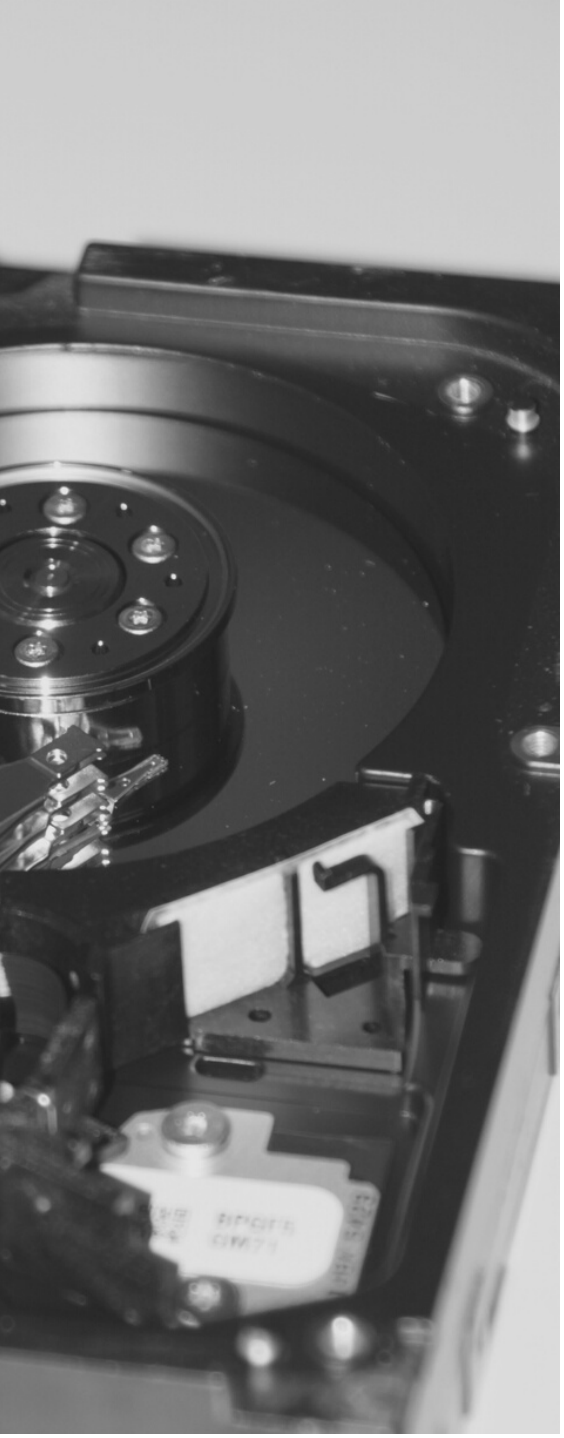
Dies kostet in der Regel nur einen einmaligen etwas höheren Anschaffungs-betrag und die laufende Stromrechnung. Hierbei werden die Daten dann weiterhin automatisch nachts von der Praxis nach Hause übertragen und es können keine Organisationsfehler auftreten. Außerdem landen die Daten nicht in einer unbe-kannten Cloud irgendwo auf der Welt.

Der Nachteil hierbei ist die Pflege und die Prüfung der eigenen Cloud. Hierfür ist eine umfassende Einweisung des EDV-Betreuers notwendig und gelegentliche Wartungsarbeiten an der heimischen Hardware.

Eine private Cloud kostet je nach Speichergrößer 300 bis 500 €.

DAS LOKALE BACKUP

Wenn die Offsite-Frage geklärt ist, bleibt noch das lokale Backup zu klären. Dieses dient hauptsächlich der schnellen Wiederherstellung im Falle eines Systemfehlers oder bei unbeabsichtigter Löschung von Daten. Als Beispiel sei die Installation eines PVS-Updates genannt, die mitten in der Installation einen Fehler verursacht und das ganze System nicht mehr nutzbar macht. Deswegen empfiehlt sich ein Backup auch immer direkt vor einem wichtigen Update. Ebenso können natürlich auch Windows-Updates oder Stromausfälle zu System-fehlern führen. Hier hilft dann ein lokales Backup, um die Daten bzw. das System schnellstmöglich wiederherzustellen.



BACKUPS

Zur Auswahl stehen üblicherweise folgende Medien:

- **USB-Laufwerke in Form von USB-Festplatten oder großen USB-Sticks**
- **Magnetbänder oder ein hybride Lösung (dies sind kleine stabile Kassetten zum Austauschen und Mitnehmen)**
- **Ein NAS (mehrere Festplatten zu einem Netzwerkspeicher zusammengefasst)**
- **Ein zweiter PC in der Praxis für diese Zwecke**

Wichtig wäre hierbei die Wahl anhand der Größe des Backups und der Geschwindigkeit zu treffen.

USB-Festplatten sind die günstigste Wahl. Ihre Haltbarkeit ist dafür aber auch am kürzesten und sie sind relativ langsam (zumindest herkömmliche Festplatten). Ist ein Backup z. B. 250 GB groß, könnte es hier schon deutliche Vorteile bringen, eine USB-3.0/3.1-SSD zu kaufen. Ein NAS im Netzwerk zu haben bringt häufig noch einige weitere Vorteile mit sich, da hier gerne auch Praxisdokumente darauf gespeichert werden können. Ein NAS ist in der Regel die schnellste, aber auch teuerste Lösung. Es kann jedoch im Netzwerk von allen Geräten (ggf. Sono und Co) mitgenutzt werden.